DLA PIPER

SPRING 2014

MONEY LAUNDERING BULLETIN

Regulatory News Update from DLA Piper

CONTENTS

Introduction

DLA Piper's Financial Services Regulatory team welcomes you to the Spring 2014 edition of our Anti-Money Laundering Bulletin.

In this issue we look at the Standard Life fine in the context of scrutiny of PEPs. We also provide updates of AML issues in the UK and internationally.

I 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.

NEWS

MONEY LAUNDERING CASES SURGE AFTER CRACKDOWN

Accountancy firm BDO have prepared a report analysing the amount of fraud cases in the UK worth over £50,000. BDO's research details that:

- Reported Money laundering related to fraud offences has surged by 309% to £288m;
- Fraud in Financial Services now accounts for 51% by value of all UK reported fraud; and
- There has been an increase in legislation and compliance in Financial Services driving the increase in reported fraud.

Kaley Crossthwaite, Head of Fraud at BDO, commented that the rise in reported cases of money laundering must be, in part, down to the "demand for transparency in the financial services sector." BDO suggest that the call for greater transparency is being driven by the increased regulation and compliance of the financial services sector by the FCA and the PRA.

BDO's research shows that finance and insurance is the sector most susceptible to fraudulent activity of which money laundering is the most common type. Money laundering accounts for almost 28% of all fraudulent activities. At the other end of the spectrum, mortgage fraud and corruption account for just over 7% of fraudulent activities within the UK.

Despite the rise in reported fraud, figures show that the value of that fraud has decreased. Kaley Crossthwaite commented that "it is very surprising that that the total value of fraud is down when the number of reported frauds has risen so steeply. Usually driven by greed, the consensus view is that fraud is increasing, but it is always very difficult to quantify given the general lack of reporting of fraud across different sectors in the UK. Unless it is easy to quantify and explain in court, many frauds do not get brought to trial."

UK COURT PROCEEDINGS AND ENFORCEMENT ACTION

STANDARD BANK PLC FINED £7.6M FOR FAILURES IN ITS ANTI-MONEY LAUNDERING CONTROLS

On 23 January 2014 the FCA fined Standard Bank PLC £7,640,400 for failings related to its anti-money laundering ("**AML**") policies and procedures governing corporate customers connected to politically exposed persons ("**PEPs**"). Following an investigation the FCA found that between 15 December 2007 and 20 July 2011 there were weaknesses in the banks AML systems and controls which put the bank at risk of being used to launder the proceeds of crime. AML policies were not applied consistently to corporate customers who were connected to PEPs.

In a press release the FCA stated that they considered the failings as particularly serious because:

- Standard Bank provided loans and other services to a significant number of corporate customers who emanated from or operated in jurisdictions which have been identified by industry recognised sources as posing a higher risk of money laundering;
- Standard Bank identified issues relating to its ability to conduct ongoing reviews of customer files early in the relevant period, but failed to take the necessary steps to resolve the issues; and
- The FCA has previously brought action against a number of firms for AML deficiencies and has stressed to the industry the importance of compliance with AML requirements.

Guidance issued by the Joint Money Laundering Steering Group ("**JMLSG**") sets out that a customer will be in a higher risk category if they are known to be linked to a PEP though either a directorship or shareholding. As a consequence the bank should have been applying enhanced due diligence measures. Standard Bank have co-operated with the FCA's investigation and have taken significant steps to provide appropriate remediation.

MODEL LOSES APPEAL TO KEEP LAUNDERED MONEY

Following the conviction of her fiancée for money laundering last year, Oxana Zubakova appealed to have £83,000 of confiscated cash returned to her. However in January 2014 her case was dismissed at the Old Bailey. Zubakova claimed that the cash, seized from her UK safety deposit box, was given to her by a Spanish businessman and was her own earnings.

At the trial, Prosecutors confirmed that they did not consider Zubakova a suspect however they believed that the money had actually been given to her by Tarik Meghrabi who was involved in a money laundering operation worth £35 million. Meghrabi is serving a prison sentence of five years and nine months after being convicted of the money laundering scam. The National Crime Agency, previously the Serious Organised Crime Agency, argued that Zubakova must forfeit the cash as they considered it was the proceeds of crime.

