FCA FINANCIAL CONDUCT AUTHORITY

12 Endeavour Square
London
E20 1JN

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

DECISION NOTICE

To: **Gatehouse Bank plc**

Firm Reference Number: **475346**

Address: **The Helicon, One South Place, London EC2M 2RB**

Date: **12 October 2022**

1. ACTION

1.1. For the reasons given in this Notice, the Authority has decided to: impose on Gatehouse Bank plc ("Gatehouse") a civil penalty of £1,584,100 pursuant to section 42(1) of the ML Regulations.

1.2. Gatehouse agreed to resolve this matter and qualified for a 30% (stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £2,263,084.

2. SUMMARY OF REASONS

2.1. Between 9 June 2014 to 5 July 2017, Gatehouse, a Shariah-compliant bank, offered services which primarily focused on real estate. This included offering Shariah-compliant investments in UK and US real estate to investors, Shariah-compliant financing for real estate transactions as well as banking and wealth management facilities to its customers. Gatehouse's customers and investors primarily originated from jurisdictions that posed a higher money laundering risk and some were politically exposed persons.

2.2. Money laundering undermines the integrity and stability of the UK financial markets and authorised financial services firms are at risk of being used by those seeking to launder the proceeds of crime or to finance terrorism. To mitigate the risk of being used to launder the proceeds of crime or finance terrorism, banks

must establish and maintain appropriate, risk-sensitive policies and procedures and implement anti-money laundering ("AML") and financial crime controls.

2.3. The Authority found serious shortcomings in the following areas of Gatehouse's AML policies and procedures in the period from 9 June 2014 to 5 July 2017, thereby breaching provisions of the Money Laundering Regulations 2007:

(a) customer due diligence to verify the identity of its customers, including those who have a beneficial interest in the customers, to establish and adequately scrutinise the source of their wealth and funds;

(b) enhanced due diligence of customers that pose a higher risk of money laundering or terrorist financing, such as those who were domiciled in high risk jurisdictions or were politically exposed persons;

(c) ongoing monitoring of its customers throughout their relationship with Gatehouse, particularly in respect of ensuring that customer due diligence and enhanced due diligence information was kept up-to-date and reflected the current level of financial crime risk presented by each customer; and

(d) internal controls that should have allowed Gatehouse to rectify the abovementioned shortcomings in an orderly and timely manner; in particular the compliance function was under-resourced. Also, although Gatehouse had adopted a three lines of defence model, this did not operate effectively, meaning that front line relationship managers did not appropriately screen customers, and an overburdened Compliance function was left to remedy deficiencies in the quality of due diligence information collected.

2.4. In one example that raises particular concerns, Gatehouse opened an account for a company based in Kuwait (Company A) for the purposes of pooling the funds of Company A's customers for a prospective real estate investment. Gatehouse relied on Company A to carry out customer due diligence of the investors, a large number of whom were high risk, high net worth customers. Gatehouse took inadequate measures to confirm the quality of Company A's AML checks, and did not require Company A to collect information about customers' source of wealth and source of funds which was required under Gatehouse's AML policies. As a result, Gatehouse

accepted US$62 million into an account associated with Company A and its clients without properly vetting the funds for money laundering risk.

2.5. In light of the above failings, pursuant to Regulation 42 of the Money Laundering Regulations 2007, the Authority has therefore decided to impose a civil penalty on Gatehouse of £1,584,100 after 30% (stage 1) discount (£2,263,084 before discount).

2.6. In deciding to impose a civil penalty on Gatehouse, the Authority has taken into account the fact that Gatehouse has taken steps to remedy the deficiencies in its AML controls and co-operated with the Authority. In particular, between June 2014 and August 2016, Gatehouse undertook a compliance review to remediate customer files. Gatehouse invested in improving its AML systems and controls, including engaging external consultants to assist it and to advise on the overhaul of its AML systems and controls. From mid-2016 to mid-2017, Gatehouse established and implemented a new suite of AML and financial crime related policies and procedures which addressed the deficiencies.

3. DEFINITIONS

3.1. The definitions below are used in this Notice.

"ARCC" means Gatehouse's Audit, Risk and Compliance Committee;

"AML" means anti-money laundering;

"the Authority" means the body corporate known as the Financial Conduct Authority;

"beneficial owner" means the term as defined in Regulation 6 of the ML Regulations;

"BRC" means Gatehouse's Board Risk Committee;

"Compliance Review" means the work undertaken by Gatehouse to remediate its customer files between June 2014 and August 2016;

"CTF" means counter terrorist financing;

"Customer Due Diligence" means customer due diligence measures as defined by Regulation 5 of the ML Regulations;

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

"Due Diligence" means together Customer Due Diligence and Enhanced Due Diligence obligations;

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

"Gatehouse" means Gatehouse Bank plc;

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

"JMLSG Guidance" means the guidance that was applicable during the Relevant Period issued by the JMLSG, and approved by the Treasury, on compliance with the legal requirements in the ML Regulations, the regulatory requirements in the Handbook and evolving practice within the financial services industry. The JMLSG Guidance sets out good practice for the UK financial services sector on the prevention of money laundering and combatting of terrorist financing;

"KYC" means the 'Know Your Customer' processes implemented and operated by firms including Gatehouse to protect themselves from facilitating money laundering and terrorist financing;

