DLA PIPER

AUTUMN 2016

AML BULLETIN

Regulatory News Update from DLA Piper

HM Treasury publishes advisory note on money laundering and terrorist financing controls in overseas jurisdictions

FCA publishes its annual anti-money laundering report for 2015/16

Solicitors Regulation Authority publishes Risk Outlook for 2016/17

FCA issues policy statement on financial crime reporting

HM Treasury publishes memorandum and consultation on the transposition of the Fourth Money Laundering Directive into UK law

National Crime Agency publishes the national strategic assessment of serious and organised crime 2016

FCA speech by Megan Butler on a more effective approach to combatting financial crime

ABI checklist on effective counter fraud measures

Home Office response to consultation on reform of anti-money laundering and counter-terrorist financing regime

FCA imposes penalties on Sonali Bank (UK) and its former Money Laundering Reporting Officer for serious anti-money laundering systems failings

New President of the Financial Action Task Force outlines objectives for 2016/17

European Commission legislative proposal for Directive amending Fourth Money Laundering Directive

EBA publishes opinion on the European Commission's proposal to bring virtual currencies into the scope of the Fourth Money Laundering Directive

CPMI final report on correspondent banking

EU Delegated Regulation identifying high-risk third countries under Fourth Money Laundering Directive

CONTENTS

UK NEWS & ENFORCEMENT ACTION **04**

HM Treasury publishes advisory note on money laundering and terrorist financing controls in overseas jurisdictions 05

FCA publishes its annual anti-money laundering report for 2015/16 06

Solicitors Regulation Authority publishes Risk Outlook for 2016/17 08

FCA issues policy statement on financial crime reporting 09

HM Treasury publishes memorandum and consultation on the transposition of the Fourth Money Laundering Directive into UK law 11

National Crime Agency publishes the national strategic assessment of serious and organised crime 2016 14

FCA speech by Megan Butler on a more effective approach to combatting financial crime 15

ABI checklist on effective counter fraud measures 16

Home Office response to consultation on reform of anti-money laundering and counter-terrorist financing regime 17

FCA imposes penalties on Sonali Bank (UK) and its former Money Laundering Reporting Officer for serious anti-money laundering systems failings 19

INTERNATIONAL NEWS & ENFORCEMENT ACTION **20**

New President of the Financial Action Task Force outlines objectives for 2016/17 21

European Commission legislative proposal for Directive amending Fourth Money Laundering Directive 22

EBA publishes opinion on the European Commission's proposal to bring virtual currencies into the scope of the Fourth Money Laundering Directive 24

CPMI final report on correspondent banking 26

EU Delegated Regulation identifying high-risk third countries under Fourth Money Laundering Directive 28

KEY CONTACTS **29**

Introduction

DLA Piper's Financial Services Regulatory team welcomes you to the Autumn 2016 edition of our Anti-Money Laundering (**AML**) Bulletin.

In this issue, we provide updates on AML news and enforcement action in the UK and internationally. This issue provides an update on recent UK AML news, including the publication of HM Treasury's advisory note on money laundering and terrorist financing controls in overseas jurisdictions, the release of the FCA's anti-money laundering annual report 2015/16 and the publication of the SRA's Risk Outlook 2016/17. This issue also provides an update on HM Treasury's consultation on the transposition of the Fourth Money Laundering Directive and the HM Treasury memorandum on proposed amendments to the Directive.

This edition also provides an update on recent international AML news, including the European Commission's legislative proposal for a Directive amending the Fourth Money Laundering Directive, the CPMI's final report on correspondent banking and the EBA's opinion on the European Commission's proposal to bring virtual currency entities into the scope of the Fourth Money Laundering Directive. This issue also provides an update on the FCA enforcement case against Sonali Bank (UK) Limited, which resulted in the imposition of a £3,250,600 fine, and the action taken against its former Money Laundering Reporting Officer.

We hope that you find this update helpful. Your feedback is important to us, so if you have any comments or would like further information, please contact one of our specialists detailed at the end of this publication.

UK NEWS & ENFORCEMENT ACTION

HM TREASURY PUBLISHES ADVISORY NOTE ON MONEY LAUNDERING AND TERRORIST FINANCING CONTROLS IN OVERSEAS JURISDICTIONS

On 6 July 2016, HM Treasury published an advisory note on money laundering and terrorist financing controls in overseas jurisdictions (**the Advisory Note**) which focuses on two statements published by the Financial Action Task Force (**FATF**) on 24 June 2016. These statements identify jurisdictions that have strategic deficiencies in terms of their anti-money laundering (**AML**) and counter terrorist financing (**CTF**) regimes. The statements are annexed to the Advisory Note.

The first statement is a public statement that addresses the AML and CTF regimes of two jurisdictions: Democratic People's Republic of Korea (**DPRK**) and Iran. In this statement, FATF called on its members and other jurisdictions to apply counter-measures to protect the international finance system from money laundering and terrorist financing risks that may be occurring in DPRK. It explained that it remains concerned that DPRK has not addressed deficiencies in its AML and CTF regime. FATF urged DPRK to address this immediately. FATF advised that its members and other jurisdictions alert financial institutions to give special attention to transactions with DPRK, including transactions with DPRK companies, financial institutions and those acting on their behalf. FATF also asked that enhanced scrutiny and effective counter-measures are put in place by all jurisdictions.

This statement also addressed the AML and CTF regimes of Iran. FATF positively recognised Iran's adoption of an Action Plan to address deficiencies in its AML and CTF regimes and its decision to accept technical assistance in implementing the Action Plan. FATF explained that it has suspended counter-measures for 12 months in order to monitor Iran's progress in implementing the Action Plan; but indicated that they may be re-imposed if sufficient progress is not made. FATF stated that Iran will remain on this statement until the full Action Plan has been completed. FATF also stated that it is still concerned about the risk of terrorist financing emanating out of Iran and, accordingly, advised its members to inform their financial institutions to apply an enhanced due diligence process with regard to transactions with natural or legal persons from Iran. FATF concluded that it would monitor the progress of Iran.

On the basis of this statement, HM Treasury advised that financial institutions treat DPRK and Iran as high-risk jurisdictions for the purposes of the Money Laundering Regulations 2007 and, accordingly, that enhanced due diligence measures should be applied.

The second statement published by FATF focused on other jurisdictions that have strategic deficiencies in terms of their AML and CTF regimes. FATF notes that it has not reviewed all jurisdictions so the list provided in this statement is not exhaustive. The jurisdictions identified in this statement are Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao PDR, Syria, Uganda, Vanuatu, and Yemen. Action Plans have been developed by these jurisdictions with FATF and each jurisdiction has provided a high-level political commitment to address the deficiencies in their AML and CTF regimes. FATF called on the jurisdictions listed in this statement to implement the Action Plans and stated that it would monitor their implementation.

On the basis of this statement, HM Treasury advised that financial institutions take appropriate actions in relation to the listed jurisdictions, which may include enhanced due diligence measures in high-risk situations.

FATF also identified jurisdictions in the second statement which are no longer subject to its ongoing global AML and CTF compliance process. These jurisdictions were Myanmar and Papua New Guinea.

FCA PUBLISHES ITS ANNUAL ANTI-MONEY LAUNDERING REPORT FOR 2015/16

On 12 July 2016, the Financial Conduct Authority (**FCA**) published its annual anti-money laundering (**AML**) report for 2015/16 (**the Report**). The FCA explained its key role in ensuring that firms have measures in place to prevent financial crime. The Report provided the FCA with an opportunity to report on its AML work from the last year. Importantly, in the Report the FCA reiterated that addressing financial crime and AML will remain one of its seven priorities, as stated in its business plan for 2016/17.

In the Report, the FCA addressed the developments in its AML supervision strategy, and also outlined the findings and outcomes of its recent supervision work. The FCA also discussed policy developments, the independent assessment of its AML supervision and how it cooperates with other supervisors both inside and outside of the UK. The Report has a separate section titled 'Looking ahead' in which the FCA outlines key aspects of the AML work it intends to carry out over the coming year.

