Original Article

Money laundering: A primer for banking staff

Received (in revised form): 16th June 2015

Mohammed Ahmad Naheem
holds a Bachelor's Degree, two Masters Degrees and has completed a PhD, all in the economic, banking and investment management domains. At the time of submitting this paper (June 2015) the author is currently working on his second doctorate level research project titled 'Trade Based Money Laundering: Exploring the Empirical Implications for Global Banks', which is expected to be published in December 2015. This current paper contributes towards a series of banking papers that focus on AML compliance and money laundering within the broader banking and financial services sector.

ABSTRACT **This article provides an introduction to money laundering (ML) and outlines the problems that banks face in detecting and assessing for risk. The article provides a brief history of earlier ML techniques such as cash deposits and the traditional model of placing, layering and integrating illegally acquired cash, before focusing on the modern-day problems. The banks are now having to deal with the progression and the increased levels of sophistication of ML techniques. Historically banks have addressed ML through national regulation systems, which have arisen from the state's focus on preventing the drug market expanding. However as other criminal activities are now funded through ML, the state regulation system has also expanded and there is now the added social obligation on banks to support the state in detecting and combatting ML activity across all criminal activities. The article considers some of the difficulties that banks face when trying to detect ML activity. A number of case studies are included, from recent reports from the Australian financial intelligence unit (FIU), to illustrate the modern level of complexity involved in each scheme. Finally, the article refers to recent research soon to be published that explores a number of suggestions made by industry experts from across the global banking, financial services, technology, audit, training and risk assessment sectors. The biggest challenge the article concludes is to be able to quickly and effectively bridge the knowledge gap between what money launderers know about using financial services and what the banks are aware of. The article proposes a new risk assessment tool that can be applied simply within the sector, which has been developed from the research material. This is a article that will be of great interest to anyone working in the financial regulation, banking or financial services sector, as well as law enforcement and FIUs across the globe.**

International Journal of Disclosure and Governance (2016) **13,** 135–156. doi:10.1057/jdg.2015.10;
published online 3 September 2015

Keywords: anti-money laundering; trade-based money laundering; banking; risk management; financial crime; compliance

INTRODUCTION

There have been a number of articles in the media and courts recently covering different banking scandals. These have highlighted, among other things, gaps in the money laundering (ML) detection and compliance systems of the major banks (Homeland Security, 2012; Hamilton, 2015). Some of these examples, such as the HSBC Bank in America (HBUS) accepting large cash deposits from Mexican banks (Homeland Security, 2012), may seem to be obvious gaps in the system, but in reality the

Correspondence: Seven Foundation, Zurich 8002, Switzerland
E-mail: mnaheem@sevenfoundation.ch

challenges facing banks have never been as complex as they are today. The reality is that ML has now become an important component of most large organised criminal activity (Durrieu, 2013) and is now considered as a major business, with a consistent estimated value at between 2 and 5 per cent global GDP (Takáts, 2007; Kar and LeBlanc, 2013). The drug market is still probably the largest contributor to this figure with an overall estimated worth of US$100 billion (Simser, 2012) and an estimated 60–80 per cent of drug profits being laundered (UNODC (United Nations Office on Drugs and Crime), 2011). The question that many might ask, given the scale and enormity of the problem, is 'what exactly are banks doing to prevent this situation escalating any further and why can't money laundering be stopped completely?'.

In order to answer this question thoroughly, a detailed level of understanding is needed of both the history of ML and an overview of the bank's responses. This article starts by reviewing the historical context of ML through the financial sector and maps out the processes that the banks have undertaken to date. Then it considers the evolution of ML as a major business and the implications that this now has on the banking sector and other services involved in the business and financial services sectors. Finally, the article concludes by considering results from a recent research project undertaken among experts within the financial and banking sector. This project looked at exploring the development of a modern risk assessment approach to tackle the more complex and covert types of ML schemes currently being presented to the formal financial sector.

HISTORY OF ML

ML is not a new crime, and although its origins are officially unknown some authors have pointed to early Chinese traders hiding profits from rulers as an example of early ML activity, as far back as 2000BC (Morris-Cotterill, 2002). Similarly the term 'ML' has several potential sources, again none of which have been determined. There are reports that state that the name can be traced back to the mafia in the United States in the early 1920s, and their use of a legitimate washing laundry as a front business to hide the proceeds of their illicit activities, although this origin has never been officially supported either (Durrieu, 2013). However, since this period in time there is no doubt that the concept of bringing money acquired through illegal activity into the legitimate financial sector, where it can be used freely, has been at the core of most business models for large-scale criminal laundering activity. The most noticeable trade for ML has been the drugs trade, which provides an estimated 20 per cent of all criminally acquired cash (UNODC, 2011) with the cocaine market alone estimated to be worth $88 million (Simser, 2012). However, there are a wide range of other criminal activities that use ML; these include illegal arms smuggling, piracy, human trafficking and political corruption.

The main financial problem for most large-scale criminal organisations and especially drug traffickers is that the crime tends to produce large amounts of cash, that then needs to be deposited into the formal financial sector. It was by using the example of these early crime scenarios that the traditional model for describing ML within banks was developed, that is, *placing* cash in the bank, *layering* the money into various accounts and finally *integrating* the money in with legitimate money to disguise its origin and illicit background (Arnone and Borlini, 2010). However with the variety and speed of financial transactions in operation in current banking situations, this model is often too simple to describe ML techniques used among the modern criminal organisations.

Changes in the legal landscape

In the United States during the 1970s, a legal framework for tackling ML was first introduced through the Bank Secrecy Act or BSA (1970) under President Nixon. The focus of this act was to try and de-escalate the drugs trade through tracking the financial trails. The acknowledgement that ML was a crime *per se* was slow to be recognised globally and the first major international legal recognition of ML was not made until the United Nations (UN) Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances was published in 1988 (usually referred to as the Vienna Convention). The UN document provided the framework for establishing an international legal response to ML, which was further expanded in the 1990s to include crimes other than drugs and again in early 2000 after the 9/11 attacks, to include the financing of terrorism (Durrieu, 2013).

There are now a number of acts that can be used in order to prosecute ML offences, such as drug laws and terrorism-related legislation, for example, UK – Drugs Trafficking Offences Act 1986, the Prevention of Terrorism (Temporary Provisions) Act 1989 (also UK), the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) (2001), the Malaysian Anti-Money Laundering (AML) and the Anti-Terrorism Financing Act (2001). Most countries are now developing their own domestic legislation, and all of these regulations and legal frameworks from around the globe focus on several key actions that banks and other financial services can do in order to detect ML activity and report it to the relevant state authorities. However, the challenge now facing law enforcement and the financial services is that each domestic law is different at some level. This provides legislative gaps that criminals can exploit in order to evade prosecution, especially when moving money between different jurisdictions (Arnone and Borlini, 2010).

Implications of the changing legislation on the financial services sector

Originally the crime of ML did not exist as a separate crime it was always linked to predicate offences, or the activity that produced the illegal money. This meant that banks were only ever indirectly linked to any criminal activity that their clients engaged in. However, in recent times the legal landscape has begun to change and ML has slowly gained recognition as a crime in its own right in some states (McCarthy *et al*, 2014). This in turn has placed greater pressure on banks because now the act of concealing ML is also a criminal activity in many countries as the ML laws are updated. Definitions such as 'suspicious' can now be cited in criminal cases (Rahman, 2013), which means that banks will have to prove that they acted in a reasonable manner, and explain to the court the measures they took with client accounts considering all the evidence and information that they had access to and the likelihood that ML activity was taking place using their institution.

