Renovating your suspicion reporting

The legal implications of the Government’s sweeping new reporting requirements

Reporting suspicions
Joe Garbutt busts some myths

Systems technology
Acquiring anti-money laundering technology is not a simple decision

Asia-Pacific insight
Singapore

Special report
Riggs Bank
The Government’s new anti-money laundering (AML) legislation is upon us. At KPMG, we can help you assess clearly and pragmatically the impacts for your business.

Our team of AML professionals offer deep knowledge and practical experience in helping financial services organisations, just like yours.

We can help you assess the money laundering and financing of terrorism risks faced by your business – and more importantly how to address them.

Our team can assist in the design and implementation of new policies and processes, systems selection and integration advice and staff training.

We have worked with leading financial institutions, globally and in Australia, in areas such as money laundering and terrorist financing risk reviews and developing AML processes, policies, training and technology. It all translates into more focused, up-to-date and relevant advice for your business.

So when it comes to understanding the new AML legislation, contact the professionals in the know – KPMG Forensic.

kpmg.com.au
The next mile post on the AML journey is the release of a revised version of the draft AML Bill and Rules. This is due by 27 May. The revised Bill and Rules will reflect input from the joint industry-government working groups that have been reviewing the original draft of the legislation for the past 5 months. In this process, many practical issues have been raised and discussed.

A small focus group has also been reviewing the legislation line by line. It’s hoped the end result will be final legislation that meets the Government’s policy objectives while proving workable for the finance sector.

When the revised Bill and Rules are released at the end of May, this will be the first time we see the legislative package as a whole. In spite of the efforts that have been made by government and industry so far, it’s likely there will still be new and outstanding issues to be dealt with.

We will have just one month to do this before the Government brings down the shutters on the consultation process.

The legislation will be introduced to Parliament early in the Spring session which starts in August and the Government intends to have it passed by the end of the year. It will again be submitted to scrutiny by the Senate Legal and Constitutional Committee where industry will have a chance to raise any remaining concerns.

Decisions about the start date and the length of the implementation period have not yet been made – these will be up for discussion when the final shape of the legislative package is known.

Issues on which discussions are presently still underway include two key Rules dealing with the identification and verification of customers and the ongoing monitoring and reporting of suspicious transactions. The treatment of domestic funds transfers, which shift the bulk of money in Australia, and relations with correspondent banks overseas are also major topics of discussion.

AFMA is playing a leading role in these consultations with members engaged in the working groups and AFMA included on the Ministerial advisory panel. We’ll continue to keep you posted on AML developments.

Duncan Fairweather
Executive Director, Australian Financial Markets Association

Turning into the home straight

Anti-money laundering
May 2006
We have the solution to reporting which minimises manual input. ASSIST//ck is a straightforward solution which produces reports in whatever format will be required for Austrac.

Experian has helped the top banks in Australia fight and prevent fraud for more than ten years. We are experts in fraud, analytics and risk-based solutions. Let us help you comply with AML reporting requirements.

☑️ Report Suspicious Activity?
We have the solution.

Experian is world leader in risk management, providing both consulting skills and software solutions to companies around the world. Experian solutions have been implemented in most major Australian financial institutions. Our products cover a wide range of credit decisioning consulting and software, Basel II compliance capabilities, AML and fraud prevention products.

Our Anti Money Laundering software is designed to automate and facilitate the monitoring and detection of suspicious activity or potential money laundering. ASSIST//ck was launched ten years ago (by Americas Software) as the pioneer in the industry and over that time the product has evolved according to market needs and new regulations. The software has been implemented in more than 150 institutions in more than 34 countries.

By profiling accounts and monitoring transaction trends, ASSIST//ck analyzes how money moves in, around, and out of a bank or other business. It systematically identifies suspect patterns of behavior, creates reports, and helps reduce the administrative burdens and costs associated with manual compliance processes.
FEATURES

6  RENOVATING YOUR SUSPICION REPORTING
In addition to considering the nature of the risk-based approach, financial institutions should also
consider the reporting requirements proposed in the AML/CTF regime. Andrew Young, Blake
Dawson Waldron takes a closer look.

10  A BALANCING ACT
Julie Beesley, Associate Director, KPMG, explores the premise, “Compliance doesn’t come cheap,
but non-compliance can cost a fortune” in the light of overseas fines.

14  SUSPICION AND INTELLIGENCE
Nick Kochan, investigative journalist and author of The Washing Machine, examines the complexities
of combating terrorist financing.

REGULARS

27  Question and answer
- Practical examples of non-electronic testing
- What checks would need to be completed for companies/
superannuation/Fund Manger companies
- Requirement to identify signatories
- Screening of employees and / or prospective
employees
- Risk ranking of ‘designated services’ under the proposed
legislation
- AML officer

18  Roundtable: Eurovision
Industry practitioners from the UK and Germany discuss
the impact of the Third European Union Money Laundering
Directive on the financial services sector

45  Profile
David Leppan, Chief Executive Officer
World-Check

Columns

43  DIY – Reporting suspicions – Let’s ‘bust’ some myths
Joe Garbutt examines the reporting of suspicions in the
first in a series of columns examining the practicalities of
implementing an effective AML program

41  Lessons learned – The Master Plan
Combating money laundering is a complex and involved
process. As practitioners grapple with new legislation, the
development of internal systems and the training of staff,
John Mair asks, “How do you ensure that what you are
doing is making a difference?”

24  Technology – Systems check
As Jim Wills, AML Business Line Manager, Searchspace
Corp. explains, acquiring anti-money laundering technology
is not a simple decision and requires homework

39  Asia-Pacific insight – Singapore
KPMG discuss the recent developments in anti-money
laundering (AML) and counter-financing of terrorism (CFT)
legislation and regulation in the Asia-Pacific region

32  SPECIAL REPORT  – Reputation damage: The price Riggs paid
David Carusso, formerly Executive Vice President of Compliance & Security
at Riggs Bank from June 2003 through to May 2005 and David Leppan, Chief
Executive Officer, World-Check examine how deficiencies in Riggs Bank’s anti-
money laundering compliance program cost the ‘bank of presidents’ over USD
189 million.
Renovating your suspicious report
Since the release in December 2005 of the draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2005 (‘Draft Bill’) and various draft Anti-Money Laundering and Counter-Terrorism Financing Rules (‘Draft Rules’), there has been much discussion about the ‘risk-based approach’ that forms an integral part of the proposed new anti-money laundering and counter-terrorism financing regime (‘AML/CTF Regime’).

However, in addition to considering the nature of the risk-based approach, reporting entities should carefully consider the nature of the obligations that will be imposed upon them by the other fundamental aspects of the proposed AML/CTF Regime – including, for example, the requirements to make reports to AUSTRAC.

In addition to requiring reporting entities to provide information to AUSTRAC on request, the Draft Bill imposes obligations on reporting entities to furnish AUSTRAC with the following types of reports:

- suspicious matter reports
- threshold transaction reports
- international funds transfer instruction reports.

This article addresses some of the legal issues arising out of a reporting entity’s obligation to provide AUSTRAC with suspicious matter reports – as that obligation is currently imposed by the publicly available (December 2005) version of the Draft Bill and Draft Rules.

**Suspicious matter reports – Draft Bill**

Clause 39 of the Draft Bill, obliges a reporting entity to report suspicious matters where:

(a) a reporting entity starts to provide, or proposes to provide, a designated service;
(b) a person requests a designated service; or
(c) a person merely inquires as to whether the reporting entity would be willing to provide a designated service,

and, at that time (or at a later time) the reporting entity has ‘reasonable grounds’ to suspect that:

(d) information it has may:

(i) be relevant to the investigation of an evasion of a taxation law;
(ii) be relevant to the investigation of, or prosecution for, an offence against a Commonwealth or Territory law (including a financing of terrorism offence);

or

(iii) be of assistance in enforcing the Proceeds of Crime Act 2002,

or

(e) the provision of the designated service is preparatory to a financing of terrorism offence.
A report must be made to AUSTRAC within three business days of the reporting entity forming the suspicion, or, if the suspicion relates to terrorist financing, the report must be made within 24 hours of the suspicion being formed.

Clearly, the circumstances in which a suspicious matter report must be lodged are more broad than section 16 of the Financial Transaction Reports Act 1988 (Cth), under which the obligation to report to AUSTRAC is limited to suspicious ‘transactions’ to which the cash dealer is a party.

‘Reasonable grounds’

Subclause 39(6) stipulates that the AML/CTF Rules may specify matters that ‘are to be taken into account in determining whether there are any reasonable grounds for a reporting entity to form a suspicion’. The current version of the Draft Rules on suspicious matter reporting sets out 24 matters that are to be taken into account in determining whether there are reasonable grounds for forming a suspicion.

Whilst the language of the regime unambiguously requires a reporting entity to take into account all of the 24 matters listed in the Draft Rules, this obligation could be interpreted such that only those of the 24 matters actually known to the reporting entity must be taken into account when determining whether the reporting entity has reasonable grounds to form a suspicion.

The reasons for this view are threefold:

(a) The obligation to report, contained in clause 39, exists even where a person merely inquires as to whether a reporting entity is willing to provide a designated service. As such, a reporting entity simply won’t have information relevant to the 24 matters – that is, a reporting entity won’t have knowledge of all of the 24 matters;

(b) not all of the 24 matters are relevant to each designated service that may be provided. For example, the source or origin of funds (Number 7 of the list of 24 matters) won’t be relevant to the issue of a debit card or a cheque book; and

(c) paragraph 10 of the Draft Guidelines to the suspicious matter rules provides that not all matters prescribed in the list of 24 will be relevant.

Nevertheless, as presently drafted, the language of the Draft Rules is somewhat unsatisfactory in that it does not expressly limit the obligation to take into account all of the 24 matters to the extent that the matters are known and relevant. This position should be clarified in the Draft Rules themselves, given that they are legally binding.

Knowledge of foreign laws?

The references in clause 39 of the Draft Bill to ‘taxation law’ and ‘law’ are clarified in clause 40. Subclauses 40(2) and (3) provide that the reference to ‘taxation law’ in clause 39 includes a Commonwealth, State, Territory and foreign taxation law. Further, subclauses 40(4) and (5) provide that the reference to ‘criminal law’ in clause 39 includes a law of a State and a foreign law that “corresponds to” a Commonwealth, State or Territory offence.

Therefore, the obligation to make a suspicious matter report exists if:

(a) the reporting entity has reasonable grounds to suspect that it has information relevant to the investigation or prosecution of a foreign criminal law that corresponds to an Australian law;

(b) the reporting entity has reasonable grounds to suspect that it has information that may be relevant to the investigation or prosecution of a foreign criminal law that corresponds to an Australian law.

This begs the question: what is the extent of a reporting entity’s obligation to know about foreign taxation and foreign criminal laws? Given that the concept of criminal law extends only to a foreign criminal law that ‘corresponds to’ an Australian law, presumably the reporting entity would only need to know about Australian law because the requirement to know foreign criminal laws is limited to those foreign laws that ‘correspond to’ Australian law. This means that a reporting entity could ask itself: ‘If the relevant conduct had occurred in Australia and not overseas, would that conduct constitute a criminal offence, and would any knowledge of that conduct have raised a suspicion?’.

On the other hand, the requirement for a reporting entity to know about foreign taxation laws is not limited to those foreign taxation laws that correspond to taxation laws in Australia. Presumably the difference between the foreign taxation law and foreign criminal law obligations in the Draft Bill was intended.

The result of this may be that the obligation for a reporting entity to know about foreign taxation laws is a far more onerous obligation than that of knowing about foreign criminal laws. If this interpretation is correct, it would impose obligations on a reporting entity that it may have great difficulties complying with.

Interestingly, Recommendation 13 of the Financial Action Task Force (‘FATF’) Forty Recommendations requires the reporting of suspicions that funds are the proceeds of criminal activities. The reference to ‘criminal activity’ in Recommendation 13 is limited by FATF’s Explanatory Notes to the Forty Recommendations to criminal acts that would constitute a predicate offence for money laundering ‘in the jurisdiction’. Interestingly, it appears not to extend to offences outside of the jurisdiction – that is, Recommendation 13 does not appear to extend to truly foreign offences, as the Draft Bill appears to do. If it was government’s intention that the requirement to lodge a suspicious foreign tax matter report be limited to those matters involving foreign taxation laws actually known to the reporting entity, this should be clarified in the Draft Bill and Draft Rules.

Certainly, given the practical difficulties caused by requiring a reporting entity to have knowledge of foreign taxation laws, it would be useful for the government to provide some assistance to reporting entities in this regard.

Content of report

Subclause 39(3) of the Draft Bill provides that a suspicious matter report must:

(a) be in the approved form; and

(b) contain such details of the matter as are specified in the AML/CTF Rules; and
always contain the information referred to in (a), (b) and (c). If the Draft Rules (in their current form) were interpreted to mean that there is such an obligation, it would follow that there would be an obligation to gather that information (taking care not to tip-off the customer) in order to provide the prescribed information. One problem with that interpretation is that it assumes that a reporting entity will have gathered the information in (a), (b) and (c) and conducted a customer identification procedure.