The FCA clarified that AML systems and controls remain high on its agenda and explained that its approach to AML supervision is risk-based. The FCA also explained that it aims to ensure effective and proportionate AML standards in regulated firms. Accordingly, the FCA said that it allocates its resources on a risk-based model by focusing resources on those firms and activities that present the highest risk of money laundering.

The FCA stated that it has continued to implement its AML supervisory strategies which includes two programmes. One of the programmes is called the Systematic Anti-Money Laundering Programme. This programme focuses on major retail and investment firms operating in the UK. The FCA stated that it also focuses on overseas operations which may be deemed high risk or of strategic importance. The other programme focuses on carrying out regular AML inspections of a group of other firms which pose a high financial crime risk. The FCA explained that it also utilises thematic reviews, outreach programmes, intelligence received about financial crime risks and events from whistleblowers, law enforcement agencies and other regulators, as components of its approach to AML supervision. It explained that it is planning on enhancing its supervision strategy by increasing the breadth of the population of firms regulated by the FCA. The FCA also proposed the introduction of a financial crime data return so that firms posing a high risk of financial crime can be identified via increased transparency and so that this data can be aggregated and published.

The FCA indicated that it is pleased with the outcomes of the above programmes so far. Another positive point identified by the FCA was that major banks have started to recognise that AML is an issue that requires the attention of senior management. However, the FCA did indicate that weaknesses have been found in the AML controls of major banks. It indicated that some banks were devoting insufficient resources to AML systems and controls, which resulted in staff often lacking the relevant knowledge of AML processes. The FCA indicated that it might refuse an application for a Variation of Permission if inspections found that there were major AML weaknesses within the applicant firm. The FCA said that it needed to intervene in the AML procedures of 12 firms between 2012-2014 due to their weaknesses, and indicated that it has intervened on two further occasions during 2015-16. The FCA stated that it has the ability to commission reports under section 166 of the Financial Services and Markets Act 2000 (**FSMA**) (skilled persons reports) in order to obtain an independent view of the systems and controls implemented by firms to combat finance crime.

The FCA also described the policy developments of the previous year; focusing, in particular, on de-risking. Referring to a report it produced in July 2015,

it identified that, in many cases, banks were carrying out a cost-benefit analysis with regard to whether to maintain certain client accounts that were not always related to financial crime risks. The FCA also outlined that it wants to foster innovation and reduce the cost of AML compliance by ensuring that the Fourth EU AML Directive is implemented so as to allow the use of digital identification. It also explained that it is working with the Financial Action Task Force (**FATF**) and the Financial Stability Board to ensure that AML standards are consistent on a global scale. The FCA highlighted that part of its role is to protect the integrity of the financial services sector and, accordingly, it indicated that it intends to encourage banks to communicate better with clients.

The FCA stated that the IMF has recently reviewed its AML supervision of higher risk banks and concluded that it is adequate. However, the FCA stated that it has some concern about the supervision of other banks.

The FCA explained in the Report that it has been involved with other EU banking supervisors through the AML Committee of the joint European Supervisory Authorities (**ESA**). It explained that its contribution included drafting guidelines on enhanced customer due diligence, and on factors that financial and credit institutions should consider when assessing money laundering and terrorist financing risk. Following the release of the ESA's draft guidelines in October 2015 on risk factors and risk-based approach to supervision, the FCA expects that the final guidelines will be published later in 2016. Furthermore, the FCA also explained that it had established a mechanism for improved information-sharing between financial institutions and law enforcement organisations as members of the Joint Money Laundering Intelligence Taskforce.

Looking ahead to the coming year, the FCA said that it will continue with its current supervision strategy and begin to utilise the data from the new data return. It also indicated that it will continue to work with the Treasury to implement the Fourth EU Anti-Money Laundering Directive and introduce its new de-risking programme. The FCA indicated that another evaluation of AML supervision is due to take place in late 2017 and early 2018 by FATF.

SOLICITORS REGULATION AUTHORITY PUBLISHES RISK OUTLOOK FOR 2016/17

On 25 July, the Solicitors Regulation Authority (**SRA**) published its Risk Outlook for 2016/17 (**the Report**). The Report provides the legal services sector with an indication of the areas on which the SRA is focusing its attention and why. The Report also provides an indication as to how the SRA is currently helping to control certain risks in the public interest and how firms should be managing risk.

The Report identifies seven priority risks; namely the lack of access to legal services, standards of service and considering vulnerability, information security, independence and integrity, protecting client money, money laundering and diversity. This summary will focus on the money laundering aspect of the Report.

The SRA explained that the risk of money laundering was described as 'significant' to the legal sector in the UK's National Risk Assessment (**NRA**). The NRA identified that there are gaps in the knowledge of the legal sector regarding its role in preventing money laundering. However, the SRA indicated that it did understand the difficulties encountered by solicitors in relation to money laundering; for example, due to legal professional privilege. Despite this, the SRA highlighted that the number of Suspicious Activity Reports passed to the Financial Conduct Authority remains low when compared with the size of the industry and the nature of its activities. The SRA indicated that the National Crime Agency also reported similar findings. As a result of its thematic review, the SRA said that generally firms have effective processes, procedures and controls in place but reminded firms that they must keep these policies up to date.

The SRA also reminded solicitors and firms that they have obligations under the Money Laundering Regulations 2007, Proceeds of Crime Act 2002, Terrorism Act 2000 and SRA Handbook 2011. It encouraged firms to take a risk-based approach to anti-money laundering (**AML**) policies and controls and also provided examples of how firms can implement such procedures cost-effectively. For example, by using online resources (such as the SRA's website) they can research the warning signs they should look out for to prevent money laundering.

The SRA explained that the UK Government's Action Plan on AML and counter-terrorist financing and the introduction of the Fourth EU AML Directive is likely to put further pressure on the legal sector. The SRA also highlighted the consequences of failing to check or report possible money laundering activities by referring to the findings of the Solicitors Disciplinary Tribunal in which solicitors were struck off or fined as a result of failing to prevent or report possible incidents of money laundering.

FCA ISSUES POLICY STATEMENT ON FINANCIAL CRIME REPORTING

On 29 July 2016, the Financial Conduct Authority (**FCA**) published a policy statement on the reporting of financial crime (**PS 16/19**). In this statement, the FCA summarises the responses it received to its December 2015 consultation on the introduction of the financial crime report (**CP 15/42**). Chapter six of CP 15/42 reflects the FCA's proposal for the amendment of chapter 16 of the Supervision manual, in order to enable the FCA to obtain regular, accurate and consistent data to identify financial crime risk. The FCA has also taken on board the comments on its publication of the proposals in a quarterly consultation paper and it has accordingly published the final rules in a standalone policy statement to maximise transparency.

The FCA received 32 responses from firms and trade associations. Although the majority of the respondents were supportive, many of them required further clarifications on definitions and guidance notes. Many expressed concern about the implementation and reporting timescales, as well as about the requirement for single-entity reporting.

The FCA addressed the feedback received and touched on the following issues: implementation and reporting timescales, group reporting, guidance and definitions, including operating jurisdictions, customer information, compliance information, sanctions-specific information and fraud, electronic money institutions, revenue thresholds for intermediaries, investment firms and consumer credit firms and publication of aggregated financial crime data.

The most important of the changes introduced are summarised below.

