SPRING 2015

AML BULLETIN

Regulatory News Update from DLA Piper

CONTENTS

Introduction

DLA Piper's Financial Services Regulatory team welcomes you to the Spring 2015 edition of our Anti-Money Laundering (AML) Bulletin.

In this issue we provide updates on AML news and enforcement action, both in the UK and internationally, including a report on Commerzbank AG's US$1.45 billion settlement with US authorities for AML and sanctions breaches committed through its New York branch and the US$8.4 million fine imposed by the Dubai Financial Services Authority (the largest fine in its ten-year history) on Deutsche Bank AG for a number of breaches including a failure to comply with AML requirements in respect of certain clients.

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 the bulletin.

UK NEWS & ENFORCEMENT ACTION

HMRC RELEASES AML AND CTF SUPERVISION REPORT 2013 – 2014

On 25 March 2015, HM Treasury, which is responsible for appointing anti-money laundering (**AML**) and counter terrorist finance (**CTF**) supervisors in the UK (**Supervisors**) (e.g. the Financial Conduct Authority (**FCA**) and HMRC), released its fourth supervision report for the 2013 – 2014 period (**Report**). A supervision report is prepared annually by HM Treasury, working with the Supervisors, in order to provide transparency of the UK's approach to supervision and promote good practice. The key points of the Report are set out below.

Disproportionate Implementation of AML Requirements in the Banking Sector

HM Treasury raises a concern that there may be a degree of over-implementation of legal and regulatory requirements in the banking sector, stating that the FCA and other supervisors should ensure that firms take a proportionate and effective approach in preventing money laundering and terrorist financing, but should not prevent access to banking by legitimate customers.

Implementation of New FATF Methodology

New methodology was published by the Financial Action Task Force (**FATF**) in 2013, which focusses on ensuring countries' systems and controls in relation to AML and CTF are effective and achieve positive results, rather than merely comply technically with FATF standards. HM Treasury met with all UK supervisors in 2014 to discuss the new FATF methodology. HM Treasury reports that all Supervisors have developed or are developing an action plan to set out steps they propose to take in light of the new FATF methodology.

Adoption of a Risk-Based Approach

Both Supervisors and their member firms are required to adopt a risk-based approach in complying with their AML obligations. This requires them to identify, assess and understand the relevant risks and take proportionate steps to mitigate these risks effectively. The Report states that while a number of Supervisors devote time and resources to implementing this approach, a number of Supervisors were still transitioning to a more risk-based approach in the 2013 – 2014 period. HM Treasury notes in the Report that while many Supervisors understood the risks facing their sector, most of these Supervisors did not demonstrate how their risk assessments translated into specific monitoring actions being taken.

Monitoring Activity

The Report sets out an analysis of the measures taken to monitor firms by Supervisors. These measures include analysis of annual returns, so that Supervisors can keep up-to-date with firms' activities allowing them to re-consider their risk assessments and compliance activities in relation to firms, on-site compliance visits, desk-based reviews and telephone interviews. A number of Supervisors were unable to report on the outcomes of all compliance visits and desk-based reviews undertaken. This was criticised in the Report on the basis that in order to demonstrate that such supervisory work is effective, such outcomes should be available and capable of analysis.

Enforcement Action

The Report summarises enforcement action taken by Supervisors in the 2013 – 2014 period. There had been a significant increase in enforcement activity taken by

Supervisors in 2013 – 2014 compared to 2012 – 2013 across all sectors. In particular, the legal and accountancy sectors saw an increase in the use of every enforcement method compared to the previous reporting period. HM Treasury states that Supervisors should ensure that they do not take enforcement action too excessively as there is a risk of causing firms to over comply with requirements. Supervisors should be able to link enforcement action taken with resulting compliance outcomes.

Advice

Supervisors provide formal guidance on AML regulatory requirements, which is approved by HM Treasury. A significant number of Supervisors also publish AML information on their websites, hold training events and operate a helpline for supervised firms to raise specific queries.