FIRM FINED £1.8MILLION FOR "UNACCEPTABLE" APPROACH TO BRIBERY & CORRUPTION RISKS FROM OVERSEAS PAYMENTS

In December 2013 the FCA issued a final notice to JLT Speciality Limited ("**JLTSL**") for "failing to have in place appropriate checks and controls to guard against the risk of bribery or corruption when making payments to overseas third parties." JLTSL, who provide insurance broking and risk management services, were fined £1.8 million for breaching the FCA's principle of management and control following an investigation.

The FCA found that from February 2009 until May 2012 JLTSL did not conduct appropriate due diligence before entering into agreements with overseas introducers who assisted JLTSL in gaining business. Further, the FCA noted that JLTSL did not adequately assess the possible risks of new insurance business that was secured through their existing overseas introducers.

During the relevant period JLTSL received almost £20.7 million in commission from business through overseas introducers and paid £11.7 million for their services. JLTSL had inadequate procedures for these payments and the FCA considered that there was "an unacceptable risk" that the overseas introducers could use payments for corrupt purposes. In an accompanying press release the FCA stated that "JLTSL's penalty was increased because of its failings to respond adequately either to the numerous warnings the FCA had given to the industry generally or to JLTSL specifically."

INTERNATIONAL

NEWS

MLD4 UPDATE

On 23 January 2014, the European Parliament updated its procedure file in relation to the Fourth Money Laundering Directive ("**MLD4**"). The European Parliament will consider MLD4 at its 10 to 13 March 2014 plenary session. This indicative date has been moved forward from the previous dates 2 to 3 April 2014. MLD4 is proposed to prevent the financial system from being used for money laundering and terrorist financing, it will replace the current Third Money Laundering Directive.

MLD4 will apply to a wide range of businesses who are at risk of money laundering and/or terrorist financing, in particular regulated financial institutions. MLD4 makes key amendments to the Third Money Laundering Directive, including:

- The extension in scope of the money laundering directive by lowering the effective threshold of persons dealing in cash payments;
- The definition of politically exposed persons will be extended;
- The proposed Article 7 of MLD4 introduces a requirement for member states to identify, assess, understand and mitigate the risks they face, and to keep their assessments up-to-date; and
- The clarity and accessibility of beneficial owner information will be enhanced.

The European Commission passed the legislative proposals of MLD4 to the Parliament and the Council for consideration. MLD4 requires a qualified majority for adoption by the Council, which must be agreed with Parliament. It is possible that MLD4 will be adopted at its first reading in Parliament. Following adoption, MLD4 will be published in the Official Journal and subsequently come into force 20 days after the date of publication.

THE ROLE OF HAWALA AND OTHER SIMILAR SERVICE PROVIDERS IN MONEY LAUNDERING AND TERRORIST FINANCING

In December 2013 the Financial Action Task Force ("**FATF**") published a report on the role of Hawala and other similar service providers ("**HOSSPs**") in money laundering and terrorist financing. Many countries view HOSSPs as essential to unbanked countries with limited financial systems. For many of the communities within these countries without HOSSPs there would be no access to financial services. In contrast there are a large amount of law enforcement agencies who view HOSSPs "as one of the leading channels for terrorist financing and money laundering." It is against the backdrop of these conflicting opinions that the FATF have written their report to demystify HOSSPs.