Of course this will not be the case in many of the circumstances in which a suspect matter report must be lodged. This is because a suspect matter report must be lodged even if a customer merely asks whether a reporting entity will be willing to provide a designated service; that is, prior to the time where a reporting entity is actually required to verify the identity of the customer. Arguably, the obligation for a report to contain a customer’s full name and address and sources used to verify the customer’s identity should only exist if this information is actually known to the reporting entity. Unfortunately the guidelines do not provide any guidance as to whether the information that must be contained in a suspect matter report must only be contained in the report if that information is known to the reporting entity. Certainly this is another aspect of the reporting regime that requires clarification.

Summary

Whilst the circumstances in which a reporting entity is required to make suspicious matter reports to AUSTRAC are undoubtedly broad, there are a number of details relating to the obligation to make such reports that require clarification in order to assist reporting entities to understand their obligations under the proposed AML/CTF Regime.

“if it was government’s intention that the requirement to lodge a suspicious foreign tax matter report be limited to those matters involving foreign taxation laws actually known to the reporting entity, this should be clarified in the Draft Bill and Draft Rules.”

Andrew Young, Senior Associate, Blake Dawson Waldron

Morning briefing:
Understanding the impact of the Government’s revised anti-money laundering Bill and Rules

Friday 28 July 2006, Sydney (9am – 12pm)

Join industry experts to examine the business and legal impact of the revised AML Bill and Rules with an in-depth analysis of KYC, monitoring and reporting requirements.

For further information or to register contact
Diana Zdrilic 02 9776 7923 or email dzdrilic@afmaservices.com
A balancing

Julie Beesley, Associate Director, KPMG, explores the premise, “Compliance doesn’t come cheap, but non-compliance can cost a fortune” in the light of overseas fines.
Some may say that compliance doesn’t come cheap; however, the cost of non-compliance is worth considering when organisations plan their approach to the proposed new Australian anti-money laundering and counter terrorism financing (AML/CTF) regime. Where organisations fail to meet the requirements of the new regime, the potential cost of non-compliance in reputational damage and hefty fines should not be underestimated. Not convinced? Then consider the following headline on the front page of a national newspaper:

‘(Insert the name of your company in bold) first to be penalised under new Australian AML/CTF regime’

In this article we explore the UK’s and US’s overseas enforcement of non-compliance penalties with money laundering regulations, as opposed to penalties levied against evidence of money laundering activity itself.

The first to fall
The first financial penalty levied by the UK Financial Services Authority (FSA) for non-compliance with UK money laundering regulations was on 17 December 2002 – just 12 months after the FSA first acquired this power on 1 December 2001. And the headline?

“FSA fines Royal Bank of Scotland GBP 750,000 for money laundering control failings.”

The fine was levied due to weaknesses in the Royal Bank of Scotland’s (RBS) AML controls across its retail network; RBS failed to obtain sufficient ‘know your customer’ documentation to establish customer identity, and/or to retain such documentation in an unacceptable number of new accounts opened.

Lessons learned
Although there was no evidence of actual money laundering having taken place, the FSA made a significant point of imposing a fine for non-compliance with the regulations. The FSA noted that:

‘This fine demonstrates that the FSA takes anti-money laundering compliance very seriously indeed.’

‘There is no evidence of actual money laundering having taken place.’

The big names keep falling
Twelve months later, the FSA fined Abbey National GBP 2 million, the biggest fine of its kind in the UK, for failing to identify its customers adequately and failing to ensure suspicious activity reports were promptly considered and reported to the National Criminal Intelligence Service (the equivalent of AUSTRAC).

Lessons learned
The FSA noted that this fine ‘reflected wider control failings, including inadequate monitoring of key regulatory risks, across the group over a prolonged period.’

Companies approached by AUSTRAC for non-compliance with the new AML/CTF regime may find that a wider regulatory framework is placed under closer scrutiny.
The overseas branch
Four months on in 2004, the FSA fined the London branch of an overseas bank, Raiffeis Zentralbank Österreich (RZB), GBP 150,000 for failing to act promptly to update its AML and compliance manual to reflect the introduction of the new money laundering rules in 2001.

Lessons learned
The FSA noted:

- The compliance manual did not include sufficient assistance to staff to enable them to comply with identification requirements for certain categories of customers.

The FSA fined RZB London for simply not updating its compliance manual on time - so pay close attention to implementation deadlines imposed by the Australian AML/CTF regime.

Across the pond
There have been a number of high-profile cases in the US for non-compliance with a range of legislation, including money laundering. The majority of high profile cases combine fines for both non-compliance with the legislation and associated incidents of money laundering activity. Of particular note is that the fines for non-compliance are far greater than the penalties incurred for the detection of money laundering activity itself. Take, for example, the cases of Riggs Bank and AmSouth Bancorporation.

Neighbours with the White house
In May 2004, the US Financial Crimes Enforcement Network (FinCEN) hit Riggs Bank, a Washington-based commercial bank, with a USD 16 million fine and five-year period of corporate probation for failing to design and implement a suitable AML program that would ensure the timely and effective reporting of suspicious activity. This was the largest penalty ever assessed against a domestic bank in connection with money laundering. While the USD 16 million fine stems from the failure to actively monitor suspicious transactions, Riggs was also investigated and fined USD 9 million for its relationship and activity with two notorious politically exposed persons (PEPs).

In deep Alabama
In October 2004, AmSouth Bancorporation, based in Birmingham, Alabama, was fined USD 50 million for failing to report suspicious transactions over USD 5,000 or more as required by US money laundering regulations. AmSouth could still be prosecuted if it fails to perform specified remedial tasks related to its AML program.

On closer inspection, AmSouth was investigated for money laundering activity and the fact that it did not file suspicious activity reports, even when it knew some of its customers where involved in fraudulent transactions or were under investigation. In other cases, AmSouth did not file because it reasoned that it suffered no loss.

Lessons learned
The most fundamental failing was the lack of a risk assessment.

According to FinCEN: ‘AmSouth failed to conduct a risk assessment of its customer base to identify high-risk customers, products, and geographic locations.’

What does this mean for Australia?
Although the new draft AML/CTF regime does not currently indicate the likely scale of penalties to be imposed in Australia for cases of non-compliance, the UK and US examples demonstrate that where evidence of non-compliance is found, regulators and law enforcement bodies have been swift to scrutinise the wider activities of the firm, entity or individual.

This indicates that the risk of non-compliance with any element of Australia’s proposed AML/CTF regime will potentially expose the firm, entity or individual to further scrutiny as to the integrity with which all elements of the regime have been implemented.

When considering the nature of your AML/CTF program, your first consideration should not be compliance doesn’t come cheap, but that non-compliance can cost a fortune.

Julie Beesley, Associate Director, KPMG:
jbeesley@kpmg.com.au:
Tel: +61 2 9335 8839
World class Anti Money Laundering and Fraud Detection solutions built on best practice

Over half of the world’s 25 largest banks use Searchspace solutions to detect fraud and money laundering.

Here’s why. Searchspace patented technology delivers:

- Detection of not only known but previously unknown suspicious behavior.
- Operational efficiency that maximizes effectiveness of fraud and AML analyst teams.
- High detection rates, minimizing the number of false positives by building behavioral and statistical profiles based on every transaction a customer makes as it happens across all lines of a financial institution’s business.
- Scalability, capable of dealing with over 50,000,000 dollar and non dollar transactions a day.
- The accommodation of rapid changes in the business such as adding newly acquired banks, lines of business, new products and customers.
- Ease of modification and tuning to reflect changes in market behavior.
- Easy integration into existing systems and capable of rapid deployment.

By sifting through every transaction and analyzing behavior in the context of the adaptive profiles, both individual and peer groups, the system automatically detects unusual or irregular activity and notifies the relevant business analysts.

‘Unusualness’ is detected via statistical algorithms, supplemented with money laundering risk assessments to ensure high-quality notifications. The system makes it easy for users to configure the parameters that define this business risk assessment, providing flexibility in setting and administering risk management policies.

Such flexibility is especially important in order to rapidly respond to today’s fast-moving regulatory and operational environment.

Searchspace monitors over 450 million accounts a day, working with community, regional, national and global banks.

For information on Searchspace call 212 422-5100, email sales@searchspace.com or visit www.searchspace.com
The role of the bank in the campaign by government and regulators against terrorist financing is pivotal, and this imperative needs to be understood at all levels of the organisation. Substantial regulatory or even criminal penalties could await any institution found to be harbouring terrorist money in its system as a result of systems failure, and the publicity surrounding those penalties could risk the institution’s very existence.

The organisation’s level of responsibility in this sensitive area is summed up by Nick Ridley, associate professor at Transcrime, University of Milan and senior associate at BakerPlatt, the anti-money laundering specialists. “The mere connection, however en passant, of a financial institution with a terrorist organisation or terrorist-linked individual can result in disproportionately disastrous results for the reputation of that financial institution. One of the major causes of reputational damage is man-made blunder. And the biggest man-made blunder is ignoring or complacency about the risk itself.”

The need to comply with terrorism-related statutes and regulations is understood and accepted by institutions. However, what is causing them concern is the extent to which they will need more systems and staff, to add to those already employed for scrutinising conventional money laundering. In other words, is compliance with the best terrorist financing standards an additional cost, even if it is also an unavoidable one, on top of the bill for anti-money laundering compliance? Unfortunately, the answer to this question is far from straightforward.

The principle of reporting suspicious transactions is common to both commercial crime and terrorist activity, and need not therefore require new systems. The same applies to the system that banks apply in consulting and running names through black lists if there is a possible suspicion. Blacklists are supplied by a number of international authorities. These include the Bank of England, whose Sanctions Unit has created a consolidated list of names of UN Security Council-sanctioned individuals and entities and individuals engaged in terrorist financing. Other key lists are published by the US Office of Foreign Assets Control (OFAC). This lists the names of individuals and entities against whom sanctions have been imposed by the US government. The United Nations, the FBI and the Federal Reserve Bank of the United States also have lists. These lists are widely published and available. A number of software companies also provide systems for searching these names online. Banks in all regulated jurisdictions are required by law to check the names of new customers (or customers where they have a suspicion) against these black lists.

The value of blacklists is weakened by two limitations. First, they can only list the names of those committing crimes in the past, ie. they cannot anticipate new names and new criminality. Second,
they are prone to throw up ‘false positives’, namely apparent matches that turn out to be incorrect. This occurs when names have multiple spellings that are easily confused.

Deception by terrorist financiers, often quite as sophisticated as their money laundering counterparts, is likely to test the competence of those compiling and applying blacklists. Apparently legitimate fronts — charitable, commercial or political — will be created to divert the attention of bank or law enforcement agency investigators.

When a bank’s checking system encounters a legitimate suspicion, it reverts to its suspicious activity reporting system. This is the conduit between regulated financial institutions (FIs) and the police and other law enforcement bodies. FIs act as the eyes and ears for law enforcement in the places where criminals and terrorists do business. The FI sends its suspicious activity report (SAR) to the Financial Intelligence Unit (FIU). The FIU is a form of post box that sifts and despatches reports to the appropriate police or law enforcement authority. Where the SAR flags suspected terrorist finance, the FIU will process and act on the report quickly.

Financial institutions will note a dramatic difference between the speed of response to the SAR that contains suspicion of money laundering and the one that indicates terrorism. Responses to a report of suspected terrorist involvement will be swift and decisive (unlike the typically — and regretfully — dilatory response to a conventional money laundering report) and law enforcement will place great pressure on the FI to provide bank account and customer information.

One bank reported that, “in the wake of an outrage, when the bank and the police were on high alert for suspected movements of terrorist money, there was no let-up. It was automatically assumed that we would work late and over weekends to comply with the requirements of the police, and of course we did.”

The speed of the response occurs for two reasons. First, and most importantly, law enforcers wish to maximise their chances of monitoring, or even seizing, the suspected individual if he seeks to withdraw money from a bank. Efficient liaison between the institution and police is critical for this to happen. The movement of suspected funds may also provide evidence of the intended purchase of materiel required for an attack, and authorities are aware that there is rarely much breathing space between a terrorist moving his money and making such a purchase.

Again, speed of response by the police or intelligence services is critical. The heightened political focus on terrorism also means that neither law enforcement nor the banks can afford to miss turning over any stone that presents the slightest chance of preventing an attack.

Banks are keen to cooperate, said William Langford, associate director for the Regulatory Policy and Programs Division at FinCEN (the Financial Crime Enforcement Network, part of the US Treasury). “Bankers are constantly saying to us, ‘help us to help you. Give us the names. If you think X is a terrorist, we will check it, and do everything.’ We may have to say, we can’t give you the name of X usually for legal and prudential reasons. All the same, we are constantly trying to do a better job of giving more information,” he said.