Information Sharing between Supervisors

HM Treasury acknowledges that an effective AML regime requires Supervisors to communicate and share information with one another, including information on how best to identify and mitigate risks that are common to a number of Supervisors. A number of fora exist to facilitate exchange of such information. The AML Supervisors forum is attended by Supervisors, HM Treasury, the Home Office and the National Crime Agency. In additional, the Money Laundering Advisory Committee, which is jointly chaired by HM Treasury and the Home Office, exists to allow industry, law enforcement, Supervisors and government to advise on the UK AML regime.

HM TREASURY HIGH RISK MONEY LAUNDERING LIST UPDATED

HM Treasury has issued an advisory notice informing firms that it has updated its list of countries that are considered to pose a high risk in respect of AML compliance. This follows the publication of two statements by FATF on 27 February 2015, which identify countries with strategic deficiencies in their AML and CTF regimes.

In the notice, HM Treasury advises firms to treat Algeria, DPRK (North Korea), Ecuador, Iran and Myanmar as high risk for the purposes of the Money Laundering Regulations 2007 and apply enhanced due diligence measures in respect of matters involving these jurisdictions.

In relation to Afghanistan, Angola, Guyana, Indonesia, Iraq, Laos , Panama, Papua New Guinea, Sudan, Syria, Uganda and Yemen, HM Treasury advises firms to take appropriate actions to minimise the associated risks, which may include enhanced due diligence measures in high risk situations.

FCA THEMATIC REVIEW INTO AML AND SANCTIONS COMPLIANCE IN SMALL BANKS

On 14 November 2014, the FCA published a thematic review: *TR14/16: How small banks manage money laundering and sanctions risk* (**Review**).

The Review follows a previous review conducted between 2010 and 2011 (**2011 Review**) by the Financial Services Authority (**FSA**) into 27 banks in order to assess their AML systems and controls in high-risk situations. Following the findings of the 2011 review, the FCA took enforcement action against five banks for failing to manage money laundering risks appropriately. In January 2015, the FCA also published new guidance: *Financial Crime: a guide for firms*.

The objective of the current FCA Review was to determine the extent to which the FCA's previous actions have affected the quality of AML and sanctions controls in smaller banks. The review focussed primarily on high-risk customers, politically exposed persons (**PEPs**) and correspondent banks. As part of the Review, the FCA visited 21 banks (eight private banks, seven wholesale banks and six retail banks) between October 2013 and June 2014. The FCA gave consideration as to how these banks had used the FCA's regulatory guidance, the 2011 Review and enforcement in relation to AML and sanctions controls.

The FCA found that some of the banks had effective AML and sanctions controls. On the whole, the private banks generally operated to higher standards than the wholesale and retail banks. In these banks there was good senior management involvement on AML, employees had a good understanding of financial crime risk, there was a good degree of oversight of high-risk customer relationships and an effective use of enhanced client due diligence.

However, on the whole, the FCA found that most banks had weaknesses in their AML systems, as summarised below.

- There were widespread weaknesses in key AML controls including (i) AML risk assessments, and (ii) enhanced client due diligence and ongoing monitoring in respect of high-risk, PEP and correspondent relationships.
- One-third of the banks reviewed had inadequate AML resources. Staff knowledge of AML and sanctions risks was often weak, including amongst Money Laundering Reporting Officers.
- Certain overseas banks' customer due diligence procedures were inadequate. These banks' group-wide policies and procedures were not always consistent with UK legal and regulatory requirements.

In the Review, the FCA states that it noticed a general improvement in senior management engagement on AML issues compared to the 2011 Review. However, banks were generally slow to assess their systems against FCA guidance and had often only made such assessments following FCA enforcement action against other similar banks.

The FCA found particularly serious problems with six of the 21 banks. Three of these banks have been required to appoint a skilled person under section 166 of the Financial Services and Markets Act 2000 to conduct a more detailed review of their AML and sanctions controls. The FCA has also commenced enforcement investigations into two of the six banks.