1. The FCA excludes both pure general insurers and general insurance intermediaries, as well as credit unions from the initial implementation. It aims, however, to bring them into scope at a later date.
2. Revisiting the length of the remittance period, the FCA doubled the submission period from 30 days to a total of 60 days. A firm with a 31 December year end is now required to submit the Financial Crime Return in late March. The implementation will proceed in the existing timeframe, but the FCA will only expect firms to submit the Financial Crime Return on a best endeavours basis for the first reporting cycle.
3. The FCA implements an optional group submission mechanism for the Financial Crime Return and submitters will have the option to submit on a group or single regulated entity basis, as long as the firms included all share a common financial year end.
4. The FCA decided to apply a £5 million revenue proportionality threshold to investment firms, in addition to intermediaries, electronic money institutions and full permission consumer credit firms.
5. The FCA requires firms to report only those jurisdictions that the firm either 'operates' in or has assessed as high-risk, within the last two years. The FCA has adjusted the definition of 'operates' to 'where the firm has a physical presence through a legal entity or actively markets its services'.

The Handbook provisions come into force on 31 December 2016.

HM TREASURY PUBLISHES MEMORANDUM AND CONSULTATION ON THE TRANSPOSITION OF THE FOURTH MONEY LAUNDERING DIRECTIVE INTO UK LAW

Background

The Fourth Anti-Money Laundering Directive (**4MLD**) was published on 5 June 2015, came into force on 25 June 2015 and was initially expected to be implemented by member states by 26 June 2017.

On 5 July 2016, the European Commission (**EC**) published a proposal for the amendment of the 4MLD and suggested its expedited transposition by 1 January 2017 (Article 67). The EC proposals included amendments regarding the definition of beneficial owner (article 3(6)), the provisions regarding beneficial ownership information for corporate and other legal entities (Article 30), as well as similar information for trusts and similar structures (Article 31).

HM Treasury Memorandum

On 5 September 2016, HM Treasury published a memorandum regarding the amendment of the 4MLD. HM Treasury generally welcomed the proposals suggested by the EC, but did raise certain concerns.

More specifically, HM Treasury has concerns about the proposed reduction of the registration threshold from 25% to 10% for some companies. HM Treasury argued that reducing the threshold would increase both the number of persons on the register and the costs to businesses. It could also create a mismatch of the Person with Significant Control thresholds on the register. The Government is concerned about the requirement to register the beneficial owners of all trusts and trust-like legal arrangements and to make this information widely accessible. It questioned the EC's argument that some trusts operate similarly to companies and should therefore enjoy the same treatment, stating that the private and family-oriented nature of most trusts raises privacy concerns.

Another source of concern for HM Treasury is the proposed introduction of automated centralised mechanisms for the identification of any natural or legal person holding or controlling payment or bank accounts. This would be a significant difference to the current system in the UK where the Financial Intelligence Unit accesses information on bank and payment accounts via credit reference agencies and through established contacts with account providers. The Government takes the view that the requirement to introduce a central data retrieval system is likely to be less onerous than the alternative option of compelling all financial institutions to report data on all bank accounts to a centralised mechanism. There may also be effects on the UK's Credit Rating Agencies.

Regarding the EC Impact Assessment of 7 April 2016 and the detailed EC Impact Assessment of 7 July 2016, the Government claims that they do not provide quantitative estimates of the costs to businesses or individuals of all of the proposals. It is suggested that the discussion of the impact of the measures on pre-paid instruments also lacks detail. HM Treasury is considering whether there are Justice and Home Affairs obligations that would trigger an opt-in.

Following the HM Treasury memorandum and within the timeframe promised by the Government, HM Treasury published its consultation on the implementation of 4MLD.

HM Treasury Consultation

On 15 September 2016, HM Treasury published a consultation paper on the transposition of the 4MLD and the revised Wire Transfer Regulation into UK national law.

The main points raised in the HM Treasury consultation are summarised below:

1. **Scope of the 4MLD**: Key changes include a lower threshold of €10,000 for cash transactions, and extending the scope to both making and receiving

cash payments. There is an option for member states to exempt persons who engage in financial activity on an occasional or very limited basis, if these persons are not money remitters. Currently, HM Treasury applies the exemption to entities of a maximum annual turnover of £64,000. However, it now plans to raise the threshold to £100,000, leaving the single transaction threshold at €1,000.

2. **Customer Due Diligence (CDD) – Simplified CDD (SDD) – Enhanced CDD (EDD)**: HM Treasury proposes the replacement of the existing list of products subject to a simplified CDD, as set out in Article 13 of the Money Laundering Regulations 2007 (**MLRs**), with the non-exhaustive list of factors contained in an Annex to the 4MLD that might seem appropriate for CDD. Respondents are invited to comment on what should trigger the application of CDD measures for existing customers and what are the relevant implications for "obliged entities"– the term which the new provisions will apply to. HM Treasury asks for respondents' views on what the money laundering and terrorist finance risks associated with pooled client accounts would be, whether SDD should be permitted for them and what the effects of removing the ability to use SDD would be. Respondents are invited to comment on whether any products not listed in 4MLD or proposed by the European Supervisory Agencies guidance should be covered by enhanced CDD, and whether any products in other sectors should also be covered.

3. **Reliance:** Respondents are asked whether firms currently rely on third parties for CDD and if so, what are the costs of doing so. HM Treasury has also asked which entities in third countries could potentially be relied upon and for feedback on the meaning of certain 4MLD expressions, such as "member organisation" and "federation".

4. **Assessment of risks and controls:** The paper asks whether there should be a threshold above which firms must appoint a compliance officer, screen employees and have an internal audit function. It also asks what should be taken into account when screening employees. The paper also seeks views on how many of the controls firms are in fact already carrying out, and the likely cost of performing them.

5. **Gambling providers:** 4MLD applies in principle to all gambling providers. This is a significant change from the current requirements, which only apply to the holders of a casino operating licence. The paper explains the CDD measures which gambling providers will need to establish. The paper asks whether any gambling providers or activities should be classified as 'proven' low-risk, and should therefore be exempt.

6. **Electronic money:** 4MLD gives member states the discretion to exempt some low-risk e-money products from parts of CDD. The paper notes that legislative change will be necessary, should the UK decide to use that discretion, and seeks views on the extent to which exemptions should be used.

7. **Estate Agents:** 4MLD extends the coverage of estate agents, for example to include lettings agents. The paper seeks views on the general application of CDD in estate agency business and on supervision of the sector.

8. **Correspondent banking:** The definition of correspondent banking set out in Article 3(8) 4MLD extends the definition provided by the Financial Action Task Force to include relationships between credit and financial institutions. HM Treasury took the view that the correspondent banking requirements under the MLRs are aligned with EDD measures set out in Article 19 of the 4MLD.

No exemptions are offered to member states, and therefore the UK will fully transpose the requirements into UK law. Firms are expected to take a risk-based approach in their activities following the identification of a correspondent relationship, while EDD measures will reflect the risks posed by the relationship and in line with a firm's risk appetite.

9. **Politically Exposed Persons** (**PEPs**): 4MLD makes a significant change in broadening the definition of a PEP to include domestic PEPs (as well as PEPs outside the UK). HM Treasury considers that 4MLD allows firms to take a risk-based approach in order to identify whether a customer is a PEP and appropriately apply EDD measures set out in Article 20 of the 4MLD. HM Treasury states that appropriate industry guidance is required and notes concerns raised over the potential inconsistencies between the Joint Money Laundering Steering Group guidance and FCA's Financial Crime Guide.

10. **Beneficial ownership:** Following the introduction of the beneficial ownership register in UK's People with Significant Control (**PSC**) regime for UK entities, 4MLD introduces the beneficial ownership register for corporates. HM Treasury also plans to introduce a public register of company beneficial ownership for overseas companies who already own or buy property in the UK or who bid on UK central government contracts. HM Treasury will need to define the entities covered by the 4MLD requirement but not caught by the PSC regime.

    The UK Government has already stated it will not share trust beneficial ownership information with private entities or individuals.

11. **Reporting:** HM Treasury recognises that the UK Suspicious Activity Reports regime needs further improvement but states that any changes must meet the stronger 4MLD requirements. It also seeks views on whether it should implement the option to require record retention for an additional five years once the normal retention period has expired.