"2013 Internal Audit" means the internal audit undertaken by a consulting firm on behalf of Gatehouse in relation to its AML controls/risk framework in 2013, the report of which was issued in June 2013;

"2016 Internal Audit" means the internal audit undertaken by Gatehouse in relation to its AML controls/risk framework in 2016, the report for which was issued in September 2016;

"ML Regulations" means the Money Laundering Regulations 2007, which were in force throughout the Relevant Period;

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

"Real Estate Business" means together Gatehouse's Real Estate Finance and Real Estate Investments business;

"Real Estate Finance" means Gatehouse's real estate financing business as described in paragraph 4.1 below;

"Real Estate Investment" means Gatehouse's real estate investment business as described in paragraph 4.1 and 4.2 below;

"Relevant Period" means the period from 9 June 2014 to 5 July 2017 inclusive;

"SPV" means special purpose vehicle;

"the Treasury" means Her Majesty's Treasury; and

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

4. FACTS AND MATTERS

Background

Gatehouse

4.1. Gatehouse was authorised by the Authority on 21 April 2008. During the Relevant Period, Gatehouse offered services which primarily focussed on real estate through its Shariah-compliant investments to investors in UK and US real estate (i.e. its Real Estate Investment business). It also offered Shariah-compliant financing for real estate transactions (i.e. its Real Estate Finance business). Gatehouse also offered treasury and wealth management services.

4.2. Customers of Gatehouse's Real Estate Business were generally SPVs incorporated in foreign jurisdictions (such as Jersey and the Cayman Islands) for the purpose of procuring real estate. Many of the SPVs had complex ownership structures, with various intermediary entities between the SPVs which purchased the real estate

and the SPVs making the real estate investments. For Real Estate Investment transactions, Gatehouse acted as an investment advisor to the SPV and/or provided investment support as a sponsor.

4.3. Investors in Real Estate Investment transactions were sourced by Gatehouse together with Company A. The investors predominantly originated from Gulf Cooperation Council countries (primarily Kuwait) and were typically high net worth individuals, personal investment vehicles, family offices, sovereign wealth funds and financial institutions.

4.4. Many of the customers in the Wealth Management and Treasury segments as well as the underlying investors of the investment vehicles in the Real Estate Business had been introduced to Gatehouse by Company A, which was ultimately responsible for the relationship with the customer. This meant that Gatehouse relied on Company A to gather information for AML purposes as Gatehouse did not have direct relationships with these customers (see below para 4.39).

AML Requirements

4.5. Authorised firms are required by the ML Regulations to put in place policies and procedures to prevent and detect money laundering and terrorist financing. They must therefore establish and implement adequate controls to identify, assess and monitor money laundering risks, by, for example, undertaking Due Diligence that is appropriate to the risk posed by a business relationship. Firms are also required by the ML Regulations to establish and maintain appropriate and risk-sensitive policies and procedures relating to internal control, risk assessment and management, and ensure compliance with these policies.

4.6. Customer Due Diligence, Enhanced Due Diligence and ongoing monitoring are measures designed to reduce the risk of a firm being used by those seeking to launder the proceeds of crime or finance terrorism.

4.7. Firms must carry out Customer Due Diligence on their customers. This means that a firm is obliged to, amongst other things:

(a) identify the customer and verify the customer's identity on the basis of documents or other data obtained from a reliable and independent source; and

(b) identify the beneficial owner of the customer and take adequate measures on a risk-sensitive basis to verify the beneficial owner's identity so the firm is satisfied that it knows who the beneficial owner is. This includes measures to understand the ownership and control structure of the customer.

4.8. If a firm assesses that the business relationship with the customer presents, by its nature, a higher risk of money laundering, it must conduct Enhanced Due Diligence. Further, where a firm proposes to have a business relationship or carry out an occasional transaction with a PEP, in order to fulfil its Enhanced Due Diligence obligations under the ML Regulations, the firm must, amongst other things, take adequate measures to establish the sources of wealth and funds which are involved in the proposed business relationship or occasional transactions, and obtain approval from senior management to establish the business relationship with the PEP.

4.9. If a firm is not able to apply Due Diligence measures, it must not accept a potential new customer or perform any transactions with or for that person. If the firm cannot apply Due Diligence measures to an existing customer, the firm must terminate its existing relationship with that customer.

4.10. A firm must also conduct ongoing monitoring of all business relationships based on its risk assessment of its customers including:

(a) keeping Due Diligence up to date through ongoing review of the Due Diligence file, or reviews of the Due Diligence in response to trigger events; and

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

4.11. Where the business relationship is considered to be of higher risk, the ongoing monitoring must be enhanced; this may entail more frequent and intensive monitoring.

4.12. A firm must also maintain appropriate governance structures and internal controls to ensure that its business remains in compliance with its AML policies and procedures.

Chronology of key events

4.13. On 21 April 2008, Gatehouse was authorised by the Authority.

4.14. On 18 June 2013, a consulting firm engaged by Gatehouse produced an internal audit report setting out the findings of a review into the internal controls and processes adopted by Gatehouse's Compliance function. The 2013 Internal Audit included a review of financial crime risks and covered a review of the AML and KYC procedures performed by the Compliance function. The findings of the 2013 Internal Audit highlighted issues in respect of the Due Diligence carried out by Gatehouse in relation to its wealth management customers. In particular, the 2013 Internal Audit found the following issues in relation to Know Your Customer (KYC) Reviews:

(a) when establishing the sources of wealth and funds for high-net worth individuals, Gatehouse relied on self-certification by such individuals without undertaking independent verification; and

(b) the process of challenge around the sufficiency of Due Diligence information received about a customer was not always documented.