MODERN-DAY ML AND AML REGULATION

There are a number of theories as to why regulation and laws were enacted in order to try and address ML. One theory is that regulation was enacted to defeat the drug traffickers and dealers on the streets in the United States and to reduce the emerging drug epidemic at that time. It is certainly true that banks hold key information that can assist law enforcement agencies in their hunt for criminal activity (Rahmen, 2013), and this theory would perhaps explain some of the history of the bank's reluctance to become involved in detecting ML, that is, there was a presumption that ML was not a risk to the bank, it was a state concern to tackle drug distribution. Other academics have argued, however, that money regulation was introduced in recognition of the impact that it did have on the financial sector 'this phenomenon produces a negative influence on the financial sector, and more broadly, on the economy as a whole' (Durrieu, 2013, p. 110).

The Financial Action Task Force (FATF)

The FATF was established in 1989 after being initiated by the G7 summit members that same year. It is an intergovernmental body comprising Ministers from its 34-country membership. Its role is to keep its members aware of and informed on ML techniques and trends affecting the financial and banking sectors.

> The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.(FATF, 2015)

FATF have produced several guidelines on risk-based approaches (RBAs) towards ML detection (FATF, 2006, 2012) and are continuing to update their indicators and red flags for different ML schemes. However like the constantly changing ML processes, financial regulation is also constantly having to evolve in order to meet the global and practical challenges emerging in the banking and financial services sectors (O'Brien and Dixon, 2013). Among these challenges is the recognition that ML is also an ethical and social corporate responsibility issue and not solely a compliance problem. O'Brien and Dixon (2013) explain how governance and accountability are now as much a part of AML solutions within banking as the traditional deterrence and compliance components. This means that more units within the banking structure need to become familiar with ML techniques and a more open and transparent communication system needs to be developed to ensure that suspicious client and transaction behaviour is shared across all the relevant sections (Naheem, 2015).

Regulatory responses

Initial regulations and laws that were introduced in the 1970s and 1980s such as the BSA were probably not considered a high priority to banks, as these along with other modern-day AML compliance issues are still perceived as cost centres rather than profit centres in the business plan of the bank (Naheem, 2015). This corporate attitude to ML is sometimes still prevalent in business thinking today and has implications for current risk assessment processes. If there is not a high priority placed on establishing the source of the money, at either governance and/or audit level, then resources and training will not be considered a high priority for AML risk assessment projects either. In order to make it an issue of priority, regulators have started challenging banks through the legal system.

Regulation

AML regulation mainly focuses on acquiring data about client behaviour and transaction history, often referred to as 'Know Your Customer' (KYC) policies. Price Waterhouse Coopers have developed a guide available to the financial services sector. This document provides a global overview of all the country responses to Customer Due Diligence (CDD) along with the local approach of regulators towards AML risk calculation – 'as well as details around KYC requirements, information about whether local regulators support the use of the risk based approach to AML, how to deal with Politically Exposed Persons ("PEPs") and whether doing business with shell banks is prohibited' (pwc, 2015, p. 6).

The KYC system revolves around tracking suspicious client accounts and producing a suspicious activity report (SAR) that the bank must send onto their national financial intelligence unit (FIU). There have been concerns about breaching the confidentiality of clients by providing such information (Rahman, 2013), while others argue that it is within the right of the bank to seek clarification on clients who may be accessing bank services, in order to instigate or participate in criminal activity.

However, the almost single-track approach of increased regulation has been criticised by some academics as potentially being counter-productive and actually encouraging risk avoidance strategies to emerge rather than developing strong risk assessment techniques (Macey, 1991). There needs to be balance as Pellegrina and Masciandaro (2008) explain as the increasing cost of regulation in order to match the complexity of criminal laundering and the overall economic environment are all factors that have to be considered when developing an appropriate AML model. At some point they argue it may not be economically viable for banks to constantly invest in regulation if criminals are only developing other ways to achieve their end result.

AML risk assessment

The basis for any AML detection scheme or risk assessment process is to try and determine the money that has been acquired illegally and which the criminal is trying to enter into the formal financial sector, where it can be accessed easier and utilised more fully. The traditional system of risk assessment for ML has revolved around using an identified series of red flag alerts that are considered to be indicators of illicit money transactions (Soudijin, 2014). The red flags have often been developed by specialist bodies such as the FATF (2012). Indicators can include examples such as the following taken from the Trade-Based Money Laundering (TBML) report (FATF, 2006):

- The transaction involves the receipt of cash (or other payments) from third-party entities that have no apparent connection with the transaction
- The transaction involves the use of repeatedly amended or frequently extended letters of credit
- The transaction involves the use of front (or shell) companies

These examples relate specifically to the process of ML that can occur through the use of goods and shipments, which aim to disguise where the money is coming from. Other guidelines for red flags can be developed in conjunction with in country FIUs. These units were established in order to process the suspicious reports that banks raise once they have a suspicious transaction that they believe could potentially be linked to ML or criminal activity. The Egmont Group report in 2000 listed six areas of concern, that they recommended as the basis for developing red flag alerts, these were:

- Large-scale cash transactions
- Uneconomical fund transfers to or from foreign jurisdictions
- Unusual business activity
- Large or rapid movements of funds
- Unrealistic wealth compared with client profile
- Defensive stance to questioning

Even since these indicators were developed in early 2000, the complexity of ML schemes has increased quite significantly. Despite this, a lot of the training for banks and other smaller financial companies has not developed at the same speed and with the same level of knowledge of what is actually possible (Naheem, 2015). The rest of this report focuses on how an effective risk assessment model could be developed that would be useful to the banking and financial services sector.

Red flag indicators

Most of the guidelines for detecting ML activity, such as FATF (2006) or the FIU reports (Egmont Group, 2000) provide indicators and red flags that can be incorporated into a risk assessment model by the bank. These risk assessment models have typically been fairly static and consist of a checklist of yes/no responses. The FATF (2012) has suggested that risk assessment should become a more dynamic and responsive process and uses the term 'RBA'. This means that banks need to be proactive in researching local context risks and ensuring that trade arrangements with other countries are also researched to assess current political and economic risks.

All of these factors take time and resources, but without them they could potentially increase the bank's exposure to ML risk. RBAs are by their very nature broad in their design, and it is not always as straightforward as simply researching a county or following a set of indicators. In fact FATF have been criticised for stopping short at advising banks how exactly they should go about achieving this more flexible RBA. While some academics have gone as far as to question the knowledge base within FATF, especially for the more complicated ML techniques such as TBML (Soudijin, 2014). The lack of understanding and clarity as to what to look for in ML cases and how to detect it seems to lie at the core of why risk assessment has stalled in its development so far.

ML patterns

Red flag alerts are developed through the analysis of known case studies, information that is generally kept within law enforcement. However, there are also many typology reports and sanitised case studies that identify the main scenarios that banks may encounter in a standard ML crime. Some countries such as Australia have produced very detailed reports on typologies that they have investigated through the FIU AUSTRAC (2013). Most countries have a report of some kind, although the format of presentation may be different in each country such as the Belgium FIU report (ctif cfi, 2013). These are all valuable research tools for local banks, which highlight the type and complexity of cases that have been uncovered locally, usually between banks and law enforcement investigations. These reports also tend to provide a standard list of red flag alerts that would be associated with each of the cases that they have reported on.

Suspicious activity reports

Once an activity has been flagged as potentially suspicious, then a SAR is filed with the national FIU. The aim of this is to assist law enforcement track criminal activity and the purpose of the SAR is threefold; to increase the level of disruption of criminal activity, second to bring money launderers to justice and third to recover the proceeds of crime (Yeoh, 2014). It is also of benefit to the bank in terms of reputational risk and ensuring compliance with the regulator and state demands, that is, to keep law enforcement aware of potential criminal activity. However, this is a resource intense exercise and there is always strong competition for resources within any business seeking to generate profit. In order for banks to prioritise spending on this level of resource for completing and filing SARs, as opposed to generating profit for the bank, there needs to be strong corporate attitude of support towards AML compliance. This support needs to extend down from the governance structure and permeate across all sections and units within the bank if it is to be effective.