12. **Supervision:** HM Treasury proposes that all supervisors should be given an express power to refuse to register or to cancel an existing registration under certain circumstances. It enquires about the powers of supervisors and the reasons for which a supervisor may cancel or refuse registration or add conditions to it.

13. **Administrative sanctions:** 4MLD sets out minimum sanctions that member states must impose on obliged entities when they breach the requirements. HM Treasury plans not to set an upper limit on the administrative fines it can impose and seeks views on this, and on whether it should consider additional sanctions and measures.

The consultation will remain open for comments until 10 November 2016. The final policy decisions made by the Government will be implemented through legislation and are expected to come into force by June 2017.

NATIONAL CRIME AGENCY PUBLISHES THE NATIONAL STRATEGIC ASSESSMENT OF SERIOUS AND ORGANISED CRIME 2016

On 9 September 2016, the National Crime Agency (**NCA**) published a National Strategic Assessment of Serious and Organised Crime 2016 (**NSA**). The NCA is a national law enforcement agency with a wide portfolio of responsibility with regard to different types of crime.

In publishing the NSA, the NCA aims to provide an indication of the risk posed to the UK and its interests by serious and organised crime. The NSA indicates the UK's national response to money laundering (**ML**) including the set priorities, the action already taken, the expected result and the means of measuring success. The NCA offers its observations regarding cybercrime, bribery, corruption and sanctions evasion, economic crime, modern slavery and ML.

More specifically, the NCA stated that ML facilitates and enables criminality. ML can potentially cause reputational damage to the UK's economy and threaten national prosperity, resulting in the withdrawal from the UK, or even to the potential collapse, of major financial institutions. ML is therefore, perceived as a national security issue and prioritised in the National Security Strategy. Although relevant numbers are not confirmed, according to the International Monetary Fund, ML globally represents between 2% and 5% of GDP. If these numbers were to be applied to the UK economy, the amount of money laundered would be between £36 billion and £90 billion (although FCA recently said the economic costs to the UK are assessed as being £24 billion).

The NSA defined high-end money laundering as laundering, wittingly or unwittingly, large amount of criminally acquired funds through the UK financial sector and related professional services. It is related to proceeds of major fraud and international corruption. ML may include illicit funds being passed electronically through the banking system and may include use of corporate structures, nominee directors and company formation agents, use of tax havens, virtual offices, investment in high-value goods and property through a network of companies or professional enablers facilitating financial and legal activity. The NSA also defines trade-based money laundering as the movement of the value of criminal funds through the manipulation of aspects of licit or illicit trade transactions, such as third party settlement, over- or undervaluation of goods or falsification of documents.

With regard to cash-based ML, the NCA said that cash still plays a major part in the criminal money-laundering process. Criminal cash may appear as legitimate by means of an investment or movement through cash-based, cash-rich businesses, such as the gambling sector. According to the NSA, a high proportion of cash movements are managed by a few international controllers based in different jurisdictions, mainly in the Middle East and Asia, and supported by networks of collectors and consolidators. In the case of UK criminality, these networks operate in both the UK and mainland Europe. A great variety of professionals, such as accountancy service providers, legal professionals, estate agents and trust and company service providers are used in order to structure complex ML activities and give them an appearance of respectability and legitimacy. NCA underlines the importance of the private sector engagement to identify and disrupt high-end ML schemes, either by targeting individuals, disrupting techniques or target hardening the UK's financial system.

The NSA mentions that cash is likely to remain a major part of the money launderer's activities with most criminality involving moving, storing or using it at some stage. If new payment methods, virtual currencies and mobile payment apps are adopted by money launderers, the risk of ML is likely to increase. The NSA concludes that high-end money laundering is among the top five threats to the UK.

FCA SPEECH BY MEGAN BUTLER ON A MORE EFFECTIVE APPROACH TO COMBATTING FINANCIAL CRIME

On 20 September 2016, Megan Butler, Executive Director of Supervision – Investment, Wholesale and Specialists at the Financial Conduct Authority (**FCA**), delivered a speech on behalf of the FCA at the British Bankers' Association's (**BBA**) Financial Crime and Sanctions Conference. This summary highlights some key points in her speech.

Megan Butler reminded the BBA that everyone has an important role in combatting financial crime. She explained that members of the BBA have a crucial role in supporting policy making and intelligence sharing. Ms Butler referred to the economic cost of financial crime, which was assessed to be £24 billion in the UK, and has been estimated as US$1.6 trillion globally. These figures emphasise the need for the UK financial system to be hostile towards such criminal activities.

Furthermore, Ms Butler explained that there are areas where policy makers could improve and indicated that the FCA have taken the Better Regulation Executive Review on board. She said that the FCA knows that banks have concerns about whether FCA inspections and investigations are sufficiently risk-sensitive. She also indicated that the FCA is aware that it is perceived as sometimes supplying inconsistent advice and lacking flexibility. She said that she hoped to address these perceptions.

Ms Butler indicated that the FCA is committed to a proportionate approach to regulation. She indicated that the FCA's approach to anti-money laundering (**AML**) supervision is risk-based. She explained that risk is sometimes concentrated in smaller firms despite their size and explained, accordingly, that these firms are targeted for visits and AML supervision due to their levels of money laundering risk. She said that the FCA has fined seven banks and one Money Laundering Reporting Officer (**MLRO**) for AML failings. Ms Butler also explained that the FCA does not want the costs of AML compliance to affect the ability of firms to combat financial crime.

She indicated that the FCA is attentive to industry concerns about Suspicious Activity Reports (**SARs**) since SARs are important for information-gathering purposes and should be submitted when appropriate; rather than as part of a 'defensive' strategy that may be used by some MLROs to avoid criminal liability.

Moreover, Ms Butler indicated that the FCA supports and encourages innovation in relation to AML arrangements. For example, she highlighted the FCA's Sandbox scheme which allows firms to test new business models without the risk of regulatory consequences. She said that the FCA is supportive of technological and innovative solutions to problems in this area which maintain market integrity. She encouraged the BBA to share such ideas with the FCA, and indicated that the FCA would not prevent such advancements.

Ms Butler also discussed the role of the banks in combatting financial crime. She recognised that banks have been making progress with regard to AML processes and have become more aware about the damage that financial crime can cause to society. She said that the FCA does not want banks to take a legalistic 'tick box' approach to combatting financial crime and encouraged banks to adopt a sense of social responsibility.

Ms Butler emphasised that de-risking is a problem in the context of financial crime compliance. She highlighted that some charities have been left without banking services and some Politically Exposed Persons have been subjected to probing due diligence questions. She indicated that de-risking and the associated practices may have been caused by the release of the Panama Papers. She also indicated that the FCA wants to encourage better communication between banks and their customers and encourage information sharing between banks.

Ms Butler concluded that the FCA remains committed to working with other firms and regulators in combatting financial crime; especially given its global nature. She said that the FCA "will continue to pursue international solutions to what is an international problem", and she encouraged engagement with the FCA to combat financial crime.

ABI CHECKLIST ON EFFECTIVE COUNTER FRAUD MEASURES

On 22 September 2016, the Association of British Insurers (**ABI**) issued a checklist on effective counter fraud measures.

The aim of this checklist is to assist insurers (especially smaller insurers) with a limited counter fraud function, and also their corporate partners, so they could ultimately establish strong fraud defences. Moreover, the checklist enables firms to contribute to the UK insurance sector's counter fraud strategy, and therefore helps to ensure that the UK remains an attractive business environment.

Even though it is understood by the ABI that insurers might already have their own commercial strategy and risk appetite and accordingly their own fraud controls established, the ABI highlighted the importance of having a unified front. It is considered that, unless all insurers and their partners work towards the same direction, fraud will shift around the market and remain prevalent.

According to the ABI checklist, the insurance industry must meet its regulatory expectations. With financial crime now being one of the Financial Conduct Authority's (**FCA**) top seven risks, the FCA has continued supervisory visits to small firms that may be exposed to a high risk of financial crime. Having documentary evidence that firms have concluded risk assessments and have taken action where necessary will help both commercial decision-making and firms' discussions with the FCA about counter fraud measures.