4.15. Hence, in 2013, Gatehouse became aware of issues with its Due Diligence. Gatehouse considered that the deficiencies had arisen due to various factors, including failing to request correct Due Diligence information, a lack of enhanced and ongoing monitoring reviews in the case of high-risk customers and a poor compliance culture within its wealth management business. In addition, Gatehouse knew that its policies and procedures, particularly in relation to the on-boarding of

PEPs, as noted in their own internal audit report, did not meet the requirements and expectations of the Authority.

4.16. From June 2013, Gatehouse's Compliance function undertook a Compliance Review to remediate the deficiencies highlighted by the 2013 Internal Audit.

4.17. As early as June 2014, Gatehouse also knew that its policies, including those relating to the on-boarding of PEPs, did not meet the required standards, and that the policies and procedures would need to be revised alongside a review of the KYC/AML on-boarding process.

4.18. In June 2014, Gatehouse brought the concerns revealed by the 2013 Internal Audit to the attention of the Authority.

4.19. In July 2014, the Compliance Review was extended to all of Gatehouse's customers. This included remediating files for investors in the SPVs that had been introduced by Company A.

4.20. On 8 December 2015, a Compliance report was provided to the ARCC, the membership of which included senior executives. This report highlighted issues and risks which were identified during the remediation exercise and the steps being taken to mitigate those risks. Some of these deficiencies included failures in undertaking Enhanced Due Diligence on customers from high risk jurisdictions, in applying effective measures to identify PEPs, and in undertaking ongoing monitoring of files after customers had been onboarded Examples of the mitigation included the implementation of a screening system and a new AML risk matrix assessment for periodic file reviews.

4.21. On 26 January 2016, Gatehouse wrote to the FCA setting out an update on the firm's progress in respect of KYC issues. This included a list of issues identified while undertaking the remediation exercise.

4.22. On 29 September 2016, Gatehouse produced a further internal audit report which rated its AML processes and controls as inadequate. The 2016 Internal Audit found that areas of high risk included an over-reliance on Compliance (traditionally the 'second line of defence' in the 'three lines of defence' risk management model) in performing customer onboarding work, a lack of ongoing monitoring and insufficient ownership of this process and a failure to implement an effective AML

or CDD training programme for the relationship managers who were in the first line of defence.

4.23. Between late 2016 and July 2017, Gatehouse implemented new AML-related policies and procedures that were better aligned with relevant regulatory requirements, and it took steps to embed an effective three lines of defence model, whereby the 'first line' relationship managers who interacted with customers took on more responsibility for ensuring that Gatehouse carried out appropriate Due Diligence. This included:

(a) the delivery of training to the first line of defence in relation to, amongst other things, the new Customer Due Diligence procedures that the first line was required to follow. This had the effect of equipping the first line to take on the majority of Due Diligence responsibilities;

(b) putting measures in place to address misunderstandings between Gatehouse and Company A in relation to Gatehouse's Due Diligence requirements. Having accepted that Gatehouse could not rely on Company A to collect and assess Due Diligence, Gatehouse worked to train Company A's staff on the process Company A would need to adopt when assisting Gatehouse with collating Due Diligence information from investors; and

(c) introducing service level agreements with third parties who assisted with Due Diligence.

4.24. Regular reviews of systems and controls were also undertaken, including formal audits. By 5 July 2017, the majority of Gatehouse's key AML policies and procedures which implemented the required AML controls took effect.

Customer Due Diligence

4.25. Gatehouse was required to establish and implement risk-sensitive policies and procedures that were tailored to its customer demographic and the business it carried on with those customers. Gatehouse's business posed a higher money laundering risk as many of the customers were based in high risk jurisdictions, a

significant proportion of the beneficial owners of the customers were PEPs and the ownership structures of customers were complex.

4.26. However, during the Relevant Period, Gatehouse failed to establish and implement such policies and procedures. Most of Gatehouse's AML policies and procedures were high level in nature and did not provide sufficient guidance on the measures that needed to be adopted to properly assess, manage and mitigate the money laundering risk posed by its customers. In particular, and as described in further detail below, Gatehouse's inadequate policies and procedures contributed to failings in respect of:

(a) establishing a customer's source of wealth and source of funds (see paragraphs 4.27 to 4.35 below);

(b) the identification of PEPs and failure to conduct Enhanced Due Diligence (see paragraphs 4.36 to 4.40 below); and

(c) ongoing monitoring of a customer relationship (see paragraphs 4.41 to 4.50 below).

Failure to establish source of wealth and source of funds

4.27. In relation to PEPs, firms must apply, on a risk-sensitive basis, adequate measures to establish the PEP's source of wealth and source of funds.

4.28. Gatehouse's policy went further than the requirements set out in the ML Regulations and required the sources of wealth and funds to be established for all individuals irrespective of their risk classification.

4.29. However, until May 2016 Gatehouse's policies did not contain adequate practical guidance in terms of how a customer's sources of wealth and funds would need to be established. The policies lacked definitions for source of wealth and source of funds and did not provide examples of the documents needed to validate these requirements.