Governance

The governance structure of the bank includes the audit committee, management and the Directors of the Board. They all play an important role in determining how effective a bank's corporate attitude towards AML compliance will be. In the case of the US branch of HSBC (HBUS), the report undertaken by the government outlined how the bank's risk assessment model was fundamentally flawed by not having the appropriate level of backing and support from the governance structure (O'Brien and Dixon, 2013). Similarly, the recent HSBC case in Switzerland also highlighted how corporate attitude dictated how the bank staff approached clients and undertook, or failed to adequately undertake, risk assessments on high risk and politically exposed clients (Chittum, 2015).

AML compliance is an issue that affects all aspects of the bank's business and this needs to be emphasised and supported by governance and management if staff are to be able to deal with it effectively. In research conducted by Naheem (2015), many of the AML experts stated that all bank staff needed to be trained in AML detection not just the AML compliance unit, as it affected all areas of work. Many FIUs now produce reports outlining the kind of cases that have been reported to them and the outcomes of these investigations after law enforcement agencies become involved. The cases are offered as sanitised versions (that is, individual details and possible identifying features that could compromise further investigations or court proceedings are omitted). These are offered as typologies or scenarios that banks or other financial institutions could face and offer a potential resource for risk assessment research and auditing purposes. This article has selected three such cases from a recent AUSTRAC (2013) report to provide an example of the types of cases that are occurring in the banking sector and to provide examples of the kind of information that banks receive from sanitised scenarios.

CASE ONE – Drugs (AUSTRAC, 2013)

The first case example is indicative of the simple ML technique used for avoiding the reporting threshold of $10000 case studies repooken down into smaller amounts in an attempt to avoid raising suspicion within the bank.

The international investigation involved Australian, German and New Zealand law enforcement agencies. AUSTRAC information assisted the investigation by linking the suspects to the purchase of the drugs and the methods used to pay for and import the drugs. From the SAR the following information was reported to the FIU:

- One of the suspects sent six international funds transfers from five different branches of the same remitter over a 1-month period
- All transfers were for amounts between AUD1300 and AUD4200
- The total amount transferred was more than AUD20000
- The funds were all sent to the same beneficiary in Colombia who collected them from three different locations.

In this particular case AUSTRAC (2013) noted, 'it appeared as if the suspect may have split the funds transfers into several transactions in attempt to avoid transaction reporting requirements by establishing a number of bank accounts at various banks' (p. 50).

After the SARs had been filed and the law enforcement officers were informed, the suspects, originally from New Zealand, flew to Australia to organise the cocaine importation. They transferred funds to Colombia to pay for the cocaine, which was hidden in industrial equipment to be shipped to Australia. They also spent over AUD4000 on arrangements with couriers, mobile phones and apartments, to avoid detection. German and Australian law enforcement agencies co-operated to intercept the packages in Germany and confirm the presence of the cocaine. Listening devices were attached to the packages, which were monitored by Australian law enforcement until they were delivered to the suspects' address in Australia.

The second example also highlights how a group sought to avoid the suspicious trigger alert for high cash deposits. However, what is interesting in this case is that it was the behaviour of the clients that bank tellers noticed that raised the suspicion to investigate the accounts.

CASE TWO – Drugs in toys (AUSTRAC, 2013)

Bank staff observed the members of the syndicate undertaking a number of suspicious activities.

The suspects:

- arrived at bank branches together;
- went to separate bank tellers to conduct structured deposits;
- left the bank branches together;
- then entered another bank nearby, indicating that the suspects were undertaking structuring activities at multiple banks.

In just 4 months these accounts received 113 deposits of AUD9000 each, totalling more than AUD1 million.

In these two cases the first was tracked through suspicious transaction patterns and the second was triggered by suspicious client behaviour, which was then supported by analysing the transaction patterns. These kind of straightforward examples can be followed or detected through fairly simple tracking software, or manual examination of accounts, especially if front office staff have flagged something suspicious with the client. The next example, however, is not as easily monitored.

The third case highlights how complicated the average ML scheme can be, this time the example involves a politically exposed person (PEP) who used third parties to try and hide their involvement. Many of these third parties can be family members who are living or studying abroad as can be seen from the illustrated version in Figure 1.

CASE THREE – Corruption and PEPs (AUSTRAC, 2013)

- Individual A and Suspect B are senior politicians and both are considered PEPs.
- Individual A provides confidential information to Suspect B about the proposed privatisation of a large government entity.
- After receiving this information Suspect B persuades a close associate to buy shares in Company X on his behalf.
- Company X submits a tender for the right to purchase the government entity.
- Suspect B uses his position to improperly exert influence and favour Company X as the purchaser of the government entity.
- Suspect B indirectly benefits financially from this venture through the profits generated by Company X.
- Suspect B's close associate moves the illicit profits through his personal and business accounts.
- The funds are then given to Suspect B and/or his family as needed.
- Suspect B's wife buys a house using the proceeds of the corruption.
- The proceeds of corruption are used to pay individual A for providing confidential insider information.

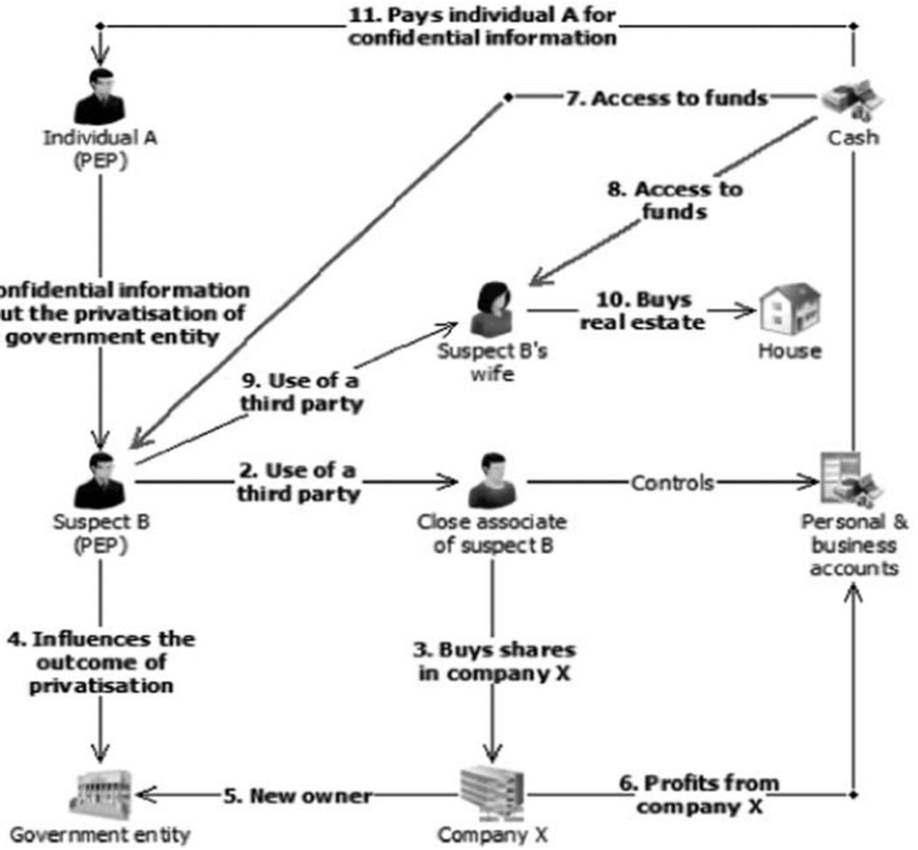

11. Pays individual A for confidential information
Individual A (PEP)
7. Access to funds
Cash
8. Access to funds
1. Confidential information about the privatisation of a government entity
10. Buys real estate
House
Suspect B's wife
9. Use of a third party
Suspect B (PEP)
2. Use of a third party
Close associate of suspect B
Controls
Personal & business accounts
4. Influences the outcome of privatisation
3. Buys shares in company X
Government entity
5. New owner
Company X
6. Profits from company X

Figure 1: Use of third parties to launder the proceeds of corruption reproduced from AUSTRAC (2013).