The checklist includes the following sections:

- Counter fraud strategy: defining scope, establishing risk appetite and setting targets
- Policies and procedures: establishing internal policies and procedures (non-negotiable and mandatory) and cascading these throughout the organisation
- Staff training: training all staff to support the counter fraud strategy
- Board level engagement: in view of the regulatory expectations, establishing good counter fraud governance is vital, with the fraud strategy being set from the top down
- Investigative capability: in-house capability and outsourced solutions
- Enforcement: considering referring cases to enforcement and bringing legal actions
- Engagement with industry bodies: supporting core industry counter fraud initiatives
- Support industry initiatives: supporting industry work to identify scale of fraud and patterns and trends
- Comply with regulatory and industry guidance: ensuring all staff are familiar with and comply with both regulatory rules and guidance
- Customers/ policyholders: taking measures to protect honest customers from insurance fraud as well as actively educating customers/policyholders

HOME OFFICE RESPONSE TO CONSULTATION ON REFORM OF ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING REGIME

On 21 April 2016, the UK Government published its Action Plan for anti-money laundering (**AML**) and counter-terrorist financing (**CTF**), which identified and proposed the steps to address weaknesses revealed by the National Risk Assessment (**NRA**) of Money Laundering and Terrorist Financing of October 2015. The NRA assessed the relevant risks and focused on three priorities: a more robust law enforcement response, reforming the supervisory regime and increasing the UK's international reach. The importance of building a new and powerful partnership with the private sector was also highlighted by the NRA, in order to improve suspicious activity reporting, deliver deeper information-sharing and enable the relentless disruption of criminals and terrorists. The Government ran a consultation from April to June 2016 and received 52 responses. The consultation did not cover the supervisory regime, as that was subject to a separate consultation by HM Treasury.

On 13 October 2016, the Home Office published its response to the above consultation regarding the reform of the AML/CTF regime. The response makes various proposals, the most important of which are summarised below:

1. Initiation of a Suspicious Activity Reports (**SARs**) reform program, including IT and process improvements and introducing immediate legislative changes to:
   - allocate the power to the National Crime Agency to obtain further information from a regulated business following receipt of a SAR, following a recommendation from the FAFT; and
   - extend the investigative period where senior officers from law enforcement agencies can prevent a transaction from going ahead, while they gather evidence needed for a law enforcement intervention. The Criminal Finances Bill 2016 will amend the Proceeds of Crime Act 2002 (**POCA**) to extend the moratorium period by a court, at the request of the senior officer, for periods of up to 31 days, up to a total of 186 days.
2. Introduction of Unexplained Wealth Orders (**UWO**) requiring an individual to explain the origin of assets that appear to be disproportionate to known income. An UWO would be made by the court and in a case where the respondent refuses to comply without providing an explanation, the court can presume that the property in question is "recoverable property" under the existing civil recovery powers in POCA. The UWO will be subject to the relevant property being aggregated to a minimum value threshold and there being reasonable grounds to suspect that known income is insufficient to obtain the property. The UWO will be available either against any person that law enforcement agencies have reasonable grounds to suspect has links to serious crime, or WWagainst overseas politically exposed persons.
3. Establishment of a new information sharing gateway introduced through the Criminal Finances Bill for the exchange of data on suspicion of terrorist financing and money laundering between private sector firms with immunity from civil liability. Firms in the regulated sector will be able to share information on suspicions on money laundering and terrorist financing with one another, under the legal 'safe harbour' of immunity from criminal or civil liability. The new powers will also enable the submission of joint SARs, so that firms can provide the whole picture of a money laundering scheme that crosses multiple firms, rather than submitting individual pieces of the jigsaw to the UK Financial Intelligence Unit.

4. Introduction of new powers to enable the more effective seizure and forfeiture of criminal proceeds held in bank accounts without the need to secure a conviction. Concern has been expressed that the existing civil recovery powers are too narrow and the £10,000 de minimus threshold is too high.
5. Power to enable the seizure and forfeiture of portable high value items used to store and move the proceeds of crime.

The Government has decided to remove the consent regime, but will keep the issue under review while the SARs reform programme develops. The Government also decided against the introduction of an illicit enrichment offence.

FCA IMPOSES PENALTIES ON SONALI BANK (UK) AND ITS FORMER MONEY LAUNDERING REPORTING OFFICER FOR SERIOUS ANTI-MONEY LAUNDERING SYSTEMS FAILINGS

On 12 October 2016, the Financial Conduct Authority (**FCA**) fined Sonali Bank (UK) Limited (**SBUK**) £3,250,600 under section 206 of the Financial Services and Markets Act 2000 (**FSMA**). With regard to SBUK's regulated activities, the FCA under section 206A FSMA also restricted it from accepting deposits from new customers for 168 days.

The FCA found that between 20 August 2010 to 21 July 2014, despite the clear warnings provided, SBUK suffered serious failings relating to its anti-money laundering (**AML**) governance and control systems. More specifically, SBUK was found in breach of FCA Principle 3 (taking reasonable steps to organise its affairs responsibly and effectively, with adequate risk management systems) of the FCA Principles for Businesses by having serious and systemic weaknesses in its AML controls. The FCA found that the weaknesses affected almost all levels of SBUK's business and governance structure, including the senior management team, money laundering reporting officer (**MLRO**) function, oversight of its branches and policies and procedures relating to AML. SBUK failed to comply with its operational obligations in respect of customer due diligence, the identification and treatment of politically exposed persons, transaction and customer monitoring and making suspicious activity reports. Moreover, while SBUK was being investigated by the FCA, it was found to be in breach of FCA Principle 11 (dealing with regulators in an open and cooperative way) by failing to notify the FCA for at least seven weeks that a potentially significant fraud had occurred.

Under section 66 FSMA, the FCA also fined the bank's former MLRO, Steven Smith, the sum of £17,900 and prohibited him from performing the MLRO or compliance oversight functions at regulated firms. Mr Smith was found by the FCA to be in breach of FCA Principle 6 (due skill, care and diligence in managing the business) of the FCA's Approved Persons and was knowingly concerned in the bank's breach of FCA Principle 3. Despite the warnings from the bank's internal auditors, Mr Smith reassured the bank's board and senior management that controls were working effectively.

Steven Smith also failed to:

- put in place appropriate AML monitoring arrangements;
- identify serious weaknesses in operational controls and a lack of appropriate knowledge among staff;
- report appropriately concerns from internal auditors and the results of internal testing; and
- impress upon senior management the need for more resources in the MLRO function.

Even though the FCA recognised that Mr Smith did not have sufficient senior management support and was overlooked, it considered that his failings were serious enough in their own right.

Both SBUK and Mr Smith agreed to settle at an early stage of the investigation and thus qualified for a 30% (stage 1) discount on their fines.

INTERNATIONAL NEWS & ENFORCEMENT ACTION

NEW PRESIDENT OF THE FINANCIAL ACTION TASK FORCE OUTLINES OBJECTIVES FOR 2016/17

On 10 June 2016, Mr Juan Manuel Vega-Serrano, the President of the Financial Action Task Force (**FATF**), published a paper on behalf of the organisation which outlined the objectives of FATF and the priorities of the Spanish presidency of FATF during 2016/17.

Mr Vega-Serrano explained that combatting terrorist financing is of critical importance to preserving the integrity of the international financial system; stating that it is FATF's top priority. Mr Vega-Serrano also said that closer collaboration is needed between international bodies and that a consolidated strategy should be implemented to tackle terrorist financing. Furthermore, he also explained that there is a need to assess the progress that countries are making in combatting terrorist financing, and to outline any additional measures that they may be required to implement.

FATF also plans to prioritise improving transparency through the implementation of beneficial ownership requirements. Mr Vega-Serrano explained that FATF intends to inform and advise international bodies with regard to FATF standards on beneficial ownership.