Financial police rarely handle a terrorist suspicion on their own. In the UK, the moment such a red flag is raised, information is initially passed to the police service’s National Terrorist Finance Intelligence Unit (NTFIU), which is expert in terrorist financing. The NTFIU then usually passes it on to the local and international intelligence services. According to one unnamed intelligence officer, “we maintain very close and regular links with the banks. They know what we want.”

These relationships are informal and have been built up over long periods. There has to be a lot of trust.” The NTFIU says it works very closely with UK intelligence services and has intelligence officials routinely seconded to its complement.

The NTFIU, which leads the fight against terrorist financing, works under the aegis of the newly formed Serious Organised Crime Agency (SOCA). It operates across the United Kingdom, comprising police officers with financial backgrounds.

The NTFIU does not disclose the size of its complement (or the names of individual officers who have assisted with this article), but says it has grown by 300% since September 11 with a strategic plan to become 10 times larger than it was five years ago. This may become possible in light of the shake-up terrorist-financing investigations envisaged by the UK Chancellor of the Exchequer.

Government agencies are dependent on the detective work of the private sector, and they happily admit it. “We know how much work the banks put into investigation on our behalf, and we are very grateful”, said one policeman from the NTFIU. “We also know that this is very difficult work, and we rely on them to come up with leads that we would never find on our own.”

“One of the major causes of reputational damage is man-made blunder. And the biggest man-made blunder is ignoring or complacency about the risk itself”. Nick Ridley, associate professor at Transcrime, University of Milan and senior associate at BakerPlatt

Nick Ridley, associate professor at Transcrime, University of Milan and senior associate at BakerPlatt
Our AML Team

Our dedicated anti-money laundering team can advise you on all aspects of the AML legislation and equip your business to deal with its impact.

Our approach is simple – we cut through the complexity of legal requirements and help you build the capability of your anti-money laundering team.

For further information, please contact:

**Stephen Cavanagh**  
Partner  
t > (02) 9258 6070  
e > stephen.cavanagh@bdw.com

**Phil Trinca**  
Partner  
t > (03) 9679 3258  
e > philip.trinca@bdw.com

**Jonathan Gordon**  
Partner  
t > (02) 9258 6186  
e > jonathan.gordon@bdw.com

**Andrew Young**  
Senior Associate  
t > (02) 9258 5881  
e > andrew.young@bdw.com

**Julian Fenwick**  
National Business Development Manager  
t > (02) 9258 6382  
e > saltinfo@bdw.com

For more information on our compliance training services contact
ROUND TABLE

ROUNDTABLE PANELISTS

- Tassilo Amtage, CC/Compliance – AML, Deutsche Bank, Frankfurt
- Paul Martin, Director, London Investment Banking Association (LIBA)
- Rob Cutler, Head of AML/NCA, UK & Western Europe, Deutsche Bank, London
In this month’s roundtable Anti-money laundering examines the affect of the Third European Union Money Laundering Directive on European financial institutions and explores the challenges they have faced implementing a risk-based approach.

**How will the Third European Union Money Laundering Directive affect European financial institutions? Will it benefit the industry – how and why?**

**John Mair, Strategy, Tactics, and Growth. Risk, Reward, and Results**

It will affect them in different ways, as they are all starting from different points, and some differ in what they are trying to achieve. If the goal of an organisation is to be effective, then the 3 EUMLD provides a greater opportunity to deploy a proportionate approach. Notwithstanding this, there will be a temptation to be overtly organised, with a well articulated risk-based approach. This sounds good, but could fail on at least two counts: beautifully articulated blueprints will enable the really serious organised criminal to better circumvent the methodology; secondly, not enough may be known about where most money is being laundered to really understand whether high risk is high risk, or whether the Maginot Line is pointing in the wrong direction.

The most effective approaches encouraged by the directive will allow for some chaos, some trial and error, and some deception in the blueprint – to mislead the organised criminals into misunderstanding the risks they run. If firms do not articulate everything about their approach, then there is less chance of the organised criminals penetrating the strategy. Unfortunately, many firms seem to feel that full articulation of their methodology gives them the best chance of ‘wowing’ the regulator – thereby giving the criminals the best chance of avoiding the hurdles. If the aim is cost limitation, then the directive initially enables firms to be more restrained with their resources. This, however, will only be as successful as events subsequently allow. The real test of a firm’s approach is likely to be made with the benefit of hindsight. Something has gone wrong, and should the firm have avoided it? The severity of the event may influence the reasonableness of the conclusions. Whatever the reaction to the 3 EUMLD, a credible approach will be essential – as tested with the benefit of hindsight.

**Tassilo Amtage, Deutsche Bank, Frankfurt**

From a German AML point of view, Deutsche Bank welcomes a great deal of the content of the 3 EUMLD. The German legal and regulatory AML level, as reflected in Deutsche Bank’s AML Policies and Procedures, already meets the standards provided for in the Directive for the most part, Deutsche Bank does not consider the Directive’s impact on German financial institutions too broad. Financial institutions have been living these standards for years and have spent enormous amounts for the fight against money laundering and terrorist financing. Deutsche Bank employs worldwide 200 members of staff mainly dealing with these subjects. The remaining concerns regarding the Directive relate primarily to the treatment of beneficial owners and politically exposed persons. Regarding these two topics, the EU Council, in its conciliation with the European Parliament, did not sufficiently take the European Banking industry’s concerns into consideration. Thus German financial institutions are facing an unworkable situation. The information as to the identity of a legal person’s beneficial owner can neither be obtained from a public register nor from the legal person itself. The definition of PEPs is far too broad and not limited to persons from third countries and people who may represent an enhanced money laundering and reputational risk.

**Rob Cutler, Deutsche Bank, London**

We believe that in the UK the impact will be less noticeable than perhaps in other EU jurisdictions. From personal experience in several major banks in the UK, the new EU Directive will not require any changes to the policies or documentary requirements apart from perhaps adjusting the percentage levels for shareholding disclosures. It is questionable whether the Directive will benefit the industry generally but may create a ‘more level playing field’ across Europe.

**Paul Martin, Director, London Investment Banking Association**

The impact of the Directive is likely to be different within each Member State and the financial institutions within those States. This is dependent upon the development and enforcement of AML and terrorist financing counter measures in those jurisdictions. The world is a relatively small place today and the larger financial institutions are global operations. These large organisations will undoubtedly have global AML and CTF policies and broadly similar implementation and operational procedures wherever they transact business in the world. For such large organisations the Directive’s requirements are not likely to cause too much change to their existing processes. However, for some smaller organisations where
human resources devoted to AML and CTF are limited the impact could be significant. So what are the areas of possible interest in this Directive? It is the first time a European Directive has mentioned a ‘risk sensitive’ approach. This is now becoming a commonly referred to term when talking about AML and compliance matters generally, but do we really know or appreciate what it means and how it is going to work in practice? Financial institutions will be able to adopt a risk-based approach to all customer due diligence (CDD) requirements under the Directive. This also reflects the FATF’s approach and is appropriate because of the wide range of sectors the Directive covers. Firms will need to consider and assess how to move to a risk-based approach – for some this will be a radical change, for others not. Europe generally has had codification of AML requirements, prescriptive requirements, and this more flexible approach may prove a test.

The Directive introduces the concepts of ‘enhanced CDD’ for high risk customers and ‘simplified CDD’ for regulated customers, listed companies, beneficial owners of pooled accounts held by professionals, domestic public authorities, EU Commission listed low-risk situations (the list is still to be drafted) and exceptions for life insurance and pensions with no surrender clauses, and e-money products and services. Firms will need to look carefully at this and formulate policy.

Of concern has been the proposals relating to the requirements for identifying and verifying beneficial owners and politically exposed persons. These have always been difficult areas, but the Directive will require all firms to reconsider their policy and processes. Reliance on third parties is an area that has been debated around the globe. The Directive has picked up on this, permitting firms to have regard to some reliance on others, but leaves the responsibility with the firm for ensuring the correctness of the information. Without an exemption from enforcement action if the reliance proves to be misplaced, who will use this reliance option?

The Directive also brings into its scope auditors, external accountants and tax advisors, notaries and legal professionals, real estate agents, trust and company service providers and casinos. These may be required for the first time to address AML issues and, furthermore, those that use some of their services such as financial institutions may have to consider how they do so in future. So what is the benefit? Legislation such as this does begin to move the industry. The noticeable change has been a steadily increasing focus on the responsibility of senior management for all systems and controls, including anti-money laundering and anti-financial crime. Fraud has now become an important issue as AML and is expected to be included under that same oversight structure, i.e. MLROs, though this has not fully crystallised.

Paul Martin, Director, London Investment Banking Association
The FSA has worked with the financial services industry to address some of the issues relating to the identification and verification of customers, especially individuals. In the UK the Joint Money Laundering Steering Group has for many years issued guidance on good practices in AML. The FSA, together with all interested parties, has assisted with a major revision of this guidance and new JMLSG Guidance was published in February 2006 (available as a pdf from www.jmlsg.org.uk) promoting the risk-based approach which is supported in the UK by the authorities. This new Guidance also for the first time sets out some sector specific guidance. Fraud has also become an issue in the UK and the authorities are focusing a lot of attention on this. Organised crime has now crossed borders and is utilising different regulations in each country to its advantage. There is more emphasis placed on co-operation between the authorities with many more memorandums of understanding/exchange of information being signed to assist in this fight against crime.

Financial institutions are facing a proliferation of regulation both at an international, European and domestic level. How should regulation be developed in the future and is there a case for international or regional harmonisation?

Tassilo Amtage, Deutsche Bank, Frankfurt
Following the September 11 terrorist attacks, governments accelerated measures to deter economic crime and particularly money laundering in order to destroy terrorist infrastructure. A long planned redefinition of the German anti-money laundering provisions was undertaken for this reason. The legislator imposed the duty on financial institutions to provide for internal business- and customer-related safeguards against their being misused for purposes of money laundering. Based on this provision, the German regulator BaFin has been focusing since then on the need for a financial institution to have an effective IT transaction monitoring system implemented. Deutsche Bank fully meets the high standards required by the German legislator as well as by the BaFin.

Rob Cutler, Deutsche Bank, London
The focus of the regulator in the UK has changed in several ways in the AML field. Post 9/11 and in the early days of the Financial Services Authority (FSA) it used to be much more prescriptive and they had a ‘tick box’ mentality, but this is now changing towards accepting a risk-based approach in applicable parts of the industry. The noticeable change has been a steadily increasing focus on the responsibility of senior management for all systems and controls, including anti-money laundering and anti-terrorist financing. Gone are the days when it is acceptable for senior management to delegate all responsibility for AML to the money laundering responsible officer (MLRO). They are expected to take an active interest in how the firm tackles money laundering and other financial crime. Fraud has now become as important an issue as AML and is expected to be included under that same oversight structure, i.e. MLROs, though this has not fully crystallised.

John Mair, Strategy, Tactics, and Growth. Risk, Reward, and Results
Some regulators may be tempted to take more interest in the quality of the safety belts, than the skill of the driver. The wisest assess the driver and ‘kick the tyres’. There can be a temptation to assess the brochure, rather than deploying the ‘so what?’ test. Impact on firms? Credibly hold the initiative, engage the stakeholders, and ask someone independent to prod the approach.

What is the current focus of local regulators, how has this changed in recent years and what impact will this have on your organisation?

John Mair, Strategy, Tactics, and Growth. Risk, Reward, and Results

20 Anti-money laundering
**John Mair, Strategy, Tactics, and Growth. Risk, Reward, and Results**

Regulation should flex. Firms should learn from mountaineers – too much risk management and the mountaineer will not be able to walk, let alone climb. Too little and a slip will be fatal. Regulators should allow firms to select their approach, but similarly should discourage complacency by putting in danger the very continuation of the firm should it fail to satisfy. This is tough on firms and regulators alike – but will be cheaper and more effective on the whole. Harmonisation of effectiveness and outcomes, but through liberalisation of method.

**Tassilo Amtage, Deutsche Bank, Frankfurt**

The fight against money laundering and terrorist financing is an international issue. Due to the proceeding globalisation, the banking industry’s business is not restricted to single jurisdictions, as financial transactions do not halt at national frontiers. On an international or at least on a European level, the need for harmonisation is obvious. Data protection and bank secrecy laws may serve as an example. The possibility to exchange data e.g. customer data or those on suspicious activity reports filed and to share intelligence information within a globally acting financial institution could be a key to better prevention. Information sharing and data exchange further an effective and sound know your customer process which is vital for money laundering prevention. Still, the harmonisation of laws and regulations can result in inflexible and locally impractical laws as local particularities may not be sufficiently considered. But those local particularities play an important role in money laundering prevention, as money laundering risks can vary from country to country. We therefore welcome the risk-based approach chosen in the 3 EAMLD, which offers the possibility for financial institutions to adapt the due diligence measures to the individual risks they are exposed to.