All three cases are designed to illustrate that the financial transactions are only one element in a law enforcement investigation to track down criminal activity. ML usually hides a number of other predicate crimes such as drug smuggling, corruption, terrorism or human trafficking as some examples. However without the financial data many investigations are not possible.

The challenge to banks is twofold:

- Many banks do not have the resources to undertake major investigations into potential criminal clients
- Most banks do not have the skills to undertake this level of data tracking or financial crime detection

The final challenge is perhaps more contentious, in that many banks do not feel that this is their responsibility to undertake investigations on behalf of the law enforcement or state agencies (Naheem, 2015). This is different to supporting law enforcement efforts. If for example law enforcement agencies have established potential clients that are deemed suspicious and they have the relevant legal search permissions and warrants, then they can deploy their own forensic auditors to work alongside the bank. However, for the bank to detect the information first is often seen as more challenging and resources intensive, especially as ML methods are constantly changing.

The evolution of ML techniques

ML techniques are constantly evolving especially as banks and other financial institutions start to monitor transactions more closely within their systems. This along with the increased availability of forensic auditing skills within law enforcement agencies means that criminals have adapted the way in which they are laundering money through the financial services sector and are constantly trying new approaches and services. The traditional method of using large cash deposits has largely been reduced, as these are known to trigger alerts within the bank (anything over $10 000 in the BSA, 1970). Instead other ways have been developed to achieve the same ends, that is, depositing large cash sums while managing to disguise the process. Systems such as 'smurfing' or structuring of funds into smaller amounts have been largely recognised within red flag alert systems in banks, whereby criminals use a number of foot soldiers to deposit small amounts of money at different branches and then either place the money in the same account or at a later stage electronically transfer the money into one account. In order for the bank to detect this process they would have to know the destination account and/or be able to monitor it for a series of smaller transactions entering close together and amounting to a large sum within a very short period of time.

However even these systems have evolved into far more sophisticated processes that seek to merge the placement, layering and integration methods into an advanced business model. Criminals, by using their knowledge of the financial services and often employing accountants and former bank employees, can easily mask the entry points for the illegitimate cash. They can produce a combination of transactions often made through legitimate business deals, of both cash and non-cash exchanges, to enter and integrate the money quickly into the financial system. These exchanges can include purchasing life insurances, trading and shipping goods and owning multiple businesses in different jurisdictions. For example, consider the example shown in Figure 2 (AUSTRAC, 2014) where the level of sophistication in ML, as can be seen from this example, can potentially be quite high. In this example four different countries are involved and three different companies in order to evade paying tax in Australia.

The future of banking

In order to develop an adequate risk assessment approach to detect ML, there is also the need to consider future risks within this ever-changing landscape. Banking products are changing and also the way in which clients use the services being provided is changing. In particular remittance systems that enable cash transfers across different countries have become cheaper, faster and easier to use, and in 2014 represented an estimated market worth of $436 billion to developing countries (Rather *et al*, 2015). Banks are also starting to use social media platforms as a means to conducting remittance services and future risk assessment strategies need to be cognisant of the opportunities these services provide for ML.

The question then is 'how advanced are the financial services sector at capturing and checking all these types of transactions?'.

ML SOLUTIONS

ML is thus a complex problem that is constantly able to change its appearance depending on the creativity of the criminals using it. From the discussion so far there are three main areas of concern that ML solutions need to address.

1. One of the major problems facing banks is the ever-increasing knowledge gap between the bank's awareness of financial crime and the criminal's knowledge of ML schemes. In particular this has become part of the problem in developing an appropriate and responsive risk assessment model across the global banking sector, as the ML models being used are constantly being adapted to respond to new local regulations.
2. The second problem is the globalisation of financial transactions and the speed of technology and electronic transfers that has effectively speeded up ML processes.

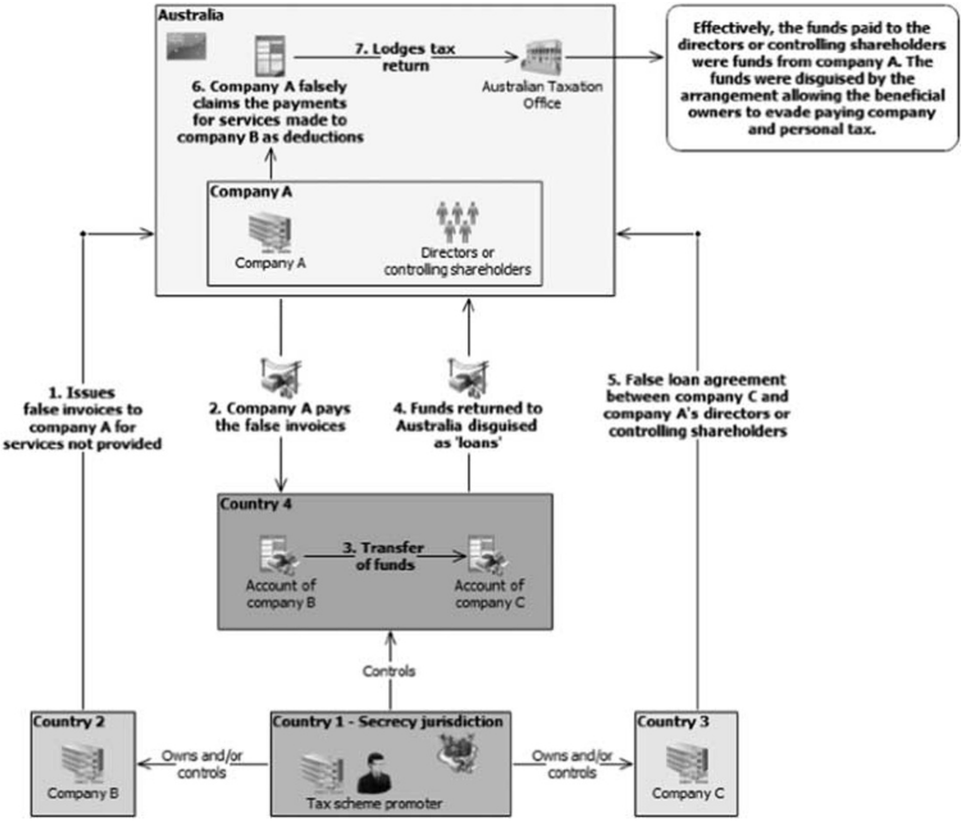

Australia
7. Lodges tax return
6. Company A falsely claims the payments for services made to company B as deductions
Australian Taxation Office
Effectively, the funds paid to the directors or controlling shareholders were funds from company A. The funds were disguised by the arrangement allowing the beneficial owners to evade paying company and personal tax.
Company A
Company A
Directors or controlling shareholders
1. Issues false invoices to company A for services not provided
2. Company A pays the false invoices
4. Funds returned to Australia disguised as 'loans'
5. False loan agreement between company C and company A's directors or controlling shareholders
Country 4
3. Transfer of funds
Account of company B
Account of company C
Controls
Country 2
Company B
Owns and/or controls
Country 1 - Secrecy jurisdiction
Tax scheme promoter
Owns and/or controls
Country 3
Company C

Figure 2: Method of using false invoices to launder funds and avoid taxes reproduced from AUSTRAC (2014).

3. The third problem linked to the globalisation of banking is the need for an international response to ML (Arnone and Borlini, 2010), as a weak entry point within a financial institution in one country can easily become a gateway into the US or European banking structures.