4.30. The 2016 Internal Audit found that Gatehouse did not sufficiently validate the sources of wealth and funds for high risk customers, even though this had been

highlighted in the report of the 2013 Internal Audit. In particular, the 2016 Internal Audit found that there was:

(a) inadequate documentary evidence being provided by high risk customers regarding the activity that generated their funds and where their funds were being transferred from; and

(b) a lack of evidence of Gatehouse's contact with customers to establish their sources of wealth and funds for high net-worth and high risk customers.

4.31. The 2016 Internal Audit noted that the root causes of the issues specified above included Gatehouse's approach to the onboarding and ongoing monitoring of customers and Gatehouse's reliance on publicly available information in the absence of documentation regarding a customer's source of wealth and source of funds.

Example of source of funds failings: Company A

4.32. In November 2012, Gatehouse opened a bank account for Company A. Company A used the bank account to pool funds from its clients, primarily based in Gulf Cooperation Council countries, who wished to invest in US real estate funds promoted by Gatehouse. Company A and Gatehouse had agreed that money received from Company A's customers would not be invested until Company A confirmed to Gatehouse that Customer Due Diligence had been satisfactorily completed on the client.

4.33. Gatehouse only required Company A to provide Gatehouse with proof of identity for its clients even though more information should have been collected pursuant to Gatehouse's own internal Due Diligence policies and the relevant regulatory requirements. It was not until October 2015 that concerns were raised by Gatehouse's Compliance function regarding funds being received into the account in the absence of Due Diligence to establish the source of wealth and source of funds of Company A's clients. Company A's bank account was subsequently closed by Gatehouse in October 2015.

4.34. Despite the serious deficiencies in Company A's limited Customer Due Diligence, Gatehouse received US$62 million into this bank account during the Relevant Period

from Company A's clients. This included 29 receipts into the bank account from as many as 26 PEP investors totalling $44.65 million.

Example of source of wealth and source of funds failings: Customer File B

4.35. In June 2015, Gatehouse acted as an investment adviser to Customer B, an SPV incorporated overseas, in relation to a real estate investment transaction. For many of the investors, Gatehouse did not possess documentary evidence regarding the investors' sources of wealth and funds, including an instance where one PEP investor refused to provide evidence of their sources of wealth and funds. Additionally, due to the absence of documentary evidence, Gatehouse relied on publicly available information to establish the investors' sources of wealth and funds, which in some instances did not enable Gatehouse to independently verify the information received about the investors. At a meeting of Gatehouse's Audit Risk and Compliance Committee on 15 September 2015 the committee's chairperson noted that he was very concerned to hear that there were outstanding CDD files in respect of Customer B – he said it was not acceptable to have current deals with incomplete files.

Enhanced Due Diligence

4.36. See para 4.8 above for the general requirements in relation to Enhanced Due Diligence. Particularly relevant for Gatehouse are the following requirements, arising from the ML Regulations and JMSLG:

(a) for customers who present a higher risk of money laundering, the firm must obtain additional information about the customer and the customer's beneficial owner(s); and

(b) in addition, where a firm proposes to have a business relationship or carry out an occasional transaction with a PEP, in order to fulfil its Enhanced Due Diligence obligations under the ML Regulations, the firm must, amongst other things, take adequate measures to establish the sources of wealth and funds which are involved in the proposed business relationship or occasional transactions, and obtain approval from senior management to establish the business relationship with the PEP.

4.37. Many of Gatehouse's customers posed higher money laundering risks because they were from high risk jurisdictions or were SPVs held in overseas jurisdictions who, as referred to in paragraph 4.2 above, had complex ownership structures. For such customers, establishing their shareholder structure is crucial to obtaining a comprehensive understanding of the identity of the ultimate beneficial owner of a customer, in addition to the nature and degree of control that the owner may have over the customer.

4.38. Gatehouse entered into business relationships with customers and transacted with customers without undertaking adequate Enhanced Due Diligence on the customers or customer's ultimate shareholders from whom the customer's wealth was derived, some of whom were PEPs. As a result, Gatehouse failed to fully identify and mitigate potential money laundering risks presented by its highest risk customers.

4.39. Gatehouse failed to understand the extent of its obligations to undertake Due Diligence in respect of the ultimate shareholders of its customers - in particular, Gatehouse considered it was not obliged to undertake Enhanced Due Diligence in relation to investors introduced by Company A. Due Diligence checks undertaken by Gatehouse on the investors were therefore limited to identification and verification documents, without undertaking a more complete assessment of the money laundering risks presented by the investors. Despite having a specific policy on PEPs, on several occasions, Gatehouse failed to identify, in a timely manner, PEPs who were underlying shareholders of its customers.

4.40. One example of the impact of this can be seen in one of the customer files reviewed by the Authority, that of Customer File D. When Gatehouse conducted a risk assessment of this customer's file in December 2014, it only identified one PEP, and failed to identify that there were six further PEPs amongst the underlying shareholders at this time. Further, the failures in ongoing monitoring of Customer D are set out in paras 4.49 to 4.50 below.

Ongoing Monitoring

4.41. The 2016 Internal Audit found that Gatehouse had not performed periodic or event driven reviews since 2011 despite the majority of customers attracting high risk. The 2016 Internal Audit also noted weaknesses in Gatehouse's controls in that:

(a) its systems did not hold all Due Diligence information about a customer, which prevented effective ongoing monitoring at periodic reviews or "trigger" events; and

(b) Gatehouse did not have automated "trigger" systems in place for event driven reviews.