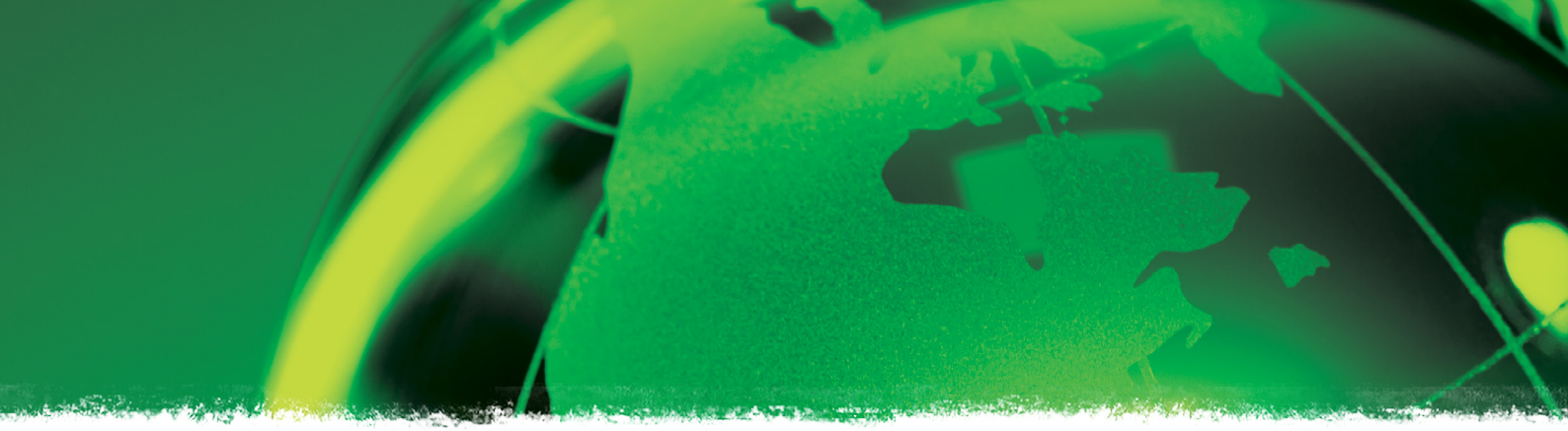
Due to the fact that HOSSPs is not a universally defined term and there are differing variations across jurisdictions the FATF clarified that for the purpose of their report HOSSPs are defined as "money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time."

The report explains that although there are some HOSSPs used by legitimate customers for reasons of geography, culture and lack of access to financial systems there are also many who use HOSSPs for illegitimate reasons. The use of HOSSPs, a cash in/cash out business, allow individuals to evade monetary controls related to currency and tax as well as transferring or concealing criminal proceeds. The report does state however, that HOSSPs can have detailed records and are not always high risk. The FATF found that HOSSPs often settle through banks who are able to notify the regulators of any suspicious activities made visible to them during this process.

The FATF highlighted the fact that although only a limited number of criminal HOSSP case studies were looked at it is clear why HOSSPs continue to pose money laundering and terrorist financing risks. The reasons included:

- That there is a lack of supervisory will and/or resources;
- In some cases HOSSPs allow for the settlement across multiple jurisdictions through value or cash outside of the banking system; and
- HOSSPs use businesses that are not regulated financial institutions.

The key concern is that the lack of supervision attracts criminals and terrorist financiers. The FATF states that the international community should bring HOSSPs under a risk based anti-money laundering and counter terrorist financing regulatory and supervisory framework.



THE RISK OF PRE-LOADED AIRLINE LOYALTY CARDS

The new airline stored-value (or prepaid) cards that are being issued to loyalty program members have raised concerns regarding anti-money laundering compliance. Both Qantas and Virgin Australia now offer an international wallet function via major credit card networks. Despite being approved by the Australian Financial Services Licence Holders the cards expose the customers and the reporting entities to a unique risk.

The airlines state that the cards offer a dual function and can be used as a standard loyalty card if the member does not want to utilise the payment function. However, the worry is that the cards, which reportedly look like credit cards, are sent out to scheme members as young as 16 without their consent to "opt in". Stored-value cards can facilitate the instantaneous transfer of funds across borders via the global ATM network.

In 2010 the Australian Transaction Reports and Analysis Centre ("**ATRAC**") identified prepaid cards as a developing money laundering and terrorist finance threat. ATRAC are aware of the risk that cards with "digital" funds are easily transferred to different jurisdictions, either by post or in someone's purse. In addition, there is concern over the ease at which the cards can be activated, particularly in a case where a card is stolen.