Mr Vega-Serrano also indicated that FATF plans to develop a 'new partnership' with the FinTech and RegTech communities. He indicated that the aim of these relationships was to support innovation whilst maintaining transparency and mitigating risk. He also explained that FATF will be proactive in developing standards and providing guidance on best practice with regard to new innovations; rather than responding to such developments after issues arise.

Mr Vega-Serrano also explained that FATF will focus on assessing and promoting the effective implementation of FATF standards in the jurisdictions within their global network. He indicated that FATF intends to use these standards to combat financial crime. Mr Vega-Serrano also explained that FATF will enhance its operational focus through greater collaboration and will provide operational benefits, such as financial intelligence units. He explained that FATF intends to develop a joint task force approach with experts from the private sector, non-governmental organisations, academia and civil society. He also explained that FATF will seek to enhance its international standing by becoming more involved in international discussions, such as those held by the G20.

He concluded that the implementation of these strategic priorities will enable FATF to continue leading global efforts to combat money laundering and terrorist financing.

EUROPEAN COMMISSION LEGISLATIVE PROPOSAL FOR DIRECTIVE AMENDING FOURTH MONEY LAUNDERING DIRECTIVE

The Fourth Money Laundering Directive (**4MLD**) was adopted on 20 May 2015 in order to improve the effectiveness of the European Union's (**EU**) efforts to combat the laundering of money from criminal activities and to counter the financing of terrorist activities. On 5 July 2016, the European Commission (**EC**) published its legislative proposal to amend the 4MLD on the basis of Articles 114 and 50 of the Treaty on the Functioning of the EU. The proposal comes as a response to the terror attacks in Europe and the leak of the Panama Papers.

The EC proposals have a twofold aim: to strengthen oversight over the financial instruments used by terrorists such as cash, trade in cultural artefacts, virtual currencies and anonymous pre-paid cards; and to prevent the large-scale concealment of funds in offshore jurisdictions and enhance corporate transparency. The proposals are consistent with global developments, such as the United Nations Security Council Resolutions 2199 (2015) and 2253 (2015), and the G20 statement of 18 April 2016, which both call for further action against money laundering (**ML**) and terrorist financing (**TF**).

The key amendments proposed by the EC are listed below:

1. Inclusion of virtual currency exchange platforms within the scope of the 4MLD as obliged entities

The EC proposes an amendment of article 2 of the 4MLD, which defines the obliged entities that fall within the scope of the Directive. The EC proposes the inclusion of virtual currency exchange platforms and custodian wallet providers. It also provides a definition of the term "virtual currency". Despite the risks attached, virtual currency transfers are not currently monitored by public authorities within the EU.

2. Reduction of the maximum transaction limits for certain pre-paid instruments

Under article 12 of the 4MLD, in some member states obliged entities are not obliged to apply certain customer due diligence (**CDD**) measures with respect to electronic money, provided certain conditions are met. However, considering the terrorism financing risks attached to pre-paid cards, the EC proposes to (i) lower the thresholds (from €250 to €150) in respect of non-reloadable pre-paid payment services instruments to which such CDD measures apply and (ii) suppress the CDD exemption for online use of prepaid cards. The EC proposals are in line with rules already laid down by the 4MLD for pre-paid cards and would not require additional obligations on behalf of the distributors of these instruments.

3. Ability for the Financial Intelligence Units to request information on ML and TF from any obliged entity

The EC proposes the amendment of article 32 of the 4MLD in order for it to be in line with the latest international standards and to facilitate Financial Intelligence Units (**FIUs**) cooperation. According to the proposal, FIUs should be able to obtain additional information from obliged entities and to have access on a timely basis to their financial, administrative and law enforcement information. This will help FIUs to undertake their functions properly, even without a previously submitted suspicious transaction report. Under the current regime, the information available to FIUs is limited in some member states by the requirement that a prior suspicious transaction report has been made by an obliged entity.

4. Greater access to information on the holders of bank and payment accounts for the FIUs

The EC proposed the amendment of article 57 of the 4MLD, requiring member states to set up automated centralised mechanisms, which will allow the identification

of holders of bank and payment accounts. Member states will be able to set up either a central registry or other centralised mechanisms, such as data retrieval systems. The proposal would allow for faster detection, both nationally and internationally, of suspicious ML and TF transactions.

5. Enhancement and harmonisation of due diligence measures for high-risk third countries

Member states are not currently required to include a specific list of enhanced consumer due diligence (**ECDD**) measures in their national regimes. Consequently, there are many differences among the member states' approaches, as well as deficiencies. The EC proposes the harmonisation of ECDD measures in compliance with the relevant FATF lists. The harmonisation will limit or even eliminate the risk of forum-shopping and address the regulatory gaps.

6. Facilitated access to beneficial ownership information

In the aftermath of the Panama Papers leak, the EC aims to address regulatory gaps and improve the transparency of beneficial ownership information. More specifically, the EC proposed to grant public access to beneficial ownership information for both companies and trusts engaged in commercial or business-like activities by amending the 1st Company Law Directive. The EC also proposed allowing access to such information on a 'legitimate-interest' basis for family or charitable trusts. The EC proposed clarifying that, with regards to trusts, the member state responsible to ensure registration is the one where the trust is administered.

7. Interconnection of national central registers

The EC will issue a report by June 2019 assessing the conditions, technical specifications and procedures for ensuring the interconnection. The interconnection will allow competent authorities, FIUs and obliged entities to identify the beneficial owners in an easy and efficient way and will increase the transparency requirements on companies and trusts. It will also allow the public to access the beneficial ownership information across the EU.

8. Additional technical clarifications

The EC proposes certain clarifications with regard to competent authorities under 4MLD, the exclusion of closed loop cards and full consistency with provisions on electronic identification.

The transposition deadline for the original 4MLD is 26 June 2017, but the EC has proposed expediting this to 1 January 2017 for both the original 4MLD and its amendments.

EBA PUBLISHES OPINION ON THE EUROPEAN COMMISSION'S PROPOSAL TO BRING VIRTUAL CURRENCIES INTO THE SCOPE OF THE FOURTH MONEY LAUNDERING DIRECTIVE

On 11 August 2016, the European Banking Authority (**EBA**) published its opinion on the European Commission's (**EC**) proposal to bring virtual currencies into the scope of the Fourth EU Money Laundering Directive (Directive (EU) 2015/849) (**4MLD**) which was published on 5 July 2016.

The EC proposed various amendments to the 4MLD, including a proposal to bring custodian wallet providers (**CWPs**) and virtual currency exchange platforms (**VCEPs**) within the scope of 4MLD. The EBA explained that this would require CWPs and VCEPs to have policies and procedures which detect, prevent and report money laundering and terrorist financing. The EBA stated that the EC proposed to subject CWPs and VCEPs to registration or licensing requirements and impose fit and proper testing on the owners and managers of such entities.

The EBA has indicated that it supports the EC's proposals and described them as an important step towards mitigating the risks of financial crime associated with the use of virtual currencies. However, it explained that the EC and legislators need to put effective supervision in place to ensure that CWPs and VCEPs comply with their anti-money laundering (**AML**) and counter terrorist financing (**CTF**) obligations. Moreover, the EBA indicated that supervision must be consistent throughout the European Union (**EU**) because of the transnational nature of virtual currencies. Taking into account these views, the EBA set out seven proposals for the EC and legislators to consider when finalising the amendments to the 4MLD.

The first proposal put forward by the EBA was that the transposition deadline for the amendments to 4MLD should be set in a way that facilitates the adoption of a consistent approach to AML/CTF supervision of CWPs and VCEPs across the EU. The EC has proposed that the deadline to transpose the 4MLD and its proposed amendments is brought forward to 1 January 2017. The EBA argued that the deadline for the transposition of the new amendments should not be changed and, accordingly, that 26 June 2017 should continue to be the deadline. The EBA put forward this proposition in order to give member states, competent authorities, VCEPs and CWPs time to implement the new amendments, taking into account that an AML/CTF regime for VCEPs and CWPs does not yet exist.