4.42. The 2016 Internal Audit also noted that the absence of ongoing monitoring had stemmed from:

(a) resourcing issues;

(b) a lack of effective AML training for customer facing staff; and

(c) the initial Due Diligence undertaken at the onboarding stage not meeting the required standards.

4.43. The findings of the 2016 Internal Audit are consistent with the Authority's review of policies and procedures. Although Gatehouse's policies did require ongoing monitoring to be undertaken, until 5 July 2017, the policies did not set out details regarding the frequency of ongoing monitoring.

4.44. Inadequate or ineffective ongoing monitoring meant Gatehouse could not adequately reassess the customer relationship as it developed over time, for example, where a customer's business ownership had changed. Gatehouse's failure to reassess Due Diligence information and perform adequate ongoing monitoring in a timely manner resulted in Gatehouse being insufficiently aware of the money laundering risk posed by the customer.

Examples of ongoing monitoring failure: Customer File C

4.45. In December 2015, Gatehouse entered into an agreement to provide a financing facility to Customer C, an SPV used to purchase real estate. Customer C was assessed by Gatehouse to pose a high risk of money laundering.

4.46. Under an agreement between Gatehouse and the investment adviser to Customer C, the investment adviser was required to notify Gatehouse of any change in Customer C's shareholdings. However, these measures were ineffective: despite

there being a change in Customer C's shareholders in May 2016, Gatehouse was not notified of this until November 2016.

4.47. When Gatehouse was notified of the change of shareholders, it did not carry out further Due Diligence to assess whether there had been any material change to the level of money laundering risk posed by this business relationship. It was not until June 2017 that Gatehouse obtained sufficient information regarding the identity of Customer C's new shareholders and their shareholdings, such that it could make this assessment.

4.48. As a result, it was not until June 2017, 13 months after the changes in Customer C's shareholders, and 7 months after Gatehouse became aware of the changes in Customer C's shareholders, that Gatehouse conducted an adequate level of ongoing Due Diligence in respect of Customer C that was reflective of the risk posed by that customer.

Examples of ongoing monitoring failure: Customer File D

4.49. In January 2012, Gatehouse agreed to act as a fund adviser and sponsor to a US based SPV (Customer D) which had been set up to facilitate various real estate investments. Gatehouse did not undertake a risk review of Customer D until almost two years later, in December 2014. Gatehouse took limited and incomplete steps to verify the identity of the investors until the customer file was reviewed in connection with Compliance Review in August 2016.

4.50. This was despite the fact that Gatehouse had been in possession of information since October 2012 which showed that one of the beneficial owners of Customer D was a PEP. Gatehouse further missed an opportunity to identify and mitigate potential money laundering risk in respect of Customer D in December 2014, when it carried out a risk assessment based on an outdated list of investors. While the file was subject to remediation work, it was not until August 2016, that Gatehouse identified a number of Customer D's more recent investors as PEPs. The lack of appropriate Due Diligence and ongoing monitoring meant Gatehouse failed to properly assess the money laundering risk posed by Customer D for almost five years up to 2017.

Internal Controls

4.51. The ML Regulations require firms to establish and maintain risk-sensitive policies and procedures relating to internal control, risk assessment and management, and ensuring compliance with these requirements. While the ML Regulations do not specify precisely what form these internal controls must take, they must be appropriate and adequate. Firms should look to industry standards and regulatory guidance provided by the Authority in determining what sorts of governance structures to put in place.

4.52. Within the Relevant Period, until the end of 2016, the ARCC oversaw Gatehouse's AML framework. Its responsibilities included monitoring the effectiveness of Gatehouse's internal controls and risk management systems and ensuring that appropriate actions were taken in response to internal audits and reviews that were undertaken. The latter included the responsibility to review and monitor management's responsiveness to the findings and recommendations of the internal auditors.

4.53. At the end of 2016, the ARCC was split into two new committees, the Audit Committee and the BRC. The BRC took over responsibility for reviewing the effectiveness of Gatehouse's internal controls and risk management systems. It was also responsible for approving compliance policies and monitoring compliance issues, AML and financial crime policies, compliance monitoring and compliance training.

4.54. The ARCC was regularly alerted to AML control failings, such as customers being onboarded, or their funds being accepted without full due diligence information having been received; or customers having been allowed to withdraw funds without adequate due diligence having been done.

4.55. The 2013 Internal Audit Report found that, although there were some positive points around the engagement between compliance and senior management, certain issues persisted. The compliance function at Gatehouse felt that they ran into difficulties with the rest of the business when they tried to perform their role. They did not feel they got adequate support from the ARCC or from senior management, to encourage the rest of Gatehouse to support compliance in its

efforts. When they raised issues and concerns with the ARCC, they did not feel these were appropriately dealt with.

4.56. For example, the compliance function reported to ARCC in September 2015 that Company A had only provided 69 out of 233 files, and it was noted that Company A seemed unhappy with the level of information that was required. One member of the ARCC suggested weekly calls to resolve outstanding issues between Gatehouse and Company A, and senior management did take other steps to try to improve the situation. However, this did not resolve the issues entirely as concerns were again escalated to the ARCC in April 2016. At this time, on being questioned as to why they were not making quicker progress in the remediation exercise, the compliance function noted that, in most instances, the relationship managers did not have the Due Diligence information. Ultimately, compliance needed to supplement the information received from Company A with publicly available information about the investor.