ML knowledge

The knowledge about different ML schemes is constantly being expanded, as criminals invent or try out new schemes in an attempt to foil regulation and banking inspections. The banking sector is constantly behind this information flow because it is only aware of schemes that have been thwarted and only then they are able to use the information when the details can be analysed. However despite the constant update of typologies from FIU reports and regulator guidance, many banks are still a long way behind implementing even basic guidelines. In the recent HSBC Swiss bank whistleblower accounts in the media, the HSBC bank were still dealing with businesses known to have connections to illegal arm smuggling and diamond smuggling (ICIJ, 2015) and had only introduced in the last 5 years a system for reporting transactions over $10000.

Globalisation of transactions

One of the factors that has assisted ML and the international transfer of illicit funds is the increasing speed of technology. This coupled with the advancements that have been made in mobile payment and remittance systems (G20, 2014), means that the banking landscape looks very different today compared with the beginning of 2000, when some of the first publications describing the use of AML tools were published. Many business clients are operating both within the formal sector and also using external banking and financial services. This means that some account information will be harder to trace, and even though technology such as Bitcoin has an open ledger system still large sums of money can be moved within seconds and tracing the destination can be difficult (Simser, 2015).

International response

The international nature of most large organised crime means that multiple jurisdictions are often involved in ML cases, and transactions occur across a number of banks and other financial institutions. This means that the transaction patterns that appear in any one bank are possibly only a small part of a much larger pattern of global ML behaviour. Although FIUs have already started working at an international level to co-operate and share data and intelligence, there is not necessarily the same level of co-operation in existence between banks or across different country offices of the same bank. This leaves a potential gap in the legislative frameworks and financial intelligence between countries, that criminals are exploiting in a phenomenon known as 'forum shopping practice' (Arnone and Borlini, 2010, p. 228), whereby criminals manipulate the gaps between different local legislations to their own advantage.

An industry-based response

Owing to the nature of international ML challenges, an industry wide response is needed in order to develop an appropriate risk assessment strategy. This risk assessment process needs to encapsulate the problems across the whole industry and to capitalise on all the available knowledge and skills within the sector. The first stage in this process has been achieved through research that was undertaken recently on TBML and risk assessment (Naheem, 2015). This research asked a range of industry experts, working within the banking and financial services sector, what in their opinion needed to change in order for banks to effectively detect TBML activity. Some of the areas that they suggested that needed to be developed further are listed below:

- *Technology* – Although the automation of complex ML risk assessments was not recommended (or deemed possible at this stage), there were areas that technology could enhance in the detection and monitoring of potential TBML and ML activity.
- *Risk Assessment* – There was concern that a lot of risk assessment processes were too simple and merely tick box exercises. Risk assessment needed to become more relevant and risk specific to both the client's business and the country of trading for export or import businesses.
- *Training* – This was seen as a large area of work and needed to include all staff in organisations, undertaking at least basic ML awareness training. Front office staff and those interacting with new client applications or reviewing existing client files needed to be particularly aware of the latest AML risks.
- *Governance* – The experts stated that governance systems needed to fully understand the risks that AML compliance posed to the future business of the bank and needed to ensure that the resources and training opportunities were provided to all relevant personnel. Audits both internal and external needed to assess the suitability of the risk assessment models being used and to make recommendations for improvement rather than merely ticking that a system was in place.
- *Financial Crime Auditing* – It was clear from the expert feedback that there is a clear difference between AML compliance and AML auditing. Although these two areas are not necessarily distinguished in any of AML training or discussions. The skills required of

an internal or external auditor need to be focused on analysing risk assessment frameworks and systems, and ensuring that they are effective and efficient for the purpose that they have been prescribed. This is a change from the auditing processes normally undertaken, which tend to be check lists to determine whether a risk assessment process is in place or not.

In Naheem's (2015) research these results were analysed and then applied to the development of a simple risk assessment framework and from there a risk assessment tool. This tool builds upon some of the systems already present within banking structures today, but it changes the emphasis of how it is applied.

Risk assessment framework

The research conducted recommended that the first stage to developing an appropriate risk assessment tool was to establish a risk assessment framework. The framework was needed to incorporate a number of additional elements that many of the experts stated were currently lacking in many approaches to risk assessment that they had witnessed within the sector. The framework was described as consisting of three layers or tiers:

Tier one – Resources and Governance
Tier two – Risk Assessment Tool
Tier three – Research and Technology

Tier one – Resources and governance

In the research many experts highlighted how working with a lack of resources, including access to appropriate levels of training, was a major impediment to a successful AML system. This was coupled with the fact that there was limited support available from the various pillars of the governance structure, including the audit committee. They stated that if AML compliance is not considered a high priority within the bank at this level then securing the appropriate resources and training skills will become very difficult to achieve.

Tier two – Risk assessment tool

This tool has been described in the next section and incorporates four areas of risk: geography, client, transaction activity and third-party influences.

Tier three – Research and technology

The final tier underpins much of the work of the risk assessment tool. This includes the use of technology to assist in research or monitor account activity, which needs to be worked alongside robust research strategies. The research focus should include reviewing current political and economic difficulties in countries that clients are working with, accessing trade data databases and analysis reports where needed, to check pricing and possible falsification of trade finance documents. It is also an area that all staff need to be involved in, including front office staff interacting with clients and reporting possible suspicious behaviour, through to business units concerned with unrealistic or suspicious business plans.

The three tiers are also an important framework to be considered by auditors, because the absence of any one of these areas will have a detrimental impact on the ability of the bank to undertake its AML compliance work effectively. The research suggested that AML auditing should be developed within the bank and this framework can also be used to facilitate internal audit reports to the audit committee and governance structure.

Developing an appropriate risk assessment tool – Tier two

The main tool that many banks use to determine AML risk is through a simple risk matrix, that looks at both client behaviour and also transaction patterns for clients. However, the model works from the presumption that ML operates in isolation, that is, there is one main client account, and that ML activity can be spotted through simple transaction patterns. This system has its weaknesses for being too simplistic and working from an unfounded assumption about how the client is involved in ML activity. Alongside that the main risk matrix tools and check box lists have been heavily criticised as an ineffective risk system, because of their inability to be responsive or specific to the context in which they are being applied (Soudijin, 2014).

Instead of this 'rules-based approach' to risk (Simser, 2012) another system known as a 'RBA' has been promoted by FATF (2012), which encourages a more responsive approach to risk assessment; although the specifics and guidelines of what this entails have not always been as forthcoming from FATF as a means to support the banks to develop this system (Soudijin, 2014). The downside to a fully RBA is that it requires an in-depth level of understanding of the topic and current empirical data has suggested that these levels of skills are not yet present within the banking and financial services sector at the moment. Therefore, an adapted form of risk assessment is needed that can provide the surety and guidance of a rules-based approach and yet can also be flexible and situation specific.

The research that Naheem (2015) developed also reviewed many of the current red flag indicators for ML activity and some of the specific TBML red flags suggested by FATF (2006). The research questionnaire had highlighted that although there were many red flags developed for detecting ML, it was almost too much information for a risk assessment process to utilise. The research sought to classify the indicators and seek a pattern that might assist in presenting the red flag information in a more constructive and user-friendly format. This was first of all achieved for generic ML activities through using the indicators supplied through the AUSTRAC reports. The model was then applied to TBML-specific indicators using the FATF (2006) suggestions to see if they followed the same classification process. The research identified that the indicators were all linked to four main headings, which were:

- Geographic Risk Indicators
- Client Behavioural Risk Indicators
- Client Transaction Risk Indicators
- Third-Party Risk Indicators

These four headings have been explained in further detail below.

Geographical risk

The nature of global banking means that every client is potentially engaged in business with another country, and therefore the bank is at risk of providing money either directly or indirectly to countries that are blacklisted, or supporting the entry of products that are blacklisted by those countries. Under this category there are also indicators linked to international transfers, shipping routes, as well as countries of trading and locations of business parties or third-party connections.