**Rob Cutler, Deutsche Bank, London**

There is a strong case for harmonisation and it is already occurring without any organised intention to do so. Peer pressure is pushing regulators to follow each other and forcing governments to introduce appropriate legislation that allows such regulation. Further, regulators appear to be copying each other in particular enforcement and investigation actions. Where the US FED or SEC have taken action, the UK FSA will follow, and we have seen Korea and India, as well as Japan, all picking up each other’s cases. There should clearly be more joint thinking and a more harmonised approach so that firms are not required to do opposite things in different jurisdictions or be held liable in one country for abiding by the rules of another. Also, regulators must become more aware of the difficulties, costs, time constraints that frequent visits by different regulators create at one single firm. We do not believe, however, that any one single or joint international regulator would be a viable option at all due to major logistical, enforcement and other issues.

**Paul Martin, Director, London Investment Banking Association**

The proliferation of regulation is possibly not unexpected as countries seek to meet local needs to shut off financial crime. However, the FATF is the organisation that sets the standards for AML on which international harmonisation should be based.

Money laundering and terrorist financing is a global issue and there is a clear case for harmonisation but this also needs to have some built in flexibility to allow for local differences in money laundering and terrorist financing. There needs to be an agreed approach to tackling the issues – perhaps it is the risk-based approach we are all talking about but which needs elaborating. Will FATF take a lead on this? The risk-based approach should permit local risks to be accommodated. A degree of harmonisation is already happening as regulators are exchanging information and co-ordinating their work in this area. This process is at an early stage but in time will lead to common approaches to many issues. This will be of significant assistance to the industry as it should lead to less cross-border differences in how specific matters are dealt with. It will also make regulators more aware of the issues firms face when meeting regulatory requirements.

There is also a need for those that set the standards to be aware of the other existing laws that affect AML issues, for example, data protection and various secrecy and confidentiality laws. These also restrict the ability to exchange useful information and share intelligence in such a way that it becomes useful to the industry as a whole. Such exchanges are essential for money laundering and terrorist financing prevention. This awareness is not always apparent when new legislation is proposed. There is also a need to couple the financial services industry’s efforts with law enforcement. Governments need to address this and support law enforcement in its efforts to reduce financial crime – this is another form of harmonisation that needs a deal of work, and firms themselves or through their trade associations should continue to press this point with governments.

What practical challenges have you faced in implementing a risk based approach to anti-money laundering in practice and what steps have you taken to overcome them?

**John Mair, Tactics, and Growth. Risk, Reward, and Results**

Implementing an effective risk-based approach demands a near-perfect understanding of risk. Anything less runs the risk of money being spent with minimal beneficial impact. Critical to this is the calibre of the professionals engaged in the challenge. Do they compare favourably with the determination, calibre, sense of purpose and risk/reward of the adversary? If not, then much of the resource applied to the challenge may be wasted. The less the mainstream management of firms are genuinely interested in this theme, the more overbearing the methodology will tend to be. The better the mountaineer, the better adjusted the risk equipment, and the best overall result.
**Tassilo Amtage, Deutsche Bank, Frankfurt**

The primary challenge results from the requirements and expectations of the German regulator regarding the global documentation of the underlying risk analysis. In general, it should be noted that the effort involved in implementing the risk-based approach should not outweigh the effort involved in complying with the rule-based approach, otherwise the advantages are lost.

**Rob Cutler, Deutsche Bank, London**

Most practical challenges are related to formulating a judgement call into a written clear requirement, which at the same time allows different approaches. It sometimes appears that overcoming barriers in perceptions with staff on the business side as, well as on the compliance side, are no less challenging. More training has been required and more experienced staff. There has been the need to reconsider written requirements, policies and processes.

**Paul Martin, Director, London Investment Banking Association**

The first challenge for most firms is to understand what a risk-based approach to AML means to their business. It also requires an understanding of ‘what is a risk’ and then being able to recognise where in the organisation these occur. A thorough risk analysis and documenting the process is a challenge. It is likely that policies and procedures will need review and revision. The revisions need to fit the risk analysis. There has to be senior management involvement and sign off. Compliance and internal audit, as well as others such as legal and human resources will also need to be kept informed and provide input into the process. Education of staff, both front and back office, is required.

There are going to be those that see this as an opportunity to do less; while this may be so in certain areas of the business it is not an attitude that all can take. Staff need to be educated and their individual responsibilities spelled out to them and the consequences of failure for them and the firm known and understood. Risk assessment will be ongoing and processes will need to be put in place to pick up on new services and products to ensure that the risk-based approach covers them both in the development phase and when they come on line – this may be new to some.

**What technology challenges have you faced implementing an effective AML program?**

**John Mair, Strategy, Tactics, and Growth. Risk, Reward, and Results**

Technology challenges mean: capturing and using data, transaction monitoring, and establishing methodologies which make the best of the interplay between IT and the human being. Finding unusual transactions is becoming increasingly easy, and increasingly irrelevant. Much criminal money looks usual, so to understand what is behind a usual transaction or amount demands a more sophisticated approach than number crunching alone. How many transaction monitoring systems are good on non-personal business? All in all, if flows of money to or from illegal acts really are a serious problem, the approach being adopted, in the public and private sector alike, is going to have to be significantly more sophisticated than currently seems the case. If it isn’t, then the resources being deployed are simply going to be a drag on the spender, and little bother to the criminal.

**Tassilo Amtage, Deutsche Bank, Frankfurt**

The implementation of business-related anti-money laundering IT tools is very complex and expensive but gives the financial institution the possibility to streamline and harmonise time and manpower consuming processes. Deutsche Bank implemented a number of IT solutions for business-related processes. Apart from the implementation of the IT transaction monitoring tools mentioned before, the implementation of a technology supported global new client adoption process may serve as an example. Compliance with legal provisions has also been simplified by finding effective IT solutions.

The German Anti-Money Laundering Act, for example, requires regular anti-money laundering training and an assessment on the employees’ reliability and its documentation. Due to the extraterritorial scope of application of the German law, these provisions have to be met within DB’s international subsidiaries and branches as well. The insertion of this assessment into an online tool and the development of a web based anti-money laundering training, as well as the automated transferral of data into the HR administrative data base avoids time costing paperwork on the business.

**Rob Cutler, Deutsche Bank, London**

Too many to list. In no particular order they include: lack of funds, technology-led development that is trying to make the requirements fit technology rather than the other way around, huge numbers of different systems that cannot feed into each other and a lack of awareness at senior management level of the importance of the technological part of implementing AML or any control system.

**Paul Martin, Director, London Investment Banking Association**

Perhaps the challenge for firms is identifying where technology can be useful in the AML process and then seeing if there is a ready-made package that can do the job. In many instances an off the shelf package may not be suitable, as it cannot be integrated with existing systems – although it can point in a direction that is useful for developing an in-house solution. Funding is, of course, a challenge as AML may not always be seen as a priority.
Individuals who have been nominated as a Responsible Officer on their organisations AFSL are required not only to be qualified to at least Diploma level but also be trained in the areas in which they work as per ASIC Policy Statement 164.

‘Responsible Officers must be directly responsible for significant day-to-day business decisions, and larger institutions with many licences could need as many as 30 people in the role. However concerns about liability mean these posts have been beset by problems. Last year The Australian Financial Review reported turnover was averaging about 100 officers a month, in an industry with only 4237 licensed organisations.

An October survey of 217 ROs, found that 73% of them were worried about whether they were being properly protected by their risk and compliance departments. Others complained they could find no relevant training courses on how to be an RO. ASIC is believed to be curious about whether the high churn rate is because officers are finding something wrong in the companies they represent or simply because of uncertainty about their roles.’ Chris Wright, Financial Review

Recent feedback AFMA has received from a number of industry RO’s, indicated that they were uncertain about their full responsibilities regarding the fulfilment of their organisation’s AFSL requirements. With the expression of these concerns and given that there is still much ambiguity surrounding these roles, AFMA has developed an RO program that offers practical guidance for RO’s in their attempt to identify and treat risks from the perspective of the AFSL using a robust risk management framework.

The RO Program consists of two specific workshops – Responsible Officers’ Workshop and the Practical Compliance for Responsible Officers. Taken in conjunction with each other, we believe they provide an excellent mechanism by which organisations can meet their AFSL obligations.

The Responsible Officers Workshop is a vital training solution for potential or existing RO’s, giving them an opportunity to:

- explore key elements of a responsible officer’s role
- examine AFSL Licensing conditions and ASIC breaching reporting
- clearly understand the RO’s responsibilities, accountabilities, liabilities, penalties and defences
- acquire a practical guide to assist RO’s identify, classify and manage risks to your organisation
- RO’s will leave with a clearer understanding of what is involved with being an RO

With interactive discussions and practical examples of the roles, responsibilities and activities of an RO, we have found that individuals attending The Responsible Officers Workshop have enhanced their understanding of their responsibilities giving them increased confidence regarding the fulfilment of their organisation’s AFSL.

The Practical Compliance for Responsible Officers Workshop is geared towards ROs who work closely with Compliance, providing them with an understanding of the practical steps involved in managing compliance, with particular emphasis on the Responsible Officers’ and Compliance Officers’ duties. Given that both roles must be actively involved in the process and application of compliance in order to develop and lead the appropriate culture, this workshop not only assists participants to make it all work, but also to literally put it into practice.

UP AND COMING DATES FOR THESE WORKSHOPS ARE:

<table>
<thead>
<tr>
<th>Responsible Officers Workshop</th>
<th>Practical Compliance for Responsible Officers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brisbane</td>
<td>Melbourne</td>
</tr>
<tr>
<td>22 May 2006</td>
<td>26 June 2006</td>
</tr>
<tr>
<td>Sydney</td>
<td>Sydney</td>
</tr>
<tr>
<td>24 July 2006</td>
<td>02 August 2006</td>
</tr>
<tr>
<td>Sydney</td>
<td>Brisbane</td>
</tr>
<tr>
<td>12 September 2006</td>
<td>29 September 2006</td>
</tr>
<tr>
<td>Melbourne</td>
<td>Sydney</td>
</tr>
<tr>
<td>24 October 2006</td>
<td>03 October 2006</td>
</tr>
</tbody>
</table>

To find out more about either of these programs then please contact Jason Sheil on 02 9776 7914
The selection, purchase, implementation and maintenance of AML technology does not lend itself to traditional return on investment (ROI) calculations. Regulatory compliance is a ‘must do’. Catching the bad guys is the role of law enforcement. Financial institutions provide the trail by filing Suspicious Transaction Reports (STRs) that allow law enforcement to ‘follow the money’.

The primary risk to the financial institution is loss of reputation for non-compliance, fines or even sanctions. That risk is seen in headlines and with the regulators. It ranges from a decline in market value of publicly traded shares to the loss of clients as they seek another financial provider with an unblemished reputation. It is difficult to quantify the long-term impact of loss of reputation. Thus the AML ROI calculation has ‘investment’ but no clearly definable ‘return’.

However, there are ways to perform good analysis on the investment by insuring you make the right short and long-term decisions, knowing your total cost of ownership and being creative in utilising the AML risk assessment process as part of a data mining process to do event-based marketing, repricing services to your clients based on behavior and activity, and looking at unusual internal behavior.

What is my true cost of an AML investment?
Technology cost

What may appear to be a ‘bargain’ solution initially could turn out to be expensive if the system investment can’t grow with you or meet continuing changes in the AML environment.

The AML investment can be a ‘buy or build’ solution. Cost is not just a check that you write to an outside vendor. What if you want to build a solution yourself? The same questions apply with the added complexity of ensuring that you have enough internal backup to maintain the system while keeping abreast of all the regulatory changes and industry best practice.

The vendor selection process can take many forms. You can use an outside consultant to do a market scan and make a recommendation. The consultant can help you design a request for proposal or your staff can do it.

What is most important is that you understand and are able to document your requirements. It is difficult to make a purchase decision when you are not clear on what you want and what you need. There is always a ‘wish list’ but you need to determine your priorities. The parameters of any project are time, money and quality. Know your priorities within these as well.

As your needs change, your system must still meet your requirements. Is the technology provider proven? Ask to learn if they have done it before for an institution like yours. As you evolve and grow, can the data and the history grow with you?

Do you have to rewrite new rules or scenarios every time there is a new finding in
the market? Does your system adapt and learn? Does the behavior modelling cover all accounts, customers and products? Can you do risk-based analysis on your entire client base and product set?

**Internal costs**

The vendor or your own internal development group is not the total cost. There is an implementation cost to set everything up and running, and have it tested and placed into production. These costs can be significant. Your company will run numerous software applications and your staff needs to know them all. A new application has a learning curve that can be time consuming and full of false starts. An application with pre-defined processes can sharply reduce your own expenses. This is not easily visible and will require some digging. The payoff is important.