The EBA's second proposal was that virtual currency transactions should remain outside the scope of the Payment Services Directive (Directive (EU) 2015/2366) (**PSD II**). The EBA indicated that it agreed with the EC's decision not to bring virtual currency transactions within the scope of Directives, such as the PSD II. The EBA agreed with the EC on this point because it does not think that the PSD II would be suitable for mitigating all of the risks associated with virtual currency transactions. Instead, the EBA argued that a separate regulatory regime, or substantial amendments to the PSD II, would be required in order to mitigate such risks.

The third proposal advocated by the EBA was that the status of CWPs and VCEPs should be clarified. The EBA highlighted that there is a lack of awareness of the meaning of the EC's proposed amendments. It explained that some VCEPs and CWPs refer to themselves as 'regulated' or 'authorised'; thereby giving the impression that certain regulatory safeguards are in place when this is not the case. Accordingly, the EBA proposed that the EC and other legislators inform the public about what the amendments to 4MLD mean in order to clarify the status of CWPs and VCEPs in the short term. The EBA said that virtual currencies should be subjected to a comprehensive framework in the long run.

The EBA's fourth proposal was that the amendments to 4MLD should enable competent authorities to exchange information easily regarding VCEPs and CWPs. The EBA

explained that the exchange of information between supervising authorities can sometimes be prevented due to 'legal obstacles'. On this basis, the EBA said that the EC should consider amending section 3 of 4MLD in order to ensure that information can be exchanged more easily between authorities responsible for the AML/CTF supervision of VCEPs and CWPs.

As its fifth proposal, the EBA also suggested that the amendments to 4MLD should provide more detail on how competent authorities should carry out fit and proper tests of owners and managers of VCEPs and CWPs. The EBA said that 4MLD does not specify what makes those who hold a management function in or the owners of VCEPs and CWPS fit and proper persons. Given that VCEPs and CWPs present a significant AML/CTF risk, the EBA proposed that more detail is provided to supervising authorities to ensure that enforcement is carried out consistently across the EU. The EBA also explained that this proposal should be considered because VCEPs and CWPs are new concepts and therefore present challenges for supervisory authorities. The EBA explained that the required detail could be provided in the amendments to 4MLD.

The EBA's sixth proposal was that the amendments to 4MLD should clarify the scope of the proposed licensing/registration regime suggested by the EC for VCEPs and CWPs. The EBA explained that 4MLD provides a choice between a licencing and registration regime. Accordingly, it is likely that different member states will choose different regimes. On this basis, the EBA proposed that the EC and legislators consider whether a licencing or registering regime would be most suitable for deterring terrorist financing in the EU. Failing that, the EBA said that clarity should be provided regarding the features that each regime should have.

The final proposal put forward by the EBA was that the proposed extension of national sanction powers to VCEPs and CWPs should be retained. The EBA explained that the basis of this proposal is to ensure that VCEPs and CWPs comply with the requirements by giving supervisory authorities dissuasive sanctioning powers for VCEPs and CWPs for failing to comply with requirements of 4MLD. The EBA identified that this included the reporting of suspicious transactions.

CPMI FINAL REPORT ON CORRESPONDENT BANKING

On 13 July 2016, the Committee on Payments and Market Infrastructures (**CPMI**) issued the final version of its report on correspondent banking. The CPMI had consulted on a draft of the report in October 2015. The changes made to the final report, which are influenced by the public comments received and the interactions with stakeholders, are intended to strengthen the analysis and sharpen the message and recommendations of CPMI.

Correspondent banking is used by banks to access financial services in different jurisdictions and provide cross-border payment services to their customers. However, the report states that correspondent banking relationships recently seem to be under threat. The impact of correspondent banking trends is uneven across jurisdictions and banks, while according to a qualitative analysis using SWIFT transaction data, there seems to be a trend towards concentration in correspondent banking activities. Some of the main reasons for cutting back on correspondent banking relationships are the rising costs and the uncertainty regarding the appropriate extent of customer due diligence (**CDD**), including 'know-your-customers' customers' (**KYCC**) obligation. The regulatory framework is assumed in the CPMI report, and the focus falls on measures that could improve the efficiency of procedures, reduce compliance costs and help address perceived uncertainty. The CPMI does not aim to alter the applicable rules and basic channels for correspondent banking services between correspondent and respondent banks.

The main CPMI recommendations are outlined below:

1. Use of "know your customer" (KYC) utilities

The CPMI recognises that KYC utilities by respondent and correspondent banking, provided they store at least a minimum set of up-to-date and accurate information, could be used as an effective means of reducing the burden of compliance with CDD requirements for banks engaging in the correspondent banking business.
The CPMI therefore invites relevant standard setters, such as the International Organisation for Standardisation, to define a standardised minimum set of information and data (including the format) that all utilities should collect and that all banks have to be ready to provide to other banks when information and data are required. Moreover, the CPMI invites the Financial Action Task Force (**FATF**) and the Basel Committee on Banking Supervisions AML/CTF Group (**AMLEG**), which have responsibility for anti-money laundering and counter-terrorist financing, to develop a set of issues that financial institutions should consider when using KYC utilities.

2. Use of the Legal Entity Identifiers (LEI) in correspondent banking

All authorities and relevant stakeholders are invited to promote Business Identifier Code-to-LEI mapping facilities, in order to allow for an easy mapping of routing information available in the payment message to the relevant LEI. Moreover, relevant authorities are encouraged to further elaborate as to what extent the banks can rely on the LEI as a means of accessing reliable information to support customer due diligence in correspondent banking.

3. Information-sharing initiatives

The FATF and the AMLEG are invited to provide additional clarity on CDD recommendations for upstream banks and further explore ways to tackle obstacles to information-sharing in order to identify potential best practices. Following the FATF recommendation, the CPMI suggests that information-sharing mechanisms for KYCC could be promoted as the first source of information by default which, if needed, could be complemented bilaterally with enhanced information.

4. Payment messages

The CPMI recommends that individual banks decide which method should be used, i.e. serial Message Type (**MT**) 103 method and the cover MT 202 CV method, in compliance with Anti-Money Laundering/Counter-Terrorist Financing and relevant regulatory requirements, when all data fields are accurately populated in a payment message. The CPMI invites the stakeholders to revisit their principles governing the use-cases for payment messages, and accordingly, review what information should be included and which data fields should be used. AMLEG is also invited to develop further guidance on the supervisors' roles in ensuring that banks meet FATF Recommendations and guidance on the quality of the payment message content.

5. Use of the LEI as additional information in payment services

The CPMI recommends that stakeholders start analysing how the LEI could be used on an optional basis and in a more structured way within the current relevant MT messages. It also suggests that stakeholders work on defining a common market practice in order to enable the inclusion of the LEI in the current relevant payment messages without changing the current message structure. Relevant stakeholders are also encouraged to consider developing dedicated codes or data items for the inclusion of the LEI in these payment messages.

The CPMI recognises that the recommendations will not in isolation resolve all of the issues raised. However, they might address some of the costs and concerns connected to correspondent banking activities. According to the CPMI, the recommendations need to be further analysed by all relevant authorities and stakeholders, in order to evaluate the potential impact of each measure and avoid unintended consequences.

The CPMI welcomes the review or investigation of the recommendations by the relevant stakeholders.
The CPMI also stated it would facilitate the implementation of payment systems from a technical perspective by contributing to the work or work streams of relevant stakeholders.

EU DELEGATED REGULATION IDENTIFYING HIGH RISK THIRD COUNTRIES UNDER FOURTH MONEY LAUNDERING DIRECTIVE

On 20 September 2016, the European Commission Delegated Regulation (EU) 2016/1675 supplementing the Fourth Money Laundering Directive ((EU) 2015/849) (**4MLD**) was published in the Official Journal of the European Union (**EU**).