The FATF have issued guidance on prepaid cards stating that they pose an anti-money laundering and terrorist financing threat due to the fact that they allow for non face to face business relationships. The FATF suggest using multiple techniques to verify the identity of customers effectively such as enhanced customer due diligence. There is no doubt that stored value cards increase money laundering and terrorist financing risks, therefore the fact that these cards are being sent out to all eligible members only heightens this risk.

BASEL COMMITTEE ON BANKING SUPERVISION – SOUND MANAGEMENT OF RISKS RELATED TO MONEY LAUNDERING AND FINANCING OF TERRORISM

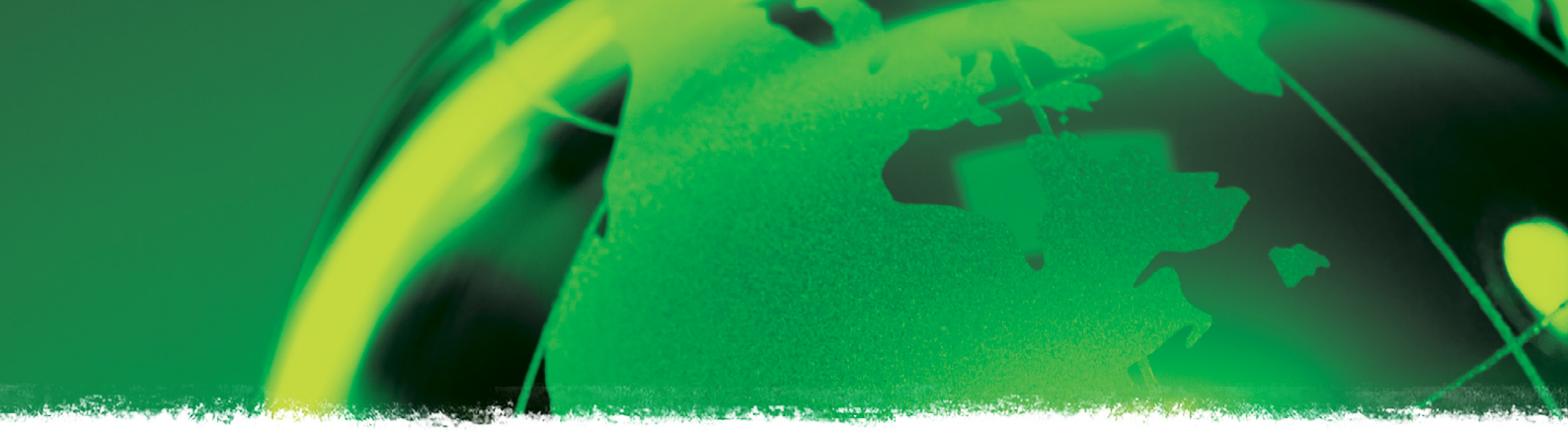
In January 2014 the Basel Committee on Banking Supervision (the "**Committee**") issued guidelines which set out that banks should include risks related to money laundering and financing of terrorism within their overall risk management framework. These guidelines are cross referenced to the standards on combating money laundering and the financing of terrorism and proliferation issued by the Financial Action Taskforce ("**FATF**") in 2012.

The Committee's Charter sets out that its mandate is "to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability", this is fully aligned with the new guidelines. The Committee considers that anti-money laundering policies and combating terrorist financing are at the heart of ensuring the safety and soundness of banks.

The guidelines recommend that:

- The board of directors should approve and oversee the policies for risk, risk management and compliance in the context of money laundering ("**ML**") and financing of terrorism ("**FT**") risk;
- Banks should develop and implement clear customer acceptance policies and procedures to identify the types of customer that are likely to pose a higher risk of ML and FT pursuant to the bank's risk assessment; and
- Banks should have an understanding of the normal and reasonable banking activity of its customers that enables the bank to identify attempted and unusual transactions which fall outside the regular pattern of the banking activity.

The guidelines state that "the inadequacy or absence of sound money laundering/financing of terrorism risk management exposes banks to serious risks, especially reputational, operational, compliance and concentration risks." The guidelines go on to state that robust enforcement actions resulting in heavy fines from the regulators could be avoided if more effective risk based policies and procedures were implemented. The guidelines also highlight that the diversion of management time and resources to resolve problems is another hindrance to banks.