**Management opportunity cost**

AML compliance does not bring new revenue to the bottom line of a financial institution. If management has to spend time worrying about a process and technology solution, then that is time that cannot be spent in other areas.

There can be subtle impacts on business direction and opportunities if management has to spend too much time on a particular project. Management oversight and sponsorship is critical to the success of any project, but a solution that takes too much management effort is not a good use of executive time. A solution that works right and meets the compliance responsibilities of the Board of Directors is best.

**Regulator compliance cost**

If you put in a solution and it does not meet the regulator’s requirements, compliance staff and management will spend time explaining why. Then a new or revised solution will have to be implemented. For example, if your regulator requires a pre-defined set of rules, individual account monitoring, special correspondent banking reviews or special cash transaction monitoring, it is always best to develop a comprehensive solution the first time.

Money launderers are highly motivated and creative. Invariably they attend the same conferences as market practitioners and are already aware of the technologies and processes being used to combat it. The regulatory environment is constantly advancing as a result, and if an inflexible solution is chosen, the regulatory cost can be high.

**Total cost of ownership**

What does it really cost me to put an AML program in place and then maintain it? A September 2002 report produced by Celent estimated that the US banking, securities and insurance industries alone will spend a combined total of USD 10.9 billion through 2005 to combat money laundering. Of that total, only 6%, or USD 695 million, will be spent on hardware and software. IT maintenance will account for 30%, or $3.3 billion. Employee training, reporting and compliance will make the remaining 64%, or $6.9 billion.

Getting the most out of your AML system and process is not just what you spend today but more importantly, what will you spend tomorrow, the day after tomorrow, and so on. To best gauge this, you need to consider the following:

- What is the expected obsolescence of my investment?
- What is the upgradeability of my investment? How complicated will it be?
- What kind of IT staff do I need to support the investment?
- How stable is my platform? Is it a one-off solution?
- How will the system give me high-quality alerts so that I can efficiently use by financial intelligence unit staff?
- How does the workflow allow me to reduce the mechanical functions (like filling in forms) so that I can focus on investigations?
- How can I know what best practice is in this area?
- What happens when the regulators suddenly insist on a new type of investigation and I have a static process?

Adding up the cost of hardware and software is not straightforward. Some questions you should ask:

- Does the hardware allow for a growing database?
- What is the database structure? How often does it change?
- Does the networking capability accommodate today’s Internet requirements?
- Does the operating system of the hardware upgrade frequently?
- Does the hardware vendor have a good relationship with the software vendor?
- Does the software allow for a standard upgrade of new product or new regulatory requirements?
- Does the out-of-the box software accommodate a simple or multi-dimensional business model?
- How can you modify the software to meet your unique requirements?
- What is the track record of the hardware and software vendors?
Technology choices:
- Buy or build
- Off the shelf or custom
- Quick and dirty or longer term
- Local, regional or enterprise
- Comprehensive or focused on one area
- Complex or simple (one size fits all)

The review of the initial expense is intense with significant checks and balances. The on-going expense gets built into the fabric of the institution, but is many times greater than the initial technology expense. The key is to establish a process that continuously challenges the process to seek ever better alerts, real cases and suspicious transaction reports (STR). A smart technology investment has a lower overall cost of ownership.

Technology Options
Daily we are bombarded by ‘new and improved’, ‘bigger, faster, better’ and ‘renders all else obsolete’. Each institution needs to understand where it is on the technology curve. Are you an early adopter, a cautious follower or one who will only change when forced by regulation? An institution with diverse lines of business and a wide geographic reach has very different requirements from a local community bank. One needs to be at the leading edge and the other can afford to wait. What is the appetite for risk? New technology fails as well as delivering on promises. What is my true cost if I have to start all over again? What is the track record of my proposed solution?

Solutions vary from a basic rules-based approach to adaptive, total account and transaction-detection techniques. The regulators will offer guidance on what they deem important, and with all of the global attention on money laundering, there are a growing number of purported solutions. Many of the alternatives are incomplete, so do your homework.

Metrics
Before you start, establish the benchmarks that will allow you to accurately judge progress and success (or failure). These could include:
- What is expected system performance, eg. the response time, end of day processing and network bandwidth?
- What kind of staff productivity can I expect? What production standard should I set?
- What is the learning curve before I achieve full proficiency?
- What kind of quality do I need?
- What is the timeliness of responses or time to compete an investigation?
Create measurement for anything possible and then benchmark against your peers. AML processes are not a competitive advantage. Industry professionals are willing and open to share their ideas on what is a reasonable metric and what is effective for the greater good?

Conclusion
If you are wondering how to move ahead with your AML technology investment, ensure you consider the following:
- understand your requirements, your market and your regulator
- understand the cost and risk of making the wrong decision
- understand your total cost of ownership
- leverage your AML investment to achieve additional tasks
- set expected metrics and manage to them
- make an informed choice so that you don’t have to make the investment twice.
Q: Under Part III of the FTRA reporting entities currently have to identify ‘signatories’ to an account. Where is this going to be covered under the new rules, as all the discussion seems to be around identifying individuals and companies as clients? Will there be a requirement to identify signatories to an account going forward?

A: The Draft Exposure AML/CTF Bill (the Bill) does require the identification of signatories to an account. Part 2 generally requires a reporting entity to identify a customer prior to providing them with a designated service.

Table 1 of Section 6 outlines what is considered as the ‘provision of a designated service’, as well as the definition of a ‘customer to whom the designated service is provided’. Before providing a designated service, it is usually necessary to identify the customer using the applicable customer identification procedure under the Bill.

Allowing a person to become the signatory to a new or existing account is classified as the provision of a designated service, and the customer of such a designated service is ‘the signatory’ (Item 2).

More importantly, allowing a transaction to be conducted with an account is a designated service. Before allowing a transaction, the reporting entity must identify all customers — which includes the account holder and all signatories (Item 3). This essentially continues the FTRA approach.

Q: Roughly how long would it take to find, integrate and set up an AML system?

A: One size doesn’t fit all. The design and build of an anti-money laundering/counter-terrorism financing (AML/CTF) solution is driven by the specific requirements of the institution. Individual institutions’ requirements will be predicated on their different business models, risk profiles and legacy environments. However, the selection and implementation of a particular software system can have a standardised process.

Clients will already understand the importance of fully determining their business requirements before assessing the products of software providers. This process can be accelerated for AML/CTF through an analysis of ‘in-house’ capability. Clients need to allow up to three months for this exercise but the results will prove invaluable:

- business requirements defined
- existing infrastructure mapped to business requirements
- functionality gaps identified
- base information prepared for request for proposal (RFP) if required.

If clients prefer to look to market for an AML/CTF software system, there are tried and trusted RFP methodologies. Some organisations have taken up to 12 months to complete an AML/CTF RFP, and while this may be at the high end three months is probably the minimum, assuming that they have undertaken the ‘in-house’ analysis first.

The three-month RFP period does not reflect the successful conclusion of contractual negotiations. This in itself can take six months depending on the number of parties involved e.g. the software provider, the system integrator, and the organisations’ outsource partner(s). Given the level of effort associated with the contract, organisations should consider managing this activity as part of the initial
implementation effort.

As with major system implementations, the major work effort begins once the vendor is selected. Depending on the nature and size of the organisation clients need to prepare for an implementation journey of years rather than months.

Some vendors will tell clients within even the biggest organisations that their software can be implemented in three or four months. This might be true, but organisations need to understand what they have after this time. After three or four months organisations will have a ‘base’ version of the system installed. They will then face the challenge of ensuring that the system is capturing all of the customer and transaction data necessary to determine suspicious activity across the enterprise. The bigger and more complex the organisation the longer this will take.

Even after all the required system interfaces are built and necessary data is sourced, organisations still face the challenge of ‘tuning and bedding down’ the AML/CTF software. There will be new processes to learn, people to train and reports to manage. Some off-shore organisations have encountered significant operational problems post their ‘go live’ date e.g. a need to quickly recruit and train staff to deal with AML/CTF alerts.

So for small to medium-sized organisations there can be a minimum period of approximately nine or 10 months from determining business requirements through to a base implementation of AML/CTF software. For larger organisations, the base implementation could be at least 12 months and then there is the issue of enterprise roll out and integration.

Tony Byrne, KPMG Forensic

Q: How necessary is it to have a dedicated AML officer both in the short and long term?
A: Interestingly, while the draft legislation requires board approval and oversight of an entity’s AML/CTF program, it does not demand the appointment of a designated officer with personal responsibility and liability for it. However, this appointment is an established practice in countries such as the UK and the US, who have deemed it a necessary role to ensure that AML/CTF programs are effectively maintained and assigned the proper importance. In the UK this role is referred to as the ‘money laundering reporting officer’, or MLRO. In the US the designated person is known as the Bank Secrecy Act officer.

Under international practice the designated AML/CTF officer is a senior position that often reports directly to the Board. Their role and corresponding responsibilities are specifically designated and formally documented in the corporate AML/CTF policy. They have the high-level authority to act independently and decisively when faced with money laundering or financing of terrorism issues and risks.

For these reasons, Australian organisations should also consider a senior appointment that has overall responsibility for the operation of the AML/CTF program. However, the extent to which they would be dedicated solely to AML/CTF compliance (and the size of the team to support him/her in this function) will vary according to the size and complexity of the organisation.

In the short-term, they may be required to act as a project director or manager, leading the development and implementation of the AML/CTF program on a day-to-day basis. Given the likely expenditure, together with the potential scale of the impact on an organisation’s business operations; this is an important and lengthy project. Larger organisations will likely have a number of staff employed full-time on this project for the next two to four years.

In the longer-term, Australian organisations should seek to assign accountability for the effectiveness and maintenance of an AML/CTF program to one individual. Maintaining an AML program is a significant task and should not be underestimated. The adoption of a risk-based approach means that an organisation must continually monitor its risk profile, at an enterprise and business line level, and adapt its controls to reflect changes in these risks. Furthermore, the draft legislation places emphasis on appropriate AML/CTF program management, including monitoring compliance, independent reviews of the program and board oversight. Finally, as AUSTRAC considers necessary enforcement a few years down the line, organisations will best manage their regulatory risk through ongoing regulatory liaison and the demonstration of strong AML/CTF program management.

Lucy Major, KPMG Forensic

Q. Can you provide some practical examples of non-electronic testing that could be utilised for AML, and which know you client (KYC) procedures should be implemented?
A: The documents currently required for 100 point checks on individuals are listed in the Financial Transactions Reporting Act and Regulations. The AUSTRAC website (and the e-learning resources contained therein) will also assist you to determine these requirements. However, there will be changes under the new laws, and the nature of these is not yet clear. You do not need to implement the new requirements until the law is passed, which is expected to be at the end of this year. There will be an implementation period that presumably will cover any change in identification requirements.

In terms of practical examples of non-electronic testing, it is assumed that you are referring to monitoring for suspicious transactions and activity. There are a number of possibilities here, depending on your industry, your business and the controls that you use. Many opportunities should exist in your business processes to construct a non-electronic monitoring environment.

Joy Geary

Q. What checks need to be completed for companies/superannuation/funds management companies? Does this require organisations to check the directors of these companies, the underlying beneficial clients or just check the company itself is registered with ASIC?
A: Where you need to establish beneficial ownership of the account, and there has been no exception provided in the legislation or rules (e.g. as might be introduced for
certain types of superannuation funds), then the beneficial owners will need to be identified and verified just as if they were individuals. It will not be sufficient to check that the company itself is registered with ASIC. The requirement relates to the beneficial ownership of the account, not the funds management company. One way to consider beneficial ownership in the absence of any legislative instruction is to consider who has entitlement to the funds in the account in the event of the fund manager’s liquidation. If the underlying beneficial owners are the beneficial owners, which it is likely that they are, then each needs to be identified and verified.

Joy Geary

Q. What requirements will there be to screen new employees? Will existing employees need to be re-screened and if so under what time frame?
A: The questions asked do not yet have answers. Certainly you would only need to screen successful candidates and not all applicants for positions. There is one argument that screening is only part of the employee due diligence program, so screening may arguably also be regarded as applying to existing employees depending on role. That argument might not be the actual intention of AUSTRAC in the way they have drafted the rule. What is required for screening and who needs to be screened and how screening can be done is not yet clear and it would appear is going to be a decision for each organisation.

The preferred wording of the rule is in the direction of flexibility and risk-based. There is a good argument to say that screening should be satisfied by existing probity processes for those reporting entities already required to have them.