FOUR MEN JAILED FOR A TOTAL OF 21 YEARS FOR MONEY LAUNDERING

On 16 March 2015, four men were sentenced to a total of over 21 years at the Old Bailey for their involvement in laundering millions of pounds' worth of criminal assets. The convictions followed an investigation by the City of London police.

Abdullah Rahim (34) from Lewisham, London, pleaded guilty to laundering just under £20.7 million of criminal money across an eight-month period and was sentenced to six and a half years' imprisonment. Zaka Din (34) from Norbury, London, and Brian Mcinerney (53) and Iftekar Choudhary (30) both from Islington, London, each pleaded guilty to conspiracy to launder criminal funds and were sentenced to eight years', fourteen months' and five and a half years' imprisonment respectively.

The gang had been involved in numerous illegal transactions of large sums of money. Thousands of transactions were faked using a travel agent business owned by Din based in Norbury and a money transfer business owned by Rahim located in Whitechapel, London.

Din had been arrested on 2 September 2014, having been identified as using his travel agency business as a cover for arranging cash exchanges from the UK to foreign destinations on the instructions of criminal groups seeking to launder their proceeds.

Choudhary, Mcinerney and Rahim were subsequently arrested on 11 September 2014. When arrested, Choudhary and Mcinerney were still in possession of £35,000 cash that Choudhary had collected from Mcinerney in order to pass on to Rahim. The intention was for Rahim to arrange for the money to be transferred to Dubai and then to other jurisdictions. When Rahim was arrested in his home in Lewisham, a laptop was found containing Excel spreadsheets which documented the illegal movement of almost £20.7 million.

Din and Rahim are now expected to be subject to confiscation orders.

INTERNATIONAL NEWS & ENFORCEMENT ACTION

COMMERZBANK FINED US$1.45 BILLION FOR AML AND SANCTIONS FAILINGS

Commerzbank AG (**Commerzbank**) has agreed to pay various United States authorities US$1.45 billion and to take a number of remedial actions, including the dismissal of four employees, after a large number of sanctions and AML regulation violations. A summary of Commerzbank's breaches and the penalties imposed on Commerzbank is set out below. The facts are set out in more detail in a consent order dated 12 March 2015 entered into between The New York State Department of Financial Services (**Department**) and Commerzbank.

Structural and Procedural Deficiencies in Commerzbank's AML Compliance Programme

Commerzbank's New York Branch (**New York Branch**) maintained correspondent accounts for Commerzbank's foreign branches. However, the New York Branch did not have access to due diligence information about customers of these foreign branches and hence could not conduct AML monitoring.

Foreign branches often transmitted payments to the New York Branch using non-transparent SWIFT payment messages that did not disclose the identity of the remitter or beneficiary. As a result of not having access to all of the relevant information about transactions, the New York Branch's compliance procedures were ineffective and fewer alerts or red flags were raised than would have been if all of the relevant information had been shared.

Even when alerts or red flags were raised in respect of transactions from foreign branches, the New York Branch compliance staff did not have direct access to the customer information necessary to investigate the alerts or red flags and had to request such information directly from the relevant foreign branch or Commerzbank's Frankfurt office. Responses to such requests often took many months or were inadequate, which prevented the New York Branch from investigating alerts properly and led to alert backlogs. On a number of occasions after information had not been provided from foreign offices, New York Branch employees carried out their own inadequate searches of the internet and public databases and subsequently closed off alerts. There were instances where compliance staff in the New York Branch attempted to strengthen transaction monitoring filters by adding the names of certain high-risk clients to the filters, but were prevented from doing so by staff at the Frankfurt office.

Alteration of Transaction Monitoring System to Reduce Number of Alerts

Until 2010, the thresholds of the transaction monitoring system were set based on a desire not to produce too many alerts. In 2011 a compliance staff member was asked by two senior compliance employees to reduce the thresholds in order to reduce the number of alerts generated.