4.57. There were serious deficiencies in the internal control and oversight model Gatehouse had implemented for managing AML risks, as identified by Gatehouse itself in a number of internal reports. These deficiencies resulted in an ineffective governance model for managing money laundering risks throughout the majority of the Relevant Period. In particular, Gatehouse:

(a) having implemented a three lines of defence model, failed to ensure it operated effectively (see paragraphs 4.58 to 4.63 below); and

(b) failed to adequately resource its Compliance function (see paragraphs 4.64 to 4.66 below).

Ineffective three lines of defence model

4.58. Gatehouse's internal audit function identified in 2016 that the firm had operated a flawed three lines of defence model of risk management, a failing which prevented Gatehouse from meeting its obligation to ensure compliance with its policies and procedures in respect of Due Diligence and ongoing monitoring.

4.59. Gatehouse identified that in this model, all business units, including the front office and customer-facing activity, are the first line of defence in charge of identifying, assessing and controlling the risks of their business. The second line of defence

includes the Compliance function. The third line of defence is carried out by the internal audit function. However, throughout most of the Relevant Period, Gatehouse's three lines of defence model was not operating effectively in that Gatehouse's Compliance function assumed responsibilities which would ordinarily sit with the first line of defence. This was demonstrated by the fact that, in addition to its normal compliance-related responsibilities, Gatehouse's Compliance function was responsible for carrying out Due Diligence when onboarding new customers as well as leading the customer file remediation as part of the Compliance Review to rectify the deficiencies in previously obtained Due Diligence.

4.60. The reasons for devolving responsibility away from the first line of defence included:

(a) the high number of concerns identified during the Compliance Review about the level and quality of Due Diligence conducted by the first line;

(b) Gatehouse's first line of defence lacked an adequate understanding of the Due Diligence requirements and their responsibilities; and

(c) the absence of bespoke and effective AML/due diligence training being provided to all first line business areas.

4.61. The 2016 Internal Audit found that Gatehouse had not implemented an effective AML and CDD training programme focused specifically towards Relationship Managers (the first line of defence). This was despite the issues that resulted in the Compliance Review being started, demonstrating a clear need to promote AML awareness across all staff. An effective AML training programme for first line staff was not implemented and delivered until April 2017.

4.62. The Authority considers that the lack of a clear division of responsibility for Due Diligence between the first and second line of defence meant that the Compliance function as the second line of defence did not act as an effective means of monitoring and mitigating money laundering risks. Since, at least until early 2016, the Compliance function was insufficiently resourced (see below), the result was that it was unable to undertake its compliance monitoring effectively.

4.63. Gatehouse was aware of the issues with its three lines of defence model as early as June 2014. However, despite the issues being flagged to the ARCC on a number

of occasions, limited steps were taken to address the ineffectiveness of Gatehouse's risk management framework.

Inadequate resourcing of the compliance function

4.64. In June 2014, Gatehouse's internal auditors noted that resources would need to be dedicated to the Compliance Review and remediation exercise promptly, given there had been very little progress on the remediation of customer files since the 2013 Internal Audit.

4.65. In addition, in June 2014, Gatehouse's external auditors highlighted to Gatehouse's management the need for the level of resourcing within the Compliance function to be evaluated "to ensure that quality and quantity of resource was sufficient". Gatehouse's Board and the ARCC were also aware that the level of resourcing was impacting the Compliance function.

4.66. The resourcing issues within the compliance function persisted for almost 2 years, from June 2014 until at least early 2016.

5. FAILINGS

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

5.2. On the basis of the facts and matters set out above, the Authority considers that, during the Relevant Period, Gatehouse breached Regulation 20(1) of the ML Regulations in that Gatehouse failed to establish and maintain appropriate and risk-sensitive AML policies and procedures in relation to:

(a) Customer Due Diligence in order to identify its customers, including those with beneficial interests in the customers, to establish and adequately scrutinise the sources of their wealth and funds;

(b) Enhanced Due Diligence in any situation that by its nature poses a higher risk of money laundering or terrorist financing;

(c) adequate ongoing and enhanced monitoring of its customers throughout their relationship with Gatehouse; and

(d) establishing effective internal controls to implement such policies and procedures, and adequately managing the remediation of the AML deficiencies once they were discovered.

Deficiencies in AML controls

5.3. As a result, Gatehouse's conduct failed to comply with Regulations 7(1) to (3), 8(1) and (3) and 14(1) and (4) of the ML Regulations. In particular, Gatehouse failed to:

(a) take adequate steps to establish the sources of wealth and funds of many customers, especially in respect of investors introduced to Gatehouse by Company A;

(b) identify PEPs and as a result carry out Enhanced Due Diligence; and

(c) consistently carry out ongoing monitoring between June 2011 (well before the start of the Relevant Period) and the end of 2016, despite many of its customers posing a high money laundering risk.

Deficiencies of internal controls and governance

5.4. In addition to Gatehouse's failings in relation to AML policies, procedures and practices discussed above, Gatehouse failed to comply with Regulation 20(1)(d) and (f). In particular, Gatehouse failed to:

(a) Implement an effective governance model for managing money laundering risks throughout the majority of the Relevant Period; and

(b) Maintain an adequate level of resourcing within Gatehouse's Compliance function throughout the majority of the Relevant Period (until early 2016). This impacted the Compliance function's ability to remediate the deficiencies in Gatehouse's AML controls.