Joy Geary

Q. Does the panel have any feedback on what ‘designated services’ will be risk ranked as under the proposed legislation, e.g. low/medium/high, as this will have ramifications for each entity’s AML/CTF programs and procedures.
A: The designation of a service as low, medium or high risk will be a decision for each reporting entity (i.e. your organisation). Should your organisation have a money laundering or terrorist financing event, your choices will form part of your risk-based approach and you may need to establish that your decisions were reasonable at the time they were made. You are therefore well advised to have good documentation around how and why you made your risk decisions, as well as regularly review such decisions for their appropriateness. I think one of the difficulties with concepts of the risk associated with financial products and services is that so many are susceptible to money laundering. One way of assessing risk is to focus on the known ways that money launderers use products and services, rather than their inherent characteristics.

Joy Geary

Q. What are the asset freezing and reporting obligations on Australian ADIs in relation to OFAC and/or UK-EU lists for transactions within Australia?
A: If the person is a customer of an Australian reporting entity undertaking domestic transactions only then there are no asset freezing or reporting obligations on the Australian ADI. However, from a risk perspective organisations should consider why they would wish to have this person as a customer, and if they do, then the attendant high risk should lead to extensive customer and transaction monitoring. The answer is different if transactions are sent to the US or UK for clearing.

Joy Geary

Q. How are the proposed changes to AML legislation likely to affect corporate advisory businesses?
A: These businesses will be within reach of the new laws. You will need to understand how money launderers use corporate advisory services, bearing in mind that many money launderers operate through front companies which appear to run legitimate businesses. You will need to understand your risks, implement measures to manage those risks and identify and verify the identity of the beneficial owners of your customers. A detailed understanding of your customer’s background, their business, the purpose of their relationship with you and the basis for requiring your services will be paramount. You may need to look at background checks in certain cases in order to acquit your AML obligations for privately owned entities.

Joy Geary

Q: Will we be required to keep the risk classification of a customer secret?
A: No. Customers will usually be able to gain access to their classification. However, banks and other reporting entities that owe duties of secrecy will hold the risk classification subject to those duties, meaning that disclosure to third parties may be prohibited without the customer’s consent.

Provisions of the Bill
The current draft of the Bill does not require a customer’s risk classification to be kept secret, and there are no provisions that provide for ‘internal restrictions’ on the use of the risk rating.

The secrecy (or ‘tipping off’) provisions in the Bill apply only where a suspicious matter report has been filed (or the relevant suspicion has been formed). Where the suspicion has been formed, or a report filed, a reporting entity must not provide any person with information that might suggest that these things have happened, or that further information has been provided to AUSTRAC.

Access by the customer
There are no general secrecy requirements in the Bill relating to a customer’s risk rating (unless the risk rating could itself show that a suspicious matter report has been filed). On general principles, the risk rating would probably be confidential (and subject to the banker’s duty mentioned above). National Privacy Principle 6 (NPP 6) usually allows an individual to access all information held about them; however, it does not have to be provided where withholding information is required or authorised by law, among
other exemptions.

The customer would be able to use Privacy Act rights to access their risk rating. They could also access other information relating to the reporting entity’s AML processes that involve them as an identifiable individual (except for information about a suspicious matter report that has actually been filed, or the suspicion that led to the report).

For example, if a particular transaction has been reviewed to see if a report should be filed, and the reporting entity decides that the customer’s behaviour is not suspicious, all details of the review would be available.

It could be argued that the exemption in NPP 6.2 (relating to ‘commercially sensitive decision making processes’) will apply to customer risk ratings and a reporting entity’s processes for assessing potentially suspicious matters. This exemption was driven by a concern that credit providers would be required to reveal their credit-scoring processes. It is not clear that it will apply to AML processes unless amended. If it did apply, reporting entities could provide ‘an explanation for the commercially sensitive decision rather than direct access to the information’. In its current form, it is not clear that NPP 6.2 will provide a complete exemption from the need to provide an individual with information about all of the reporting entity’s AML processes, as they apply to the customer.

Policy issues
The Senate Legal and Constitutional Affairs Committee report on the AML/CTF Bill considers privacy issues in some detail. The Committee’s recommendations suggest that information about a reporting entity’s AML program should be fully subject to Privacy Act protection (even where a reporting entity would not otherwise be subject to the Privacy Act).

Equally, it could be argued that the Bill should be amended so that reporting entities are authorised to withhold information about the inner workings of their AML/CTF processes (particularly individual customer risk ratings, and details of the processes followed to determine whether a matter should be reported to AUSTRAC). If the processes became publicly known, there could be a threat to the effectiveness and integrity of the organisation’s AML/CTF program.

Reporting entities may also be concerned about potential ‘customer management’ issues if customers learn their risk ratings. Many of the customers assessed as ‘high risk’ because of the kinds of products they hold are law abiding citizens, unlikely ever to be involved in money laundering. If they learned that they were classed as ‘high risk’ (implying additional scrutiny), it could cause unnecessary offence.

Q: Should the customer risk classification be internally restricted in much the same way as a TFN is now, and made available only on a need to know basis?
A: This is not required under the Bill. There are no restrictions in the Bill on the use of a customer’s risk rating within the organisation (or, as discussed, on disclosure to the customer). The Privacy Act requires organisations to use personal information only for the primary purpose of collection, or for related secondary purposes. All aspects of a customer’s use of designated services are likely to be ‘related’ to the purpose for which the risk classification is collected.

However, because of the customer management issues noted above, institutions may wish to impose internal restrictions. Of course, information about suspicious matter reports should be tightly controlled, because it is a serious offence for that information to be disclosed.

Andrea Beatty, Mallesons Stephen Jaques
James Moore, Mallesons Stephen Jaques
Anti-money laundering
Combating money laundering in financial services

Read by over 3,000 banking and finance practitioners across Australia and New Zealand

Providing unrivalled coverage of the latest issues impacting the financial services sector

- Regulation
- Governance
- Know your customer
- Risk based approach
- Counter terrorist financing
- Monitoring systems
- Systems architecture and technology
- Legal implications

Claim your free subscription today
Email your contact details to Diana Zdrilic on dzdrilic@afmaservices.com or call 02 9776 7923

CONTACT THE ANTI-MONEY LAUNDERING PUBLISHING TEAM
Subscriptions
Anti-money laundering is free to qualified practitioners. To register for your subscription email dzdrilic@afmaservices.com with your contact details.

Advertising
For a media pack and advertising rates contact Diana Zdrilic 02 9776 7923 or email dzdrilic@afmaservices.com
The price Riggs paid

How deficiencies in Riggs’ anti-money laundering compliance program cost the ‘bank of presidents’ over US$ 189 million.
The following case study was prepared by World-Check, the market pioneer and industry standard for PEP screening and customer due diligence — serving over 1,600 financial institutions and government agencies in more than 120 countries, including 45 of the world’s 50 largest financial institutions.

Foreword
by David B. Carusso

Riggs is a story about the price paid when an anti-money laundering (AML) compliance program lacks proper oversight by management and the board of directors. As you will read in this paper the outcome of such failure in the case of Riggs was rather dramatic and as in any good drama there were lots of twists and turns in the various plots and sub-plots. Who could have imagined that one, relatively small bank in Washington DC, could have participated in the questionable financial activities of two of the more notorious dictators of the last quarter century?

One of the many thing my staff and I learned over the two years we were at Riggs busy trying to build a compliance program and ultimately uncovering almost all of the facts you’ll read about in this paper, is how harmless most poor business decisions seem at the time they are made. Bad decisions and their ramifications take years to be understood. In the case of Riggs it took almost 20 years for errors in judgement to come to fruition.

Beginning in the 1980’s Riggs management and ownership launched efforts to dominate embassy and diplomatic banking in Washington DC. It seemed like a good idea at the time. It was prestigious, glamorous, and offered the bank’s ownership the opportunity to hobnob with the world’s political, economic, and diplomatic elite. It even provided justification to buy a Gulfstream V jet. Riggs entered into this market without ever understanding the risks it posed.

Therein lies the failure. Understanding the money laundering, fraud, and terrorist financing risks presented by your customers, your products, your services, and the locations where you operate is the most essential responsibility of an organisation in today’s environment.

In the aftermath of Riggs many believed that banking embassies or diplomats was in and of itself high risk. I don’t believe that nor do I believe banking PEPs is automatically high risk. What is true is that these customers present a potential for higher risk, and it is the job of compliance, management, and the board of directors to understand what those risk are, how to mitigate them, the costs of mitigation, and whether proper risk management is sustainable.

As you read this paper keep in mind that the failures of Riggs to properly identify its risk and manage them is not unique. Ask yourself how well your institution knows all of its risks and how well they are controlled.

Introduction
by David Leppan, CEO and Founder of World-Check

‘Things fall apart’

For many years, compliance officers have tried to place a value on their institutions’ reputations, often in an attempt to convince reluctant board members and CEOs to approve increased compliance budgets. This case study offers a unique and valuable snapshot of the cost of reputational damage and the fallout caused by an array of AML issues including the lack of proper controls and procedures.

Riggs Bank was no ordinary bank. It was an historic cornerstone in the U.S. financial community with its origins, as a brokerage house, dating back to 1836, and its depository and checking services dating to 1840 (Corcoran & Riggs). Often referred to as the ‘bank of presidents’, some 20 presidents held accounts at Riggs, including Abraham Lincoln and Dwight D. Eisenhower. It was Riggs that in 1868 supplied the U.S. government with gold bullion to purchase Alaska from the Russians. Riggs was an institution. It banked 95% of all embassy accounts in Washington. But in less than three years, things went horribly wrong for this institution, its management and its shareholders.

What were the issues? Could your institution face the same fate?

In the pages that follow, we will outline several key events and AML issues that dramatically affected Riggs’ name, reputation and ultimately its share price.

There is nothing unique about the issues that plagued Riggs and before you jump to the hasty conclusion that ‘none of this could happen to or at our bank’, might I suggest you read on.

There is much to be learnt from what happened at Riggs. Compliance Officers and more importantly the CEOs and Board Members of all financial institutions should take the time to read this case study illustrating the true cost of reputation damage.

‘The most important bank in the most important city in the world’

Riggs Bank Advertising Campaign, 1983

David B. Carusso was the Executive Vice President of Compliance & Security at Riggs bank from June 2003 through May 2005. Carusso and his staff were hired to address concerns raised by U.S. regulators of the Riggs relationship with the Saudi Arabian embassy and royal family. Over the next two years Carusso and his senior staff uncovered the fraud involving a Riggs banker and government officials of Equatorial Guinea as well as much of the history between Riggs and Chilean dictator Augusto Pinochet.

Carusso and his staff used World-Check to help identify PEPs and other high risk customers at Riggs Bank.
Understanding the issues at Riggs: Two leaders, too many?

Riggs, known as the ‘bank of presidents’ ended up with 1 or 2 world leaders too many: the Chilean former dictator (1973-1990), General Augusto Pinochet and Equatorial Guinea’s president (since 1979), Brigadier General Teodor Obiang Nguema Mbasogo.

Our understanding of the relationships between Riggs and these two leaders is derived entirely from open source research. Our aim with this case study was not to highlight the exact or detailed nature of the relationships or the banks shortcomings but rather to provide an overview of the reputation damage caused to Riggs during a period of a few years, and more importantly, understand how many of the world’s institutions are knowingly or unknowingly facing the very same risk.

Riggs & Pinochet

It is reported that Pinochet (or family members/representatives) held a total of 28 accounts at Riggs spanning 25 years (earliest account opened in July 1979) and totalling approximately US$8 million. The bigger picture however is to be appreciated in a Riggs memorandum in 2002, which stated that the value of the Chilean business at Riggs had “average balances exceed $100 million”.

It was while Riggs’ International Private Banking Department was under review during a routine regulatory examination in April 2002 that the Pinochet accounts came to light.

Riggs had failed to disclose the existence of accounts associated with a Politically Exposed Person (PEP) in response to a direct request by its regulators. A Senate report alleged that managers at Riggs Bank had not only failed to comply with AML legislation but were also being asked to disclose the Pinochet accounts when the OCC requested a list of all PEP customers.

Pinochet’s accounts were terminated after serious concerns about the oversight of the accounts was raised by the Office of the Comptroller of the Currency (OCC). The OCC had 3 main issues with the way Riggs had dealt with the Pinochet accounts. These were:

- choosing – on the basis that the bank felt Pinochet was no longer a PEP - not to disclose the Pinochet accounts when the OCC requested a list of all PEP customers.
- no suspicious activity/transaction reports were filed when Pinochet moved large sums of money from accounts at Riggs to other foreign institutions. No disclosures were made about sums moved from the U.K. and Spain ahead of attempts to seize Pinochet’s funds by Spanish authorities.
- lack of documentation on the source of the Pinochet funds. By the time the investigation was concluded, Riggs would face the largest fine for noncompliance handed down to a bank in the U.S.

By the time the investigation was concluded, Riggs would face the largest fine for non-compliance handed down to a bank in the U.S.

Riggs held around 95% of the embassy business in the US and 40% in London.

The question is not as simple as whether or not your institution is meeting the standard laid out by your regulator.