INTERNATIONAL ENFORCEMENT ACTION

CFATF DECIDES TO CALL FOR COUNTER MEASURES AGAINST BELIZE AND GUYANA

The Caribbean Financial Action Task Force ("**CFATF**") is comprised of twenty-nine jurisdictions of the Caribbean Region who implement the Financial Action Task Force ("**FATF**") Recommendations. The recommendations encourage anti-money laundering policies and ways to combat the financing of terrorism through compliance with international standards. However the CFATF previously found anti-money laundering deficiencies within both Belize and Guyana and are now calling for counter measures against them.

In May 2013 the CFATF recommended that Belize and Guyana take steps to ensure that they have addressed their deficiencies. Both countries have made some effort although they have failed to approve and implement certain required legislative reforms. The CFATF has stated that Members are advised to implement counter measures to protect their own financial system until Belize and Guyana have implemented all the outstanding issues in their Action Plan. Belize is required to, among other things, address customer due diligence requirements and prohibit dealings with shell banks. Guyana on the other hand must fully criminalise money laundering and terrorist financing offences as well as strengthening the requirements for suspicious transaction reporting, international co-operation, and the freezing and confiscation of terrorist assets.

The CFATF feel that these counter measures are necessary to protect the international financial system from the on-going money laundering and terrorist financing risks arising from Belize and Guyana.

BITCOINS AND AML

Charlie Shrem, a founding member and the vice chairman of the Bitcoin Foundation was arrested on 26 January 2014 and charged with conspiring to commit money laundering. US Prosecutors have accused Shrem of engaging in a scheme which sold more than US$1 million in bitcoins to users of an anonymous online drug market place known as Silk Road. Shrem was also accused of operating an unlicensed money transmitting business. Robert Faiella has also been charged with related money laundering offences.

Bitcoin is an international "virtual" currency that is able to be traded online anonymously. Bitcoin exchanges allow users to trade bitcoins for traditional currencies. Due to the nature of the bitcoins the exchange has attracted negative comments in the press. This was exemplified in October 2013 when the FBI shut down Silk Road and arrested Ross Ulbricht on suspicion of being the chief operator of Silk Road. The majority of items sold on Silk Road were illegal drugs or weapons and all transactions were made by bitcoins.

James Hunt, from the US Drug Enforcement Agency, said in a statement following the arrests that "Hiding behind their computers, both defendants are charged with knowingly contributing to and facilitating anonymous drug sales, earning substantial profits along the way. Drug law enforcement's job is to investigate and identify those who abet the illicit drug trade at all levels of production and distribution, including those lining their own pockets by feigning ignorance of any wrong doing and turning a blind eye."

Following his arrest Shrem resigned from the Bitcoin Foundation. If convicted, money laundering carries a maximum sentence of 20 years in prison while operating an unlicensed money transmitting business carries a maximum sentence of five years in prison.

Simultaneously, Russian authorities have issued warnings about the risk of using bitcoins. The Russian Prosecutor General's office issued a statement on 6 February stating that Russian law specifies the rouble as the sole official currency and that using, or treating, bitcoins as a parallel currency is illegal. The authorities warned that the virtual currency could be used for money laundering or the financing of terrorism. At the end of January the Russian Central Bank also expressed their view that bitcoin trades are highly speculative and that the unit carried a big risk of losing value. The Prosecutor's General Office and the Central Bank are working together to tighten Russia's regulations.

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

Simon Wright
Financial Services Regulatory
Legal Director
London
T +44 (0)20 7796 6214
simoncj.wright@dlapiper.com

FINANCIAL SERVICES TEAM

DLA Piper's dedicated Financial Services team offers specialist legal expertise and practical advice on a wide range of contentious and advisory issues. The team has an experienced advisory practice which gives practical advice on all aspects of financial services regulation and anti-money laundering. The team can also assist clients on contentious legal matters including: internal and regulatory investigations, enforcement actions and court proceedings in the financial services sector.

If you have finished with this document, please pass it on to other interested parties or recycle it. Thank you.

www.dlapiper.com