5.5. The weaknesses in Gatehouse's AML controls created an unacceptable risk that Gatehouse could be used by those seeking to launder money or finance terrorism.

6. SANCTION

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

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

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

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

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

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

6.7. Paragraph 19.15.5 of the Enforcement Guide states that, when imposing or determining the level of a financial penalty under the ML Regulations, the Authority's policy includes having regard, where relevant, to relevant factors in DEPP 6.2.1G (deciding whether to take action) and DEPP 6.5 to DEPP 6.5D (determining the appropriate level of financial penalty).

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

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

Financial Penalty – Breach of the Money Laundering Regulations

Step 1: Disgorgement

6.9. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.

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

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

Step 2: the seriousness of the breach

6.12. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

6.13. The Authority considers that the revenue generated by Gatehouse is indicative of the harm or potential harm caused by its breaches and failings. The Authority has therefore determined a figure based on a percentage of Gatehouse's relevant revenue. The period of Gatehouse's breach was from 9 June 2014 to 5 July 2017. The Authority considers Gatehouse's relevant revenue for its failings relating to the abovementioned business areas for this period to be **£9,429,524**.

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

Level 1 – 0%

Level 2 – 5%

Level 3 – 10%

Level 4 – 15%

Level 5 – 20%

6.15. In assessing the seriousness level, the Authority takes into account various factors which reflect the impact and nature of the breach. 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:

(a) DEPP 6.5A.2G(11)(b) - "*the breach revealed serious or systemic weaknesses in the firm's procedures or in the management systems or internal controls relating to all or part of the firm's business*"; and

(b) DEPP 6.5A.2G(11)(d) - "*the breach created a significant risk that financial crime would be facilitated, occasioned or otherwise occur*".

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

(a) DEPP 6.5A.2G(12)(a) – *"little, or no, profits were made or losses avoided as a result of the breach, either directly or indirectly"*;

(b) DEPP 6.5A.2G(12)(b) – "*there was no or little loss to consumers, investors or other market users individually and in general"*; and

(c) DEPP 6.5A.2G(12)(e) – *"the breach was committed negligently or inadvertently".*

6.17. Taking these factors into account, the Authority considers the seriousness of the failings to be level 3 and so the Step 2 figure is 10% of **£9,429,524.**

6.18. The figure after Step 2 is therefore **£942,952.**

Step 3: mitigating and aggravating factors

6.19. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2 to take into account factors which aggravate or mitigate the breach.

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

(a) Gatehouse was aware from as early as June 2013 (i.e. prior to the Relevant Period) that there were deficiencies in its AML controls. However, limited or no steps were taken until mid-2014 to commence remediation of those deficiencies;

(b) the Authority has published guidance on the steps firms can take to reduce their financial crime risk and has provided examples of good and bad practice since 2011. In addition, since 1990, the JMLSG has published detailed written guidance on AML controls. During the Relevant Period, the JMLSG provided guidance on compliance with the legal requirements of the ML Regulations, regulatory requirements in the Authority's Handbook and evolving practice within the financial services industry. Before, and during, the Relevant Period, the Authority published the following guidance relating to AML controls, which set out good practice examples to assist firms in interpreting the ML Regulations:

(i) in June 2011, the Authority published a report titled "*Banks' management of high money-laundering risk situations: How banks deal with high-risk customers (including politically exposed persons), correspondent banking relationships and wire transfers*". The report set out the requirements banks must adhere to when dealing with high-risk customers and PEPs and examples of good and poor practices identified at banks;

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

(iii) in November 2014, the Authority published a report titled "*How small banks manage money laundering and sanctions risk*". The report set out findings relating weaknesses in practices adopted by small banks in relation to Enhanced Due Diligence and ongoing monitoring of high risk customers and PEPs; and

(c) the Authority published a number of Decision Notices and Final Notices against firms for AML weaknesses both before and during the Relevant Period, including Guaranty Trust (UK) Bank Limited on 8 August 2013, Standard Bank Plc on 22 January 2014, Barclays Bank plc on 25 November 2015, Sonali Bank (UK) Limited on 12 October 2016 and Deutsche Bank AG on 30 January 2017. These actions stressed to the industry the Authority's view of firms with AML deficiencies especially in relation to higher risk customers and the importance of compliance with AML requirements. Gatehouse was accordingly aware of the importance of implementing and maintaining robust AML systems and controls, and its importance to the Authority.

6.21. Having taken into account these aggravating factors, the Authority considers that the Step 2 figure should be increased by 20%.

6.22. The figure after Step 3 is therefore **£1,131,542.**

Step 4: adjustment for deterrence

6.23. Pursuant to DEPP 6.5A.4G, if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm that committed the breach, or others, from

committing further or similar breaches, then the Authority may increase the penalty.

6.24. The Authority considers that the Step 3 figure of **£1,131,542** does not represent a sufficient deterrent to Gatehouse Bank and others, and so has increased the penalty at Step 4 by a multiplier of 2.

6.25. The figure after Step 4 is therefore **£2,263,084.**

Step 5: settlement discount

6.26. 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.

6.27. The Authority and Gatehouse reached agreement at Stage 1 in relation to all relevant facts, all issues as to whether those facts constitute breaches and the financial penalty], and so a 30% discount applies to the Step 4 figure.