Riggs & Obiang

In 1995 Equatorial Guinea opened its first accounts at Riggs. This client was to become Riggs’ biggest depositor with, at its highest point, a balance of around US$700 million. Riggs held the Equatorial Guinea government treasury accounts as well as the private accounts of President Obiang, his family and senior government officials. Some 60 accounts were reported to have contained ‘gifts’ made to the leadership of this country by U.S. oil companies.

Equatorial Guinea’s oil production had increased tenfold after the discovery of a new oilfield in 1995 (Zafiro field). Diplomatic relations which had been broken off by the Clinton Administration in the mid-90’s were re-established in 2003 under President Bush as oil from alternative sources became of great importance.

Accounts held in the first family’s name or in the name of offshore shell companies, which had been established reportedly with the assistance of Riggs for the first family, had seen cash deposits of almost US$13 million between 2000 and 2003. In addition, large payments by oil companies had been made directly into private accounts or accounts held by officials.

After an investigation by Riggs’ new Compliance staff got underway, the senior banker responsible for the Equatorial accounts, Simon P. Kareri, was fired in January 2004.

The US Senate Report of July 14th, 2004, found Riggs “had serviced the Equatorial Guinea accounts with little or no attention to the bank’s anti-money laundering obligations…”. It was apparent Riggs had been aware of the proceeds of large scale bribery and corruption. The Report went on to state that the bank had “exercised such lax oversight of the account manager’s activities that, among other misconduct, the account manager was able to move more than $1 million from an account belonging to a ruling family member at Riggs to another bank for an account opened in the name of Jadini Holdings, an offshore corporation controlled by the account manager’s wife.”

January 27th, 2005, Riggs pleaded guilty to one felony count of failing to file suspicious activity reports and agreed to be fined US$16 million. The fine was the largest amount ever imposed on a bank of Riggs’ size.

On 3rd June 2005, Kareri and his wife, Ndeye Nene Kareri were indicted on 27 counts of conspiracy to defraud the bank and other related charges including bank fraud, wire fraud, money laundering and income tax evasion. If convicted they face up to 30 years in prison and a million dollar fine.

Simon P. Kareri also opened an account in 1997 at Riggs for Foutanga Dit Bahani Sissoko, a businessman and politician from Mali who was accused of embezzling almost US$250 million from the Dubai Islamic Bank.

Prior to its ‘Presidential Problems’...

The Saudi Arabian Diplomat Accounts

The allegations that triggered the initial investigation into Riggs by US authorities appeared in a Newsweek article in December 2002 (‘9-11 Hijackers: The Saudi Money Trail’ By Michael Isikoff). The article suggested a ‘steady stream’ of monthly payments had been uncovered that were being made to Omar Al Bayoumi, who had
had dealings with two of the September 11th hijackers, namely Khalid Almihdhar and Nawaf Alhazmi. The money, it was reported, had come from the accounts of Princess Haifa Al Faisal, wife of the former Saudi Ambassador to the U.S., Prince Bandar and daughter to the late King Faisal of Saudi Arabia.

The article went on to state “After Al Bayoumi left the country in July 2001 – two months before the September 11 terrorist attacks – payments for roughly the same amount began flowing every month to Osama Basnan, a close associate of Al Bayoumi’s who also befriended the hijackers. A federal law-enforcement source told NEWSWEEK that Basnan – who was recently convicted of visa fraud and is awaiting deportation – was a known “Al Qaeda sympathiser” who “celebrated the heroes of September 11” at a party after the attacks and openly talked about ‘what a wonderful, glorious day it had been’.”

March 2004, Riggs announced it was closing all Saudi accounts.

In late November 2004, Saudi officials acknowledged that the Princess had given money to the family of Osama Basnan. The money, it was explained, had been given as a donation towards medical expenses.

Princess Haifa Al-Faisal was finally cleared of the allegations. The 9/11 Commission Report stated: “We have found no evidence that Saudi Princess Haifa al Faisal provided any funds to the conspiracy, either directly or indirectly.”

The Results: Shareholder suits and fines

Shareholders take action

In April 2004, a shareholders’ derivative complaint was filed against Riggs. The suit alleged that 11 directors “breached their fiduciary duties of loyalty, honesty and care and caused a waste of corporate assets and other harms to Riggs by failing to conduct appropriate due diligence of the Bank’s Middle Eastern and Equatorial Guinea customers and by failing to exercise reasonable control and supervision over Riggs and its officers and employees in connection with Riggs’ compliance with applicable banking laws, including the BSA and federal anti-money laundering laws.”

This was to be the first of several shareholder suits brought against the bank and its management.

The OCC Fine

13 May 2004, Riggs was fined US$25 million by the OCC for numerous violations of the Bank Secrecy Act relating to the Saudi Arabian and Equatorial Guinea issues and the lack of suspicious activity reporting. No criminal activities were uncovered within the Saudi transactions.

This amount was the largest civil monetary penalty ever brought against a U.S. financial institution for violations under the Bank Secrecy Act (BSA), the statute requiring financial institutions to guard against money laundering.

The OCC’s report stated that the banks internal controls “were, and continue to be, seriously deficient”. “Riggs failed to properly monitor, and report as suspicious, transactions involving tens of millions of dollars in cash withdrawals, international drafts that were returned to the bank and numerous sequentially numbered cashiers’ checks.”

Riggs’ former chairman and largest shareholder, Joseph Allbritton resigned from the Riggs National Corporation Board as did Timothy Coughlin, president of Riggs National Corporation.

Time to get out of the business

By mid-June 2004, Riggs had received preliminary proposals from 7 potential institutions looking to acquire it.

On July 15th, 2004, the Riggs Board accepted a bid from PNC (The PNC Financial Services Group, Inc.) of a combination of cash and PNC common stock. The amount offered was US$24.25 per Riggs common stock.

The very same day, the U.S. Senate Committee on Government Affairs Permanent Subcommittee on Investigations issued its report, “Money Laundering and Foreign Corruption: Enforcement and Effectiveness of the Patriot Act; a Case Study involving Riggs Bank”. The report concluded that Riggs had assisted Pinochet in “evading legal proceedings related to his Riggs Bank accounts and resisted OCC oversight of these accounts,” and that the bank had, while managing several accounts for the Equatorial Guinea officialdom “allowed numerous suspicious transactions to take place without notifying law enforcement.” Finally the report stated that Riggs had “ignored repeated directives by federal bank regulators to improve its anti-money laundering program.”

September 11th Class Action

On September 10th, 2004, claims were made against Riggs on behalf of the victims of the September 11th attacks (Vadhan). The class action was later dropped. By mid-June 2005, the claims were dismissed and PNC, by then Riggs’ new owner, made a contribution as part of the agreement to a charitable foundation. A second action (Cantor) was filed on September 13th. By April 2005, this action had been resolved.

Yet more shareholders suits

By November 2004, a civil lawsuit had also been filed against former Riggs officers and directors by shareholders (‘Freeport Partners’). The complaint alleged that the banks action “was the proximate cause of a decline in value of Riggs…and therefore resulted in injury to Plaintiff’s property” and that this “made the sale of Riggs necessary and reduced the price at which that sale could be made.”

November 2004 brought a similar class action and derivative complaint from other shareholders (‘The Delaware Plaintiffs’).

The Spanish Criminal Action, another fine and the CEO resigns

On 27th January 2005, Riggs Bank and two members of the Allbritton family, the banks largest shareholders, agreed to pay US$9 million into a fund for victims of Augusto Pinochet, to settle a case over the bank’s role in hiding the former dictator’s ill-gotten gains.

On the same day, Riggs pleaded guilty to a single felony count of failing to submit accurate suspicious activity reports. A fine of US$16 million was levied which was paid on March 29th, 2005. The judge in the case, Ricardo Urbina, referred to the bank as “a greedy corporate henchman of dictators and their corrupt regimes.”

7th March 2004, the chairman and CEO of the parent company of Riggs Bank, Robert L. Allbritton resigned. The bank’s biggest shareholder was left without any direct board representation.

The Washington Business Journal reported on 26th March
that Riggs had “spent more than US$5 million trying to come into compliance, but regulators still aren’t satisfied.”

**Renegotiating the merger**

Early 2005, Riggs submitted its latest financials and an update on its compliance and legal issues to PNC. In early February, PNC revised its offer from US$24.25 per Riggs share to US$19.32 per share. The offer was rejected and Riggs filed a suit against PNC.

On February 10th, Riggs accepted PNC’s revised offer of US$20 per share. PNC had reduced the price per share by more than US$4.

The revised offer and Riggs’ acceptance thereof brought a second amended shareholders class action by the Delaware Plaintiffs. The action argued that the board had breached their duty to maximize shareholder value after agreeing to the reduced PNC offer.

**By March 2005**, the ‘Delaware Plaintiffs’ and Riggs had reached a settlement. PNC would finally pay the action group US$2.7 million.


**On July 21st 2005**, the Freeport Partners Action reached an agreement in principle with PNC.

**October 2005**, PNC, the new owners of Riggs agreed to pay US$5.25 million to settle the final shareholder lawsuit it faced26.

**Understanding the effects – reputation fallout**

From late 2002 until Riggs was sold to PNC in mid-2005, we witnessed a series of investigations that resulted in fines and settlements totalling US$59 million. In two years’ time legal and consulting fees topped $35 million. However the true cost of reputation damage is clearly reflected in the drop in share price.

June 15th 2004, Riggs accepted an offer made by PNC of US$24.25 per share. February 10th 2005, Riggs had accepted a renegotiated price of US$20 per share. **An approx. 20% drop in a matter of 8 months. Instead of achieving US$779 million, the shareholders finally accepted approx. US$643 million.**

During a two year period, the banks CEO, Robert Allbritton resigned (March 2005), its Chief Legal Officer, Joseph M. Cahill was replaced (December 2004), the Chief Operating Officer and Executive Vice President (and former MD of Riggs Europe), Robert C. Roane was suspended (September 2004), and the banks former Chief Bank Examiner and Executive Vice President, R. Ashley Lee was put on paid leave (August 2004). In addition the manager of Riggs’ African and Caribbean division, Simon P. Kareri, was fired and ultimately charged with 27 counts ranging from money laundering to fraud (June 2005)27.

“You have rid Chile from the threat of totalitarian government and an archaic economic system based on state-owned property and centralized planning,” Riggs chairman Joe L. Allbritton wrote Pinochet on Nov. 14, 1997. “We in the United States and the rest of the Western hemisphere owe you a tremendous debt of gratitude and I am confident your legacy will have been to provide a more prosperous and safer world for your children and grandchildren.”

**Timeline**

5. Civil suit, class action and derivative compliant brought against officers and directors by shareholders.
6. 28 January 2005: Riggs admits guilt in failing to report suspicious transactions & accepts fine $16m. Riggs also agrees to pay US$9 million to fund for victims of Pinochet.
7. 7 February 2005 – Riggs shares drop 5% after PNC deal collapses. 8th Feb. - Riggs shares tumbled $1.21, or nearly 6 percent, to $20.02. 10th Feb. PNC agree to buy Riggs at $20 per share. Shares in Riggs fell 59 cents, or 2.9 percent, to $19.63 on the Nasdaq.
9. 13 May 2005 – Riggs acquired by PNC

**The final bill**

- Approximately US$59 million in fines, penalties and settlements.
- Numerous very public resignations.
- Hundreds of embarrassing newspaper articles and headlines.
- Millions of dollars in consulting, auditing and legal fees.
- Millions of dollars in software and other AML solutions.
- A very tainted reputation, and ultimately, one of the most respected banks in the U.S. closed its doors and its name ceased to exist after more than 160 years of business.

“PNC is buying damaged goods and they understood that going into the transaction,” said Gerard Cassidy, an analyst at RBC Capital Markets. “The amount of damage has increased and it’s worse than the fines. The fines are the easiest part. The bigger question is the damage that is being done to Riggs’ reputation”
Lessons to be learnt

What must be apparent is that Riggs’s issues were less about banking on behalf of PEPs and much more about what the regulator expects from an institution. Riggs was fined primarily because of a lack of vigilance and procedure only made worse by the purposeful attempting to conceal activities of great concern to the regulator once under investigation. As compliant as Riggs might have been on OFAC, its basic KYC, AML and suspicious reporting procedures were grossly lacking. Some of the following suggestions may seem basic but there are too many institutions that have not yet committed themselves in the way the regulators would approve of.

Legal and compliance risk

■ Ensure your employees are well (and regularly) trained on legal and compliance issues.
■ Ensure the Legal & Compliance departments are properly staffed, have the systems and procedures in place to meet all legislative requirements and that they have a budget to do so. Cutting corners will cost you more in the long run...including, quite possibly, your job and your own reputation!
■ Ensure compliance are empowered to do what needs to be done within your institution.
■ Ensure your compliance team is not made up of only lawyers. Former enforcement and agency staff may be far better trained in investigative methods and are more likely to know how to catch a thief/fraudster/money-launderer etc. Compliance is not only about complying with the law. It’s about understanding and evaluating risks.