This is probably the area of greatest change for bank's risk assessment processes. It does involve more research initially but obviously once a country's risk status has been researched then that information can be used with all clients involved. Research needs to be ongoing to monitor media and other reports such as UN updates on products or countries in civil unrest. However it is no different to traditional risk research into companies and investment options, the focus of the research is slightly different and would need a researcher competent in political and financial risk analysis. Alternatively certain FIUs may already have collated some of this information and it could be made available to bank research units (or trade finance units) as required.

Client behavioural risk

Client risk has tended to focus on obvious data verification methods such as establishing identity and credit history. However, many clients are either using falsified documents or using legitimate clients and businesses as fronts for their criminal activities; therefore, standard CDD checks are not necessarily picking up on this level of fraudulent behaviour. Suspicious behaviour such as making multiple deposits into different branches, evading verification checks and being reluctant to provide information on clients or business partners are all indicators of suspicious behaviour that needs to be documented. Front office staff who deal with customers are often most likely to witness any of these behavioural traits, and therefore a system for filing alerts internally at this level would need to be developed.

Client transaction risk

Transaction risk is the one area where automation and technology may be introduced, to enable computers to trawl through data-seeking anomalies or sudden changes in transaction patterns. However, the programmes still need to be informed by human observations and data analytic software needs to be developed specifically to seek out trade patterns that could be risk related. Currently, the standard indicators of ML activity relate to examples such as the structuring of funds through micro deposits to avoid detection. However, finance trade patterns also need to focus on possible under and over invoicing through price misrepresentation activities, and complex financial transactions involving multiple accounts and different jurisdictions.

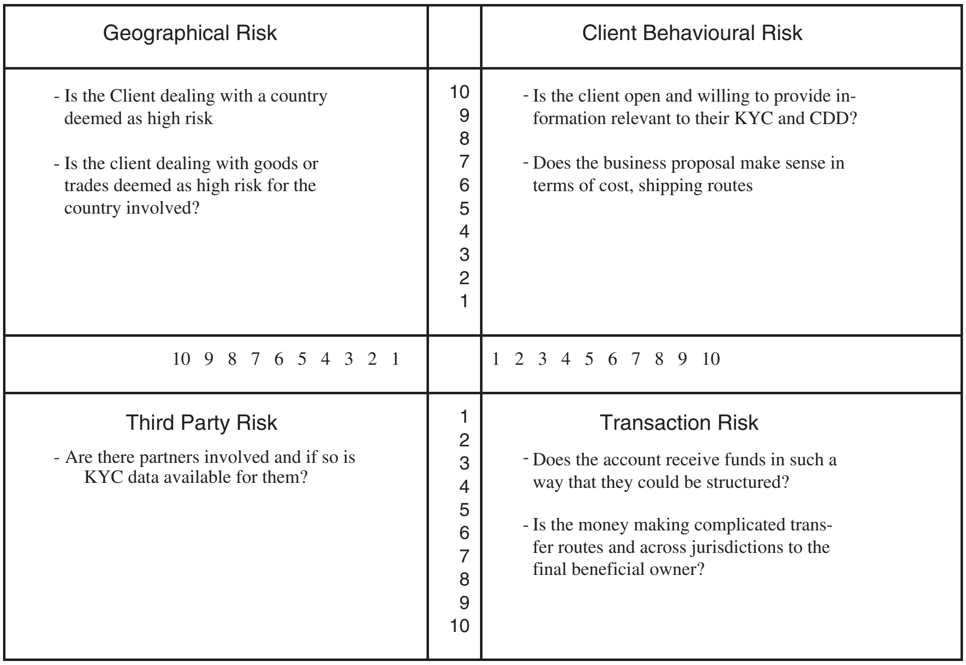
Third-party risk

This is also a new area of risk assessment and links into the increased focus on beneficial ownership of companies and transactions. It has become increasingly evident through FIU reports and media coverage of banking cases, that many clients are hiding their trading activity through the use of third-party businesses and people. Illicit financial flows from developing countries into the Western economies often involve PEPs (Kar and Freitas, 2013). These PEPs know that they will be checked through enhanced due diligent systems and so they use third-party members and friends to hide the source of the money (AUSTRAC, 2013). Sometimes criminal organisations will also approach legitimate business owners for them to undertake financial transactions on their behalf and avoid CDD checks. This means that the bank CDD process also needs to incorporate the analysis of key beneficiaries within the business and to verify ownership information. It is often through this process that suspicious client behaviour may come to the fore, as the client becomes uncomfortable with the process.

Risk assessment matrix

Naheem's (2015) research reviewed the standard risk matrix model used in ML assessments and considered using this as a starting framework, but proposed a number of additional changes. In the original risk matrix model, the client behaviour and account transactions were viewed as the two main components of the matrix. Assessments were made as to whether the client was deemed as high or low for each area. This produced four possible outcomes for each assessment: Low (low for both), High × 2 (for either client or transaction) or Very High (high for both). However if this matrix is expanded further, to incorporate two additional components, namely, geographical risk and client partner risk, then this will provide a different style of outcome as shown in Figure 3.

If a traditional risk rating was applied, for each of the four areas of the risk assessment model on a scale of 1–10, this would lead to four scores marked on the matrix. The next stage is to draw a simple line between each of the rated points on the four axis and this would produce a shape in the middle of the risk assessment matrix around the centre cross. How far out the shape expands would depend on the rating for each sector, so four axis × 10 rating would be the maximum or very high risk score and would produce a shape covering the four outer sides of the matrix. At the other extreme, four × 1 ratings would produce a small square in the centre and most of the matrix



Geographical Risk		Client Behavioural Risk
- Is the Client dealing with a country deemed as high risk - Is the client dealing with goods or trades deemed as high risk for the country involved?	10 9 8 7 6 5 4 3 2 1	- Is the client open and willing to provide information relevant to their KYC and CDD? - Does the business proposal make sense in terms of cost, shipping routes
10 9 8 7 6 5 4 3 2 1		1 2 3 4 5 6 7 8 9 10
Third Party Risk - Are there partners involved and if so is KYC data available for them?	1 2 3 4 5 6 7 8 9 10	Transaction Risk - Does the account receive funds in such a way that they could be structured? - Is the money making complicated transfer routes and across jurisdictions to the final beneficial owner?

Figure 3: Risk matrix (Naheem, 2015).

would remain outside of this space indicating that it was a low risk score.

Instead of a High/Low outcome there is now a pattern graphically depicting the amount of risk this client and the business is to the bank. The four quadrants are four completely separate risk assessment areas that can be reviewed in more detail through further research, interviews and analysis of account data. The scoring provides a simple means of communicating the risk to other staff in the bank, as well as highlighting the areas for further analysis if required.

Risk assessment applied to new methods of ML

One challenge that faces ML risk assessment is the constant adaptation that criminals will make in order to conceal their activities. As a test for this new risk assessment tool, the next section of the article will consider the implications of the latest set of red flag indicators for virtual and digital currencies.

Virtual currencies are perceived as one avenue in which money launderers will use in order to move funds without detection.

> Virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanction evaders to move and store illicit funds. (FATF, 2014, p. 5)

However the 2014 report by FATF only developed guidance as far as agreeing common definitions, associated with virtual and digital currencies, it did not actually provide any red flag indicators. The AUSTRAC (2014) report only had two indicators related to digital currencies, which were already included in Naheem's research, these were:

- Increase over time in the value of transactions with a digital currency exchange
- Multiple low-value international funds transfers

The UNODC (2014) report is perhaps the only detailed list of case studies specifically focused on digital and virtual currencies. They also provide a detailed breakdown of the major components of virtual currency crime and they predict that it will continue to grow and expand as a ML tool.