The EU aims to ensure efficient protection mechanisms for the internal market and to increase legal certainty for economic operators and stakeholders in their relationships with third-country jurisdictions. According to the Delegated Regulation, some jurisdictions have in place deficient legal and institutional frameworks with poor standards for controlling money flows. These deficiencies threaten the financial system of the EU. All EU obliged entities the 4MLD should therefore apply enhanced due diligence measures in their relationship to natural persons or legal entities established in high-risk third countries in order to ensure equivalent requirements for market participants across the EU.

The Regulation identified high-risk third countries with strategic anti-money laundering (**AML**) and counter-terrorist financing (**CTF**) deficiencies. The identification was based on an assessment of the compliance with the criteria laid down in the 4MLD regarding its legal and institutional AML and CTF framework, the powers and procedures of its competent authorities and the effectiveness of the AML and CTF system.

According to the European Commission's analysis:

- Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao PDR, Syria, Uganda, Vanuatu and Yemen are high-risk third countries that have strategic deficiencies in their AML and CTF regimes. They have provided a written high-level political commitment to address the identified issues and accordingly develop an action plan with the Financial Action Task Force (**FATF**).
- Iran is a high-risk third country that has strategic deficiencies in its AML and CTF regimes. Iran has provided a high-level political commitment to address the identified deficiencies and has decided to seek technical assistance in the implementation of the FATF Action Plan.
- The Democratic People's Republic of Korea (**DPRK**) is a high-risk third country that has strategic deficiencies in its AML and CTF regime. This country identified by a FAFT Public Statement presents ongoing and substantial money-laundering and terrorist financing regimes.

The European Commission will permanently monitor the developments in the assessment of legal and institutional frameworks in place in third countries, the powers and procedures of competent authorities and the effectiveness of their AML and CTF regimes, in order to keep the list of high-risk third countries with strategic deficiencies up to date.

KEY CONTACTS

FOR FURTHER INFORMATION OR ADVICE, PLEASE CONTACT:

For further information or advice, please contact:

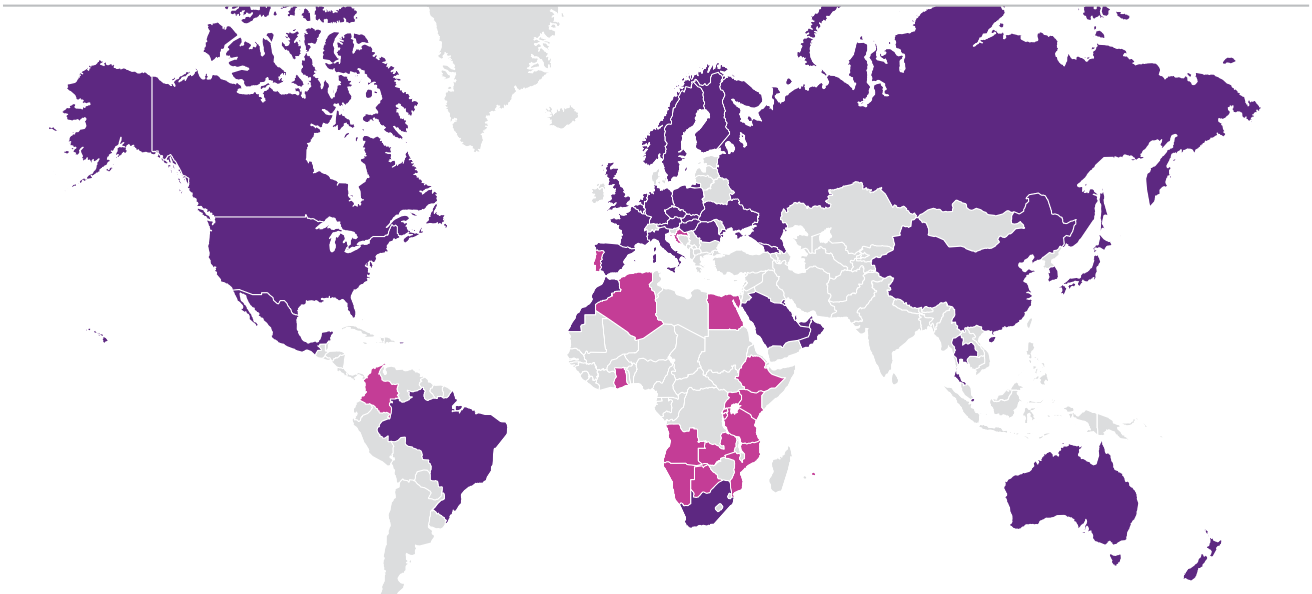
Michael McKee
Head of Financial Services Regulatory, Partner
T +44 (0)20 7153 7468
michael.mckee@dlapiper.com

Tony Katz
Head of Financial Services and Investigations, Partner
T +44 (0)20 7153 7835
tony.katz@dlapiper.com

Sam Millar
Partner
T +44 (0)20 7153 7714
sam.millar@dlapiper.com

Ian Mason
Legal Director
T +44 (0)20 7153 7464
ian.mason@dlapiper.com

OUR GLOBAL FOOTPRINT



DLA PIPER

AUSTRALIA
Brisbane
Canberra
Melbourne
Perth
Sydney

AUSTRIA
Vienna

BAHRAIN
Manama

BELGIUM
Antwerp
Brussels

BRAZIL
São Paulo

CANADA
Calgary
Edmonton
Montreal
Toronto
Vancouver
Yellowknife

CHINA
Beijing
Hong Kong
Shanghai

CZECH REPUBLIC
Prague

FINLAND
Helsinki

FRANCE
Paris

GEORGIA
Tbilisi

GERMANY
Berlin
Cologne
Frankfurt
Hamburg
Munich

HUNGARY
Budapest

ITALY
Milan
Rome

JAPAN
Tokyo

KUWAIT
Kuwait City

LUXEMBOURG
Luxembourg

MEXICO
Mexico City

MOROCCO
Casablanca

NORWAY
Oslo

NETHERLANDS
Amsterdam

NEW ZEALAND
Auckland
Wellington

OMAN
Muscat

POLAND
Warsaw

QATAR
Doha

ROMANIA
Bucharest

RUSSIA
Moscow
St. Petersburg

SAUDI ARABIA
Al Khobar
Jeddah
Riyadh

SINGAPORE
Singapore

SLOVAK REPUBLIC
Bratislava

SOUTH AFRICA
Johannesburg

SOUTH KOREA
Seoul

SPAIN
Madrid

SWEDEN
Stockholm

THAILAND
Bangkok

UKRAINE
Kyiv

UNITED ARAB EMIRATES
Abu Dhabi
Dubai

UNITED KINGDOM
Birmingham
Edinburgh
Leeds
Liverpool
London
Manchester
Sheffield

UNITED STATES
Albany
Atlanta
Atlantic City
Austin
Baltimore
Boston
Chicago
Dallas
Houston
Los Angeles
Miami
Minneapolis
New York
Northern Virginia
Philadelphia
Phoenix
Raleigh
Sacramento
San Diego
San Francisco
San Juan
Seattle
Short Hills
Silicon Valley
Washington, DC
Wilmington

RELATIONSHIP FIRMS

ALGERIA
Algiers

ANGOLA
Luanda

BOTSWANA
Gaborone

BURUNDI
Bujumbura

COLOMBIA
Bogota

CROATIA
Zagreb

EGYPT
Cairo

ETHIOPIA
Addis Ababa

GHANA
Accra

KENYA
Nairobi

MAURITIUS
Port Louis

MOZAMBIQUE
Maputo

NAMIBIA
Windhoek

PORTUGAL
Lisbon

RWANDA
Kigali

TANZANIA
Dar es Salaam
Mwanza

UGANDA
Kampala

ZAMBIA
Lusaka

COOPERATION FIRM

BRAZIL
Rio de Janeiro
São Paulo