Facilitation of Fraud by the Olympus Corporation

Between the late 1990s and around 2011, the Olympus Corporation (**Olympus**) perpetually committed account fraud in order to conceal hundreds of millions of dollars in losses from its auditors and investors. This fraud was carried out through several Commerzbank group companies and branches including the New York Branch. The New York Branch facilitated transactions totalling more than US$1.6 billion that supported or were related to Olympus' fraud, most of which did not trigger alerts in the New York Branch's transaction monitoring system. However, two large transactions in 2010 did raise alerts in the New York Branch. When responding to a request by the New York Branch for information on these transactions, personnel in the Singapore office did not relay any concerns about Olympus. This was despite personnel employed by the Singapore office having identified the same two transactions as suspicious and having broader concerns about Olympus in respect of its structure and transactions.

Previous Warnings of Compliance Failures

Internal auditors, the Department and other US regulators had on several occasions warned the New York Branch about its compliance deficiencies and Commerzbank had failed to take sufficient remedial action. In particular, an external consultant had identified that the New York Branch should implement a new transaction monitoring system.

Wire Stripping and Non-Transparent Cover Payments Used to Circumvent Sanctions

Commerzbank used wire stripping and non-transparent payment messages to process tens of thousands of transactions through the New York Branch on behalf of customers subject to US sanctions.

Between at least May 2003 and June 2004 Commerzbank altered or stripped information from wire messages for payments involving Iranian entities in order to hide the true nature of the payments. Commerzbank even had a dedicated team of employees to facilitate Iranian transactions by removing information from SWIFT payment messages that could trigger sanctions-related controls. Instructions were circulated amongst Commerzbank employees, directing them to remove information from wire messages that could identify sanctioned parties.

Between 2002 and 2007, Commerzbank used non-transparent cover payments to process transactions for clients subject to US sanctions. Commerzbank instructed employees to split incoming payments messages into two outgoing messages. One would be sent to the beneficiary's bank and the other to the US clearing bank, which would not contain any information about the remitter in order to prevent transactions from being detected and frozen, blocked or delayed.

Between 2002 and 2006, Commerzbank maintained US dollars accounts for 17 Sudanese banks and processed transactions valued at more than US$224 million using non-transparent methods.

Penalties

Commerzbank has agreed with various United States authorities including the Department to pay a total of US$1.45 billion for its AML and sanctions breaches.

In addition, an independent monitor shall review the New York Branch's AML and sanctions compliance procedures now in place and report directly to the Department. The independent monitor's report will include required corrective measures. Commerzbank will be required to implement these measures by making changes to its compliance programme.

Commerzbank has also been required to dismiss four employees that were involved in the bank's improper conduct.

Prosecutors agreed to defer criminal charges for three years in consideration for Commerzbank boosting its AML and sanctions compliance regimes.

DEUTSCHE BANK FINED US$8.4 MILLION BY DUBAI REGULATOR

The Dubai International Financial Centre (**DIFC**) branch of Deutsche Bank AG (**Deutsche Bank**) has been fined US$8.4 million by the Dubai Financial Services Authority (**DFSA**) as set out in a decision notice dated 29 March 2015.

The DFSA fined Deutsche Bank for:

- Providing misleading information to the DFSA
- Failing to comply with AML and conduct of business requirements in respect of certain clients of Deutsche Bank
- Failing to have in place adequate governance, systems and controls and compliance arrangements to meet regulatory requirements

The decision notice followed an investigation into Deutsche Bank by the DFSA in respect of activities carried out by the bank between January 2011 and January 2014. The investigation was launched after it was suspected that Deutsche Bank was failing to classify certain customers as clients of the DIFC branch in breach of DFSA rules.

The investigation confirmed that Deutsche Bank's private wealth management business had been advising on financial products and credit, and arranging credit and deals in investments, whilst failing to classify a number of customers receiving those services as clients, despite DFSA rules prescribing that the provision of such services requires such classification. Instead, Deutsche Bank had been classifying those customers as clients of the booking locations where the relevant transactions were executed, each of which were other Deutsche Bank group branches or entities. In failing to classify customers appropriately, Deutsche had deprived them of certain regulatory protections.