> Virtual currencies therefore can act as an enabler for the creation of new laundering methodologies. It is reasonable to expect that criminals will continue to evolve their techniques for laundering crime proceeds using virtual currencies and other techniques. (UNODC, 2014, p. 75)

The report is aimed at law enforcement and financial intelligence investigations and so some of the indicators are probably outside the bounds of the banking sector. Some examples of the indicators that they provide are as follows:

- Large number of bank accounts held by the same virtual currency administrator or virtual currency exchange company (sometimes in different countries) apparently being used as flow-through accounts (may be indicative of layering activity), without a business rationale for such a structure
- Virtual currency administrator or virtual currency exchange company located in one country but holding accounts in other countries where it does not have a significant customer base (unexplained business rationale, which could be suspicious)
- Back and forth movement of funds between bank accounts held by different virtual currency administrator or virtual currency exchange companies located in different countries (may be indicative of layering activity as it does not fit the business model). The volume and frequency of cash transactions (sometimes structured below reporting threshold) conducted by the owner of a virtual currency administrator or virtual currency exchange company do not make economic sense

The fundamental challenge of these indicators is if the multiple accounts are held with different banks. This makes it very difficult for front office staff in one bank to be aware of suspicious behaviour of the client unless they begin to detect that the client is using another account.

ML SOLUTIONS

The focus of the article so far has been to highlight the many challenges facing the banking industry and many other financial services across the globe in relation to tracking and monitoring ML activity. In order for the industry to move ahead on this issue a number of factors need to be addressed, and the overall approach to detecting ML activity needs to be updated. From the research answers and reading other relevant literature, most suggestions for risk assessment development can be classified under a number of key strategies. However regardless of the current level of development that a bank's AML compliance system is at, most of these solutions listed below require some level of investment in order to enhance and update the risk assessment strategies currently in place.

Learning from criminal behaviour

The obvious place to start to learn about ML activity is from the criminals who perpetuate such activity. There are a number of typology reports (AUSTRAC) and FIU findings (ctif cfi, 2013) that highlight the current systems being used by criminal organisations to launder money into Western banks. In the research by Naheem (2015) there were several suggestions made in relation to the quality of training programmes being delivered on TBML and AML detection, and a recommendation was made to incorporate current typology cases within these. In addition other interested parties such as the UNODC and law enforcement agencies across the globe are also beginning to develop their own typologies and case studies relating to ML activity. All of these resources should be utilised by external training agencies and bank AML compliance and research staff.

The easiest way in which to acquire this information is through tailored training programmes that suit the level of expertise already present within the bank staff. Alternative suggestions in Naheem's research from industry experts also included developing industry forums similar to the ACAMS chapters in the United States.

Investigation skills

Staff risk assessment processes are becoming more aligned to criminal profiling or 'risk profiling' rather than risk assessment. Profiling acknowledges the client behaviour from a psychological as well as an observational stance (Collins, 2015). It uses this insight to analyse the trading patterns and requests for trade finance, being presented to the bank through the client's business plans and transaction history.

There are those who feel that this level of investigation skill is beyond the scope of the bank (Naheem, 2015), but others are more supportive. Especially those who share the view that AML compliance and risk assessment need to radically change their approach if they are to have any chance of solving many of the current ML and financial crime problems. A closer working relationship with local law enforcement agencies might encourage an exchange of tips and tricks, that bank staff can incorporate into their own risk assessment processes.

Regulation as a response not the solution

There have been a number of pieces of research, which highlight that increased regulation is not a sustainable solution for tacking AML compliance issues within banks by itself (Macey, 1991; Pellegrina and Masciandaro, 2008). In fact increased regulation can cause criminals to move to weaker areas of the globe, or to develop more sophisticated ML schemes (Ferwerda *et al*, 2011), which are harder for law enforcement agencies to detect and follow in their investigations.

Ideally perhaps regulation should be a guide to support and raise the standards of AML assessment across the banking sector. This means that banks need to develop their own proactive approaches to assessing risk, rather than waiting for the regulator to take decisive action through court cases and industry fines. The appropriate legal structure also needs to be in place internationally if regulation is to be effective. This would enable the legal structure to act as a mechanism that encourages appropriate risk reporting to FIUs and then onto law enforcement agencies for investigation.

Technology

There are a number of technology solutions available to banks to help manage their large data analytics. However, trade-specific algorithms have not really been developed at the moment, although some trade price databases are available (Zdanowicz, 2009) to assist bank staff in their research. However similar to the point made on regulation, the use of technology is part of an overall response, it cannot be relied upon as the solution. It could be used in association with a risk model such as the matrix in the previous section, which highlights potential areas of weakness for each client. That way technology can be used to search for specific knowns about a client or transaction pattern and to search for selective data, such as geography, trading routes and so on without having to subject every client account to a full database search. The latter point is time consuming for all involved and with so much data to analyse could be of limited use overall.

International co-operation

The Belgium FIU stated in its 2013 report that a number of foreign FIUs were approached throughout their work in order to seek clarification on data or to further research suspicious cases; as an example the top six countries that they regularly referred to were listed as follows:

- Luxembourg 177
- France 108
- The Netherlands 71

- The United Kingdom 19
- Germany 10
- Spain 10

There is increased recognition that an international response to ML is what is really required and that without this criminals will simply exploit the gaps in the different jurisdictional systems (Arnone and Borlini, 2010). Some authors have suggested that increased investment needs to be targeted at intelligence analysis units and law enforcement rather than increased regulation (McCarthy *et al*, 2014), although in-house banking intelligence also needs to be developed otherwise the reports will not be generated within the bank to send to the intelligence units.

CONCLUSION

This article has considered some of the issues surrounding the global ML industry and tried to explain some of the challenges and complexities from the financial landscape, in which banks are trying to operate. Part of the problem is undoubtedly a slow response from the banking sector to realise the impact that crimes such as ML can have on their business. However, a number of other factors are emerging as challenges to the sector and there have been calls for a major overhaul of the regulatory and compliance sectors in order to address many of these issues (Soudijin, 2014).

Included among these concerns is the rapid escalation of the technology and mobile payments markets. This has brought with it a variety of challenges such as the anonymity of client transaction history, the time needed to trace virtual currency transactions and the speed at which large amounts of money can be transferred across the globe. In addition to the more known and probably more straightforward methods of abusing the financial system for criminal means, there are now added complications of many clients having access to anonymous and unregulated transfer systems alongside their use of the formal financial sector.

Risk assessment

This article has considered a new approach to risk assessment that may well be of benefit to the financial sector in the future. Underpinning this approach is the need to consider four areas of risk for each client instead of the traditional two factors. The increased global nature of money transfers and the increased use of third parties and hidden beneficiaries means that these elements need to become standardised in risk assessment processes.

The main weakness in any risk assessment tool is the failure of the staff involved to complete it properly. The tool mentioned in this article is no exception to this and the greater the level of research and analysis, the more realistic the risk assessment score will be. However even with no real research, the collective risks of geography, beneficial ownership, as well as suspicious client behaviour and transaction anomalies will be included and this at least provides a starting point upon which to build a more informed picture of the overall client risk.

Future work

There is evidently a lot of research and discussion that needs to occur on risk assessment and AML compliance within the banking sector. The ML sector is evolving quickly and banks need to be able to keep ahead of any developments related to their sector. This can only occur if academics and industry experts continue to work together and co-develop research projects and practical empirical literature to keep the industry up-to-date. There is also the need to pilot the risk assessment tool developed by Naheem (2015) and to monitor its success so that it can be developed further to meet the specifics of various players across the financial services sector.

ACKNOWLEDGEMENTS

The author acknowledges being the recipient of a research grant awarded by Princess Ālae as part of Seven Foundation's '2020 Banking

Vision – building banks of the future' and he thanks her for the continued support and motivation both to himself and other students who benefit through her generosity (www.sevenfoundation.ch). The author also thanks Professor Muhammad Jum`ah (a leading economist of this era based in Damascus), who has continued to provide valuable input both through his teaching of the science of economics and for his continued guidance.