6.28. The figure after Step 5 is therefore **£1,584,100** (rounded down to the nearest £100).

Total penalty

6.29. The Authority has therefore decided to impose a financial penalty on Gatehouse of **£1,584,100.**

7. PROCEDURAL MATTERS

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

Decision makers

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

The Tribunal

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

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

7.5. Further details are available from the Tribunal website:

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

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

Manner and time for payment

7.6. The financial penalty must be paid in full by Gatehouse to the Authority by no later than 28 October 2022.

If the financial penalty is not paid

7.7. If any or all of the financial penalty is outstanding on 28 October 2022, the Authority may recover the outstanding amount as a debt owed by Gatehouse and due to the Authority.

Access to evidence

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

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

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

Third party rights

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

Confidentiality and publicity

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

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

Authority contacts

7.12. For more information concerning this matter generally, contact Kate Penhallurick (direct line: 020 7066 6374) or Steve Page (020 7066 1420) of the Enforcement and Market Oversight Division of the Authority.

Mark Steward
Settlement Decision Maker, for and on behalf of the Authority

David Geale
Settlement Decision Maker, for and on behalf of the Authority

ANNEX A - RELEVANT STATUTORY AND REGULATORY PROVISIONS AND GUIDANCE

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

Relevant extracts from the Money Laundering Regulations 2007

Meaning of customer due diligence measures

1. Regulation 5 states:

"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.

Meaning of beneficial owner

2. Regulation 6 states:

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

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

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

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

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

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

Application of customer due diligence measures

3. Regulation 7 states:

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

(a) establishes a business relationship;

(b) carries out an occasional transaction;

(c) suspects money laundering or terrorist financing;

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

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

(3) A relevant person must—

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

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

Ongoing monitoring

4. Regulation 8 states:

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

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

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

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

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

Enhanced customer due diligence and ongoing monitoring

5. Regulation 14 states:

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

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

(b) In any other situation which by its nature can present a higher risk of money

laundering or terrorist financing.

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

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

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

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

[…]

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

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

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

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

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

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

(i) a state other than the United Kingdom;

(ii) a Community institution; or

(iii) an international body,

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

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

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

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

Policies and procedures

6. Regulation 20 states:

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

(a) customer due diligence measures and ongoing monitoring;

(b) reporting;

(c) 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- […]

(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; […]

Relevant extracts from the JMLSG Guidance

7. The JMLSG Guidance provisions set out below are taken from the November 2014 version of the guidance. The JMLSG Guidance is periodically updated, however, there were no material changes to the provisions set out below during the Relevant Period.

Part I, Chapter 2 Internal Controls

General legal and regulatory obligations

8. Paragraph 2.1 states:

There is a requirement for firms to establish and maintain appropriate and risk-based policies and procedures in order to prevent operations related to money laundering or terrorist financing. FSA-regulated firms have similar, regulatory obligations under SYSC.

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

Monitoring effectiveness of money laundering controls

9. Paragraph 3.27 states:

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

Part I, Chapter 5 Customer Due Diligence

Meaning of customer due diligence measures and ongoing monitoring

10. Paragraph 5.1.4 states:

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

11. Paragraph 5.1.6 states:

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

12. Paragraph 5.1.10 states:

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

13. Paragraph 5.1.11 states:

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

14. Paragraph 5.1.12 states:

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

- *to help the firm, at the time due diligence is carried out, to be reasonably satisfied that customers are who they say they are, to know whether they are acting on behalf of another, and that there is no legal barrier (e.g. government sanctions) to providing them with the product or service requested; and*

- *to enable the firm to assist law enforcement, by providing available information on customers or activities being investigated.*

15. Paragraph 5.1.13 states:

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

Application of Customer Due Diligence measures

16. Paragraph 5.3.1 states:

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

17. Paragraph 5.3.110 states:

Where an entity is known to be linked to a PEP (perhaps through a directorship or shareholding), or to a jurisdiction assessed as carrying a higher money laundering/terrorist financing risk, it is likely that this will put the entity into a higher risk category, and that enhanced due diligence measures should therefore be applied (see sections 5.5 and 5.7).

18. Paragraph 5.3.125 states:

To the extent consistent with the risk assessment carried out in accordance with the guidance in Chapter 4, the firm should ensure that it fully understands the company's legal form, structure and ownership, and must obtain sufficient additional information on the nature of the company's business, and the reasons for seeking the product or service.

19. Paragraph 5.3.144 states:

Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, firms should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identities of other shareholders and/or controllers. It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may influence its operations (political connections, etc).

Enhanced due diligence

20. Paragraph 5.5.1 states:

A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the 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.

21. Paragraph 5.5.2 states:

As a part of a risk-based approach, therefore, firms may need to 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.*

22. Paragraph 5.5.5 states:

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.

23. Paragraph 5.5.18 states:

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

24. Paragraph 5.5.25 states:

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

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

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

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

d. *conduct enhanced ongoing monitoring of the business relationship.*

Monitoring customer activity

25. Paragraph 5.7.1 states:

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

- *Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile;*

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

26. Paragraph 5.7.2 states:

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

27. Paragraph 5.7.12 states:

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

Part I, Chapter 7 **Staff awareness, training and alertness**

Why focus on staff awareness and training?

28. Paragraph 7.1 states:

One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions which may prove to be suspicious.

29. Paragraph 7.2 states:

The effective application of even the best designed control systems can be quickly compromised if the staff applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the firm's AML/CTF strategy.