It was further revealed that certain Deutsche Bank employees had represented expressly to the DFSA that the DIFC branch had been merely referring and introducing customers to other parts of the Deutsche Bank group, activities which do not trigger the requirement to classify customers as clients.

As a result of inappropriate classification, Deutsche Bank failed to comply with certain Conduct of Business requirements and AML requirements in relation to a number of customers.

Contrary to DIFC AML rules, Deutsche Bank failed to:

- Subject customers to customer identification and verification in the DIFC
- Subject customers to an AML risk assessment in the DIFC
- Ensure that its records were held in accordance with AML rules
- Establish and maintain effective AML policies, procedures, systems and controls to prevent opportunities for money laundering in relation to its activities
- Ensure its employees complied with the requirements of its AML systems and controls
- Review the effectiveness of its AML systems and controls

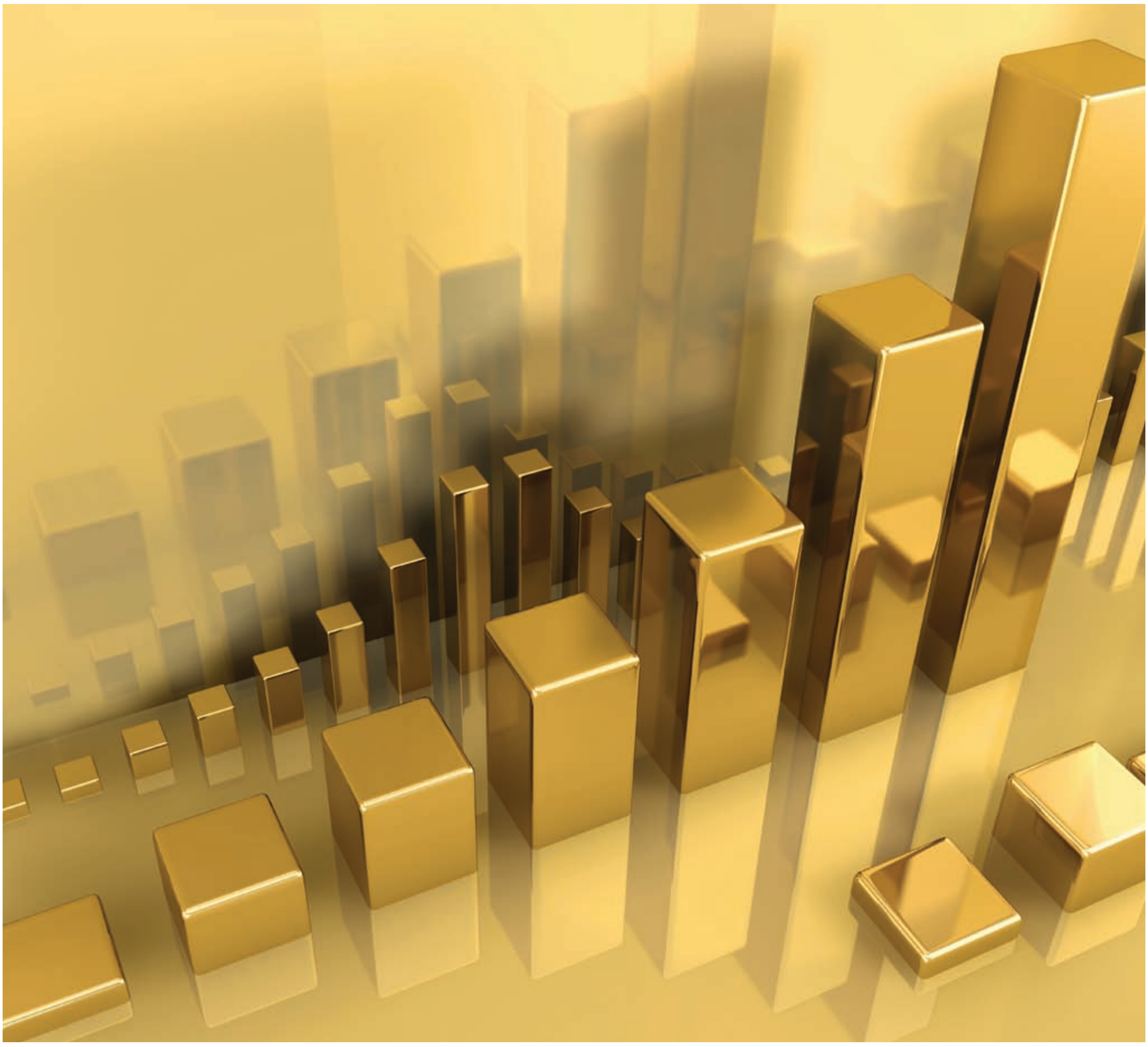
The DFSA decision notice further criticised Deutsche Bank for failing to have:

- Adequate systems and controls in place to ensure that it complied with DIFC legislation
- Adequate resources to conduct and manage its affairs, including financial and system resources as well as adequate and competent human resources

- A corporate governance framework in place adequate to promote the sound and prudent management and oversight of its business and to protect the interest of its consumers and stakeholders

The DFSA has imposed a number of directions in relation to Deutsche Bank's governance systems and controls. In the decision notice, the DFSA acknowledged that Deutsche Bank had already made certain improvements in this regard. No clients were found to have suffered an actual loss as a result of the acts and omissions of Deutsche.

The US$8.4 million fine is the largest ever imposed in the DFSA's ten-year history. The limits of the fines that the DFSA can impose were increased in 2014. Almost half of the total fine amount is attributable to Deutsche Bank's concealing of information, which misled the DFSA.



SUMMARY OF FATF PLENARY MEETING, FEBRUARY 2015

A FATF Plenary meeting was held between 25 – 27 February 2015 under the Australian presidency. The main outcomes of the meeting are set out below.

- Michel Sapin, the French Minister of Finance and Public Accounts, opened the meeting and spoke about the importance of a united global front in the fight against terrorism
- A statement was issued on FATF action against terrorist finance
- FATF adopted and published a report on the financing of Islamic State in Iraq and the Levant
- Two documents were produced by FATF, identifying jurisdictions that pose a risk to the international finance system due to their strategic AML/CTF deficiencies
- An update was provided to the meeting on improvements made to the AML and CTF systems in Albania, Cambodia, Kuwait, Namibia, Nicaragua, Pakistan and Zimbabwe
- There was a discussion of the mutual evaluation reports of Australia and Belgium, setting out the level of effectiveness of each country's AML/CTF system and compliance with FATF recommendations
- Increased collaboration between FATF and the Egmont Group of Financial Intelligence Units (an informal international network of financial intelligence units) was discussed
- An update was given on the voluntary tax compliance programmes of Argentina, Australia and France, each of were found to be consistent with FATF's four basic principles on voluntary tax compliance
- FATF decided to continue its work on "de-risking" in line with implementation of a risk-based approach
- Following a 2014 report on virtual currencies, FATF decided to progress this issue for a decision at the June 2015 Plenary meeting

SPEECH SETTING OUT FATF AGENDA AND PRIORITIES

FATF Vice-President Je-Yoon Shin gave a speech on 10 March 2015, setting out the current agenda and priorities of FATF in order to further its purpose to protect the global financial system from money laundering and terrorist financing. The main points of the Vice-President's speech are summarised below.

Global Regulatory Arena

The Vice-President commented on the increasing importance of AML and CTF as a regulatory focus across the past decade. Although strong AML and CTF controls are at the heart of many financial institutions, recent cases have shown that contraventions of these controls can result in fines in the billions of dollars and sanctions that can threaten the licenses of those institutions. Financial centres look to FATF for guidance on international standards as part of coordinated efforts to protect markets from the risks of money laundering and terrorist financing. FATF establishes robust "Recommendations" to fulfil its standard-setting role. The most recent version of FATF recommendations were adopted in 2012 (**2012 Recommendations**) and cover a wide range of measures to prevent money laundering and terrorist financing.