REFERENCES

Arnone, M. and Borlini, L. (2010) International anti money laundering programs. *Journal of Money Laundering Control* 13(3): 226–271.

AUSTRAC (2013) Typologies and case studies report. Australian Transaction and Analysis Centre, http://www.austrac.gov.au/sites/default/files/documents/typ13_full.pdf, accessed 17 July 2015.

AUSTRAC (2014) Typologies and case studies report. Australian Transaction and Analysis Centre, http://www.austrac.gov.au/sites/default/files/typologies-report-2014.pdf, accessed 17 July 2015.

Chittum, R. (2015) Diamond dealers in deep trouble as bank documents shine light on secret ways, http://www.icij.org/project/swiss-leaks/diamond-dealers-deep-trouble-bank-documents-shine-light-secret-ways, accessed 20 February 2015.

Collins (2015) Online Dictionary definition Criminal Profiling, http://www.collinsdictionary.com/dictionary/english/criminal-profiling, accessed 5 May 2015.

ctif cfi (2013) Belgian Financial Intelligence Report. Brussels, Annual Report, http://www.ctif-cfi.be/website/images/EN/annual_report/ar2013.pdf, accessed 4 August 2015.

Durrieu, R. (2013) *Rethinking Money Laundering & Financing of Terrorism in International Law*. Boston, MA: Martinus Nijhoff.

Egmont Group (2000) FIU's in action. 100 cases from the Egmont Group, Canada.

FATF (2006) Trade based money laundering, France.

FATF (2012) International standards on combatting money laundering and the financing of terrorism & proliferation. France: The FATF Recommendations.

FATF (2014) Virtual Currency Key Definitions and Potential AML/CFT Risks. Paris. FATF Report.

FATF (2015) Who We Are, http://www.fatf-gafi.org/pages/aboutus/, accessed 2 May 2015.

Ferwerda, J., Kattenberg, M., Chang, H., Unger, B., Groot, L. and Bikker, J. (2011) Gravity Models of Trade-Based Money Laundering. Discussion Paper 11–16. The Netherlands: Tjalling C Koopmans Research Institute, 1–23.

G20 (2014) G20 plan to facilitate remittance flows, https://g20.org/wp-content/uploads/2014/12/g20_plan_facilitate_remittance_flows.pdf.

Hamilton, R. (2015) Whistleblower or opportunist? The source of the data that shook HSBC, http://www.irishtimes.com/business/financial-services/whistleblower-or-opportunist-the-source-of-the-data-that-shook-hsbc-1.2096064, accessed 20 February 2015.

Homeland Security (2012) HSBC exposed US financial system to money laundering, drug, terrorist financing risks. From permanent sub committee on investigations: US Senate, http://www.hsgac.senate.gov/subcommittees/investigations/hearings/us-vulnerabilities-to-money-laundering-drugs-and-terrorist-financing-hsbc-case-history, accessed 4 August 2015.

ICIJ (2015) Swiss leaks: Murky cash sheltered by bank secrecy, http://www.icij.org/project/swiss-leaks/banking-giant-hsbc-sheltered-murky-cash-linked-dictators-and-arms-dealers, accessed 2 March 2015.

Kar, D. and Freitas, S. (2013) Russia illicit financial flows and the role of the underground economy. Washington DC: Global Financial Integrity, http://www.gfintegrity.org/wp-content/uploads/2013/02/Russia_Illicit_Financial_Flows_and_the_Role_of_the_Underground_Economy-Web.pdf, accessed 4 August 2015.

Kar, D. and LeBlanc, B. (2013) Illicit financial flows from developing countries 2002–2011. Washington DC: GFI, http://iff.gfintegrity.org/iff2013/Illicit_Financial_Flows_from_Developing_Countries_2002-2011-HighRes.pdf, accessed 4 August 2015.

Macey, J. (1991) Agency theory and the criminal liability of corporations. Faculty Scholarship Series. Paper 1716: 315–340, http://digitalcommons.law.yale.edu/fss_papers/1716.

McCarthy, K.J., van Santen, P. and Fiedler, I. (2014) Modeling the money launderer: Microtheoretical arguments on anti-money laundering policy. *International Review of Law and Economics*. doi:10.1016/j.irle.2014.04.006.

Morris-Cotterill (2002) A brief history of money laundering, http://www.countermoney-laundering.com/public/content/brief-history-money-laundering, accessed 30 April 2015.

Naheem, M.A. (2015) Trade based money laundering: Exploring the implications for global banks. PhD thesis scheduled for publication in December 2015.

O'Brien, J. and Dixon, O. (2013) Common link in failures and scandals at the world's leading banks. *The Seattle University Law Review* 36(19): 941–972.

Pellegrina, L.D. and Masciandaro, D. (2008) The Risk Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View. 'Paolo Baffi' Centre Research Paper Series No. 2008–22, 1–24.

pwc (2015) Know your customer: Quick reference guide. London, http://www.pwc.com/gx/en/financial-services/publications/anti-money-laundering-know-your-customer-quick-reference-guide.jhtm, accessed 4 August 2015.

Rahman, A.A. (2013) The impact of reporting suspicious transactions regime on banks: Malaysian experience. *Journal of Money Laundering Control* 16(2): 159–170.

Ratha, D. *et al.* (2015) Migration and remittances: Recent developments and outlook – Special topic: Financing for development, http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationandDevelopmentBrief22.pdf, accessed 4 August 2015.

Simser, J. (2012) Money laundering: Predicate crimes, laundering techniques and the AML response. Emerging Issues 6195: Matthew Bender & Company.

Simser, J. (2015) Bitcoin and modern alchemy: In code we trust. *Journal of Financial Crime* 22(2): 156–169.

Soudijn, M. (2014) A critical approach to trade-based money laundering. *Journal of Money Laundering Control* 17(2): 230–242.

Takáts, E. (2007) A theory of "crying wolf": The economics of money laundering enforcement. Ana Lucia Coronel. IMF Working Paper.

UNODC (United Nations Office on Drugs and Crime) (2011) Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes, Vienna, https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

UNODC (United Nations Office on Drugs and Crime) (2014) Basic manual on the detection and investigation of the laundering of crime proceeds using virtual currencies.

Yeoh, P. (2014) Enhancing effectiveness of anti-money laundering laws through whistleblowing. *Journal of Money Laundering Control* 17(3): 327–342.

Zdanowicz, J. (2009) Trade based money laundering and terrorist financing. *Review of Law and Economics* 5(2): 855–878.

FURTHER READING:

Naheem, M. A. (2015) AML compliance – A banking nightmare? The HSBC case study. International Journal of Disclosure and Governance, advance online publication, May 21, 2015; doi:10.1057/jdg.2015.5.

Naheem, M. A. and Hakam, S. S. (2015) Allegations of bribery and corruption in FIFA – are there implications for the banking sector? *Finance Regulation International* 18(5), http://www.financialregulationintl.com/financial-crime/allegations-of-bribery-and-corruption-in-fifa–are-there-implications-for-the-banking-sector-109228.htm.

Naheem, M. A. (2015) Trade-based money laundering among biggest banking risks. Complinet (Thomson Reuters), http://www.complinet.com/global/news/news/article.html?ref=177933, accessed 27 May 2015.

Naheem, M. A. (2015) Suspicious transaction alerts in AML: the Credit Agricole case. Complinet (Thomson Reuters), http://www.complinet.com/global/news/news/article.html?ref=179394.

Naheem, M. A. (2015) FIFA case highlights need for new PEP, client-risk criteria. Complinet (Thomson Reuters), http://www.complinet.com/global/news/news/article.html?ref=179959.

Naheem, M. A. (2015f) HSBC Swiss bank accounts-AML compliance and money laundering implications. *Journal of Financial Regulation and Compliance* 23(3): 285–297.