Risk-Based Approach

The 2012 Recommendations place more emphasis on a risk-based approach to AML and CTF. As such, countries, relevant authorities and financial institutions should assess and understand money laundering and terrorist financing risks to which they are exposed and take measures proportionate to the magnitude of those risks. This approach allows greater resources and enhanced measures to be applied where the risks are higher.

FATF has produced a guidance document on applying a risk-based approach in the banking sector, which is intended to assist banks in strengthening their internal risk assessment, due diligence processes and risk mitigation controls.

De-Risking

"De-risking" describes a situation where financial institutions terminate or restrict business relationships with clients in order to altogether avoid, rather than manage, the risk of money laundering or terrorist financing. De-risking can introduce risk into the global financial system as the termination of relationships with clients can force them into less regulated or unregulated channels, making the movement of funds less traceable and impeding the implementation of AML and CTF measures.

Although the 2012 Recommendations require institutions to terminate client relationships on a case-by-case basis where money laundering and terrorist financing risks cannot be mitigated, the wholesale termination of relationships with entire classes of customer is not in line with FATF standards.

Financial institutions are required to identify, assess and understand money laundering and terrorist financing risks and take measures to mitigate them, however this is not a zero-failure approach.

Mutual Evaluation Process

The Vice-President spoke about how FATF member countries, including both government agencies and private sector institutions, are subject to a vigorous mutual evaluation process in order to assess their success in the implementation of AML and CTF

measures. Norway, Spain, Belgium and Australia are among the first countries to have their AML and CTF regimes, including financial sector regulation, carefully scrutinised by a group of expert assessors. FATF has increased the emphasis in these assessments on the effectiveness of such regimes, ensuring that laws and agencies work effectively to deliver positive results.

Action on Terrorist Finance

As an increasingly global problem, terrorism requires action by a united international community. FATF has published a report on the financing of Islamic State of Iraq and the Levant, which will contribute to international efforts to combat terrorist financing. FATF and regional bodies will work together with international organisations to develop proposals to strengthen CTF tools and will report to the G20 in October 2015.

The Vice-President also referred to the United Nation's (**UN**) recently created consolidated sanctions list, containing designated persons and entities from all of the UN's sanctions committees. Feedback is encouraged from the private sector to ensure that the list is useable by private sector institutions.

FOURTH MONEY LAUNDERING DIRECTIVE – LATEST DEVELOPMENTS

On 20 April 2015, the Council of Europe adopted the Fourth Money Laundering Directive (**MLD4**) and the Wire Transfer Regulation (**WTR**). This will allow the European Parliament to adopt MLD4 and WTR at a future plenary session, after which they will be published in the Official Journal of the European Union and become law. Each Member State will then have two years to implement the provisions of MLD4 through national legislation. The WTR has direct effect and as such will automatically become law in each Member State.

The European Commission put forward proposals for MLD4 in order to update and enhance the existing AML/CTF framework prescribed under the Third Money Laundering Directive, which was passed in 2005, and to implement FATF's February 2012 AML and CTF standards.

Some of the key changes that will be made to the AML/CTF regime by MLD4 include:

- Widening the scope of the regime to include a broader range of transactions, including requiring customer due diligence to be applied to persons carrying out cash transactions of €7,500 or more where trading in goods (the current threshold is €15,000)
- Tightening the rules on customer due diligence
- Requiring corporate entities established within Member States to hold accurate information on their beneficial ownership and trustees to disclose their status and information on underlying beneficial ownership
- Removing provisions allowing exemptions for certain aspects of customer due diligence in respect of third countries that are considered to have AML/CTF systems equivalent to those in the EU
- Requiring Member States to adopt a risk-based approach to addressing the threat of AML and CTF by identifying, assessing, understanding and mitigating the risks they face in respect of AML/CTF

KEY CONTACTS

FOR FURTHER INFORMATION OR ADVICE PLEASE CONTACT:

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

Phil McEachen
Associate
London
T +44 (0)20 7153 7713
philip.mceachen@dlapiper.com

www.dlapiper.com