PEP risk

■ Ensure your institution is 100% aware of all of its customers that are PEPs – in the broadest sense - no matter how many years ago they were in office.
■ When asked by regulators to disclose all PEPs, do so. Rather err on the side of caution.
■ Do not assist or turn a blind eye to PEPs concealing their identity whether by using alternative spellings of their names, aliases or corporate structures.
■ Do not assist PEPs in setting up (offshore) corporate or trust structures without being prepared to disclose your assistance in the matter.
■ Report all major transactions and large cash deposits related to a PEP especially if they are deposits/gifts by large corporations.
■ Ensure multiple sign offs on all PEP business by officers that are well trained in compliance and legal requirements.
■ When dealing with diplomatic account holders, be aware of the geo-political risks and conditions in their country.
■ Within banking institutions, set up PEP-Desks i.e. a PEP Department with a team of private bankers who are well trained in compliance issues and know how to deal with PEPs.

Correspondent risk

■ Ensure you carry out regular audited due diligence on all correspondent banks, their ownership and management.
■ Continue to review your correspondent banks and the countries they are based in for risk issues.
■ The same is true for referrers of business, law firms and other service providers.

Employee risk

■ Ensure checks and balances are in place and that no (private) banker or trader goes unsupervised, no matter how much of a ‘star’ they are.
■ Bankers responsible for PEPs need additional scrutiny. Have several people sign off on all major PEP transactions.
■ Ensure your employees are well trained in their legal and compliance requirements.
■ Should you bank deal with PEPs from heightened risk countries, ensure your employees are educated and kept updated on the risks that country poses.
■ It is often the case that employees pay an unfairly high price for failure by an institution or its management. One seldom hears about how many people have lost their jobs because of a scandal that brought their employers to their knees.

One should also consider…

■ Shareholder risk – the risk of management being sued because of incompetence or noncompliance.
■ Management risk – the risk of being sued by shareholders, being investigated by the government and ultimately going to jail
■ Jurisdictional risk – in smaller jurisdictions a case of this nature and magnitude would have a knock on effect on the entire financial community.

…however of primary concern must be one’s …

Reputational risk

■ Understand that your institution is only as good as its name and reputation.
■ Ensure all board members, management and employees understand this.
■ Set out to improve your reputation every day and do so by measuring, understanding and mitigating your risks.
■ Never underestimate the ‘bad guys’ – they are craftier then you think. They set out everyday to do what they need to do. You have to set out every day to prevent them from doing it at your institution.
■ Set up a Damage Control Team to include internal and external marketing teams for when it does go wrong. Have a strategy to put out fires.
■ Understand that a good compliance team should not be seen as a department that ‘costs money’ but rather as a ‘reputation protection department’ that could save you millions (and your job!).
■ Accept that the mass media would love nothing more than to cover their front pages with articles of ‘greedy bankers doing business with the bad guys’.
■ As your institutions shares plummet, the company is put up for sale and lawsuits are brought against you, remember you were warned. ■
FOOTNOTES:

2 http://hsgac.senate.gov/_files/PINOCHETREPORTFINALv8charts.pdf
3 http://www.guardian.co.uk/pinochet/Story/0,1488929,00.html
4 US Senate Report: Money Laundering and Foreign Corruption: Enforcement and Effectiveness of the Patriot Act: Case Study involving Riggs Bank
7 http://www.usdoj.gov/usao/DC/Press_Releases/2005_Archive/20050518.htm
11 http://www.time.com/time/world/article/0,8599,8599,00.html
19 http://www.msnbc.msn.com/id/4687305/
23 http://www.occ.treas.gov/_files/ACFS9K.xml
24 http://www.washingtonpost.com/wp-dyn/content/article/2005/10/12/AR2005101202163_pf.html
29 http://abcnews.go.com/Business/wireStory?id=559779
34 http://www.cmht.com/cases_riggsarticle.php
35 http://www.washingtonpost.com/wp-dyn/content/article/2005/05/27/AR2005052701471.html
36 http://www.chile-usa.org/p46.htm

About World-Check

World-Check was founded in late 2000 to meet the specific requirements of the Swiss financial industry.

Today, 5 years on, World-Check intelligence is relied upon by 1600 institutions in more than 120 countries, including over 200 government, enforcement and regulatory agencies in over 90 countries.

45 of the world’s 50 largest financial institutions choose to use World-Check. We serve more institutions than all other PEP vendors put together.

World-Check’s coverage includes PEPs, money launderers, fraudsters, terrorists and sanctioned entities — plus individuals and businesses from over a dozen other categories. World-Check offers a downloadable database for the automated screening of an entire customer base, as well as a simple online service for quick customer screening.

Please visit www.world-check.com for further information or contact World-Check at contact@world-check.com

www.world-check.com
The risks
The US Department of State’s 2005 International Narcotics Control Strategy Report recognises Singapore as a major money laundering country. This report notes that Singapore operates a sizable offshore banking market, and has a significant non-bank financial system with a large number of moneychangers and remittance agencies. Furthermore, Singapore has strict bank secrecy laws and banks will only disclose information about customers and their accounts under narrowly prescribed circumstances. There is also a significant lack of routine currency reporting requirements.

These factors make Singapore vulnerable to foreign drug traffickers, other foreign criminals, terrorist organisations and their supporters seeking to launder their money through Singapore’s banking system.

Singapore is also a hub for transportation in South-East Asia, which increases the risk of the country being a transit point for Golden Triangle heroin. Furthermore, in January 2006, the Government of Singapore announced the Casino Control Bill. This bill lifts the ban on casinos and, as a result, exposes Singapore to the money laundering risks associated with gambling activity and institutions.

Despite the aforementioned risks, Singapore has been recognised as a country with a low rate of corruption. Transparency International’s Corruption Perceptions Index 2005 ranks Singapore as one of the least corrupt nations in the world, with a country rank of 5 out of 158 in the 2005 index.

The response
Singapore has demonstrated a strong commitment to implementing an effective AML/CTF framework. The International Monetary Fund and the World Bank Financial Sector Assessment Program (FSAP) concluded in April 2004 that Singapore “has in place a sound and comprehensive legal,
Anti-money laundering

enacted the Mutual Assistance in Criminal Matters Act in March 2000 to enhance international cooperation in law enforcement and information exchange. However, the FSAP noted serious limitations remained surrounding the provision of bank records, search and seizure of evidence, restraining proceeds of crime, and the enforcement of foreign confiscation orders.

In conclusion
Singapore continues to demonstrate a strong commitment to addressing the money laundering and terrorist financing risks associated with doing business in its country. The current AML/CTF legal, institutional, and policy and supervisory framework is considered to be sound and comprehensive. Despite this proactive approach, Australian organisations with business interests in Singapore should be aware that the sizable offshore financial sector, bank secrecy laws and lack of routine currency reporting may make the country attractive to those seeking to launder money.

Further, Singapore has demonstrated its commitment to AML/CTF as a member of the Financial Action Task Force, Asia-Pacific Group on Money Laundering and Egmont Group. Singapore is also party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism and has signed, but not yet ratified, the UN Convention against Transnational Organised Crime

Singapore has enacted anti-money laundering laws for narcotic offences and other serious offences, and anti-terrorist laws for terrorist financing. In 2002, the Monetary Authority of Singapore (MAS) issued a series of AML/CTF regulatory guidelines or ‘notices’ that are applicable to the financial sector and are enforceable by prosecution. In January 2005, MAS issued a consultation paper revising Singapore’s current AML/CTF regulations to reflect international standards.

Singapore has few restrictions on providing inter-governmental mutual assistance for terrorist financing-related matters. Singapore

---

1 Defined as a country or jurisdiction whose ‘financial institutions engage in transactions involving significant proceeds from all serious crime’.
2 The CPI ranks more than 150 countries in terms of perceived levels of corruption, as determined by expert assessments and opinion surveys.
The master plan

Combating money laundering is a complex and involved process. As practitioners grapple with new legislation, the development of internal systems and the training of staff, John Mair asks, “How do you ensure that what you are doing is making a difference?”

You’ve identified your customer, researched some background information, trained your staff, have a transaction monitoring system, and send a reasonable number of SAR’s in good faith to your FIU. You probably feel that you have done well. You will probably have had to fight hard for the resources and may have got most of what you asked for. In good shape then? You could be, but not because of all the above. What you have done would have satisfied the majority of onlookers – in name and theme. It has probably been hard work and there will be a sense of achievement. But have you made any difference? Was it worth it? Are you protected from criticism and will you pass the hindsight test?

It is hard enough to organise all the input activity without trying to assess its value. But what was the point if the outputs and outcomes are uncertain? One of the advantages of the regulatory shift from prescription and inputs to design and outcomes is that there’s a greater chance that the resources expended will be more productive and even more proportionate. But this isn’t guaranteed, and increasingly outputs will be tested not by what they look like, but how well they survive the hindsight test. Could you, should you, and have others, done better? You can assume that sooner or later you will have a nasty transaction or counterparty, and how will you fare in the glare?

If your implementation selects the right risks, and still one case slips through, then you probably deserve to feel some comfort. Your risk based approach, a mantra of many, picked out the real risky transactions and counterparties, the risk calibration adjusted naturally to reflect that the canny criminal may have penetrated you and steered clear of your original high ‘risk areas’. You can conclude you may still be hitting the right targets. But most are probably calibrating their risk, codifying it and making that higher risk area less likely to harbour the canny criminal than even before.

In other words, as soon as you designate an area or activity higher risk, the serious and organised criminal takes his or her ‘high risk’ transactions or selves to areas you have designated lower risk – which in the ‘risk based approach’ of many practitioners receives less scrutiny. The angle of attack has shifted.

Can we learn from elsewhere how to make more of a difference then? Possibly from your AML colleagues, but maybe everyone has just benchmarked themselves to the same approach and built the most superb ‘Maginot lines’. Perhaps asset management teaches AML better. Trying to pick the best investment is not so different from trying to pick the nastiest customer transactions. Or to take another analogy, it is about as hard to win a quiz as it is to come last, provided you are not trying to lose. How often do most asset managers beat their index consistently, predictably and in an organised fashion? Why is there a place for diversification, avoiding correlation? And is there a similar advantage in not being so certain that we can designate some transactions and customers
as ‘high risk’? If we can correctly identify suspicious transactions, why do we not do this successfully in selecting investments; and why the success of index trackers? So why is it a good idea to be highly focussed on picking the equivalent of winners? Who consistently manages investments well, even with the transparency and information flow of the open market; and how much more difficult is it to do this with the opacity and deceit of serious criminality?

So, how will we make a difference? In asset management, managers who consistently come closest to ‘selected success’ are the truly brilliant. After the truly brilliant, the best seem to be the trackers. I can hear cogs moving. Who do we know, and how many are there, who fall into the category of truly brilliant AML managers and leaders?

We’re getting there. If the challenge of AML and anti-terrorist finance really is important, and we truly want to make a difference, then brilliance is needed, not just diligence. Could it even be that the equivalent of the tracker fund is required whilst we develop or find ‘the brilliant’? Now that is an irreverent suggestion. But would you really give a poor marksman a sniper’s rifle to hit a small target, or would you give him a shotgun? If this really is an important challenge (which I believe it is), and in the absence of the brilliant, I am unsure that I would put all my eggs in the risk based basket.

So, some help? Whilst the brilliant emerge (are they or will they?), get the best advice you can. Build the links with the people who can provide you with brilliant ideas – public and private sector. Be prepared to change your views. And when the hindsight test exposes you, your firm, or your department (which is bound to happen, unless you are certain who all the baddies are), make sure you can, first, honestly think and, secondly, honestly say you did your best – you engaged the right people and used the right tools. Because if you gave a sniper’s rifle to someone who could neither see nor hit the correct target, you will spend far more time and money clearing up the mess, under the close scrutiny of media and regulator, than if you had employed the right tradesman with the right tools, for the job in hand.

Next time: process vs. culture – why balance of both is vital. If you can only have one, it certainly isn’t process that will save you.

---

### Anti-Money Laundering Manager (Sydney)

- Very attractive package
- Sydney CBD base with national travel opportunities
- Highly visible position

This position occupies a pivotal role within the Sydney practice of an internationally recognised professional services firm. This firm has a commitment to recruiting excellence and offering their staff unparalleled continued growth.

Our client’s Fraud and Corporate Investigative practice has grown substantially over the past 12 months and this impressive growth is expected to continue with no anticipated down turn. As such they are seeking an experienced AML professional to cope with this demand and grow with the business.

To be successful in this position you will possess the following attributes:
- be aware and familiar with the new and upcoming AML legislation in Australia
- have an understanding of the importance of AML legislation and its application to business environments
- have an enquiring, questioning and consultative style together with excellent communication, presentation and report writing skills

This role will include:
- Analysis of prospective client products/services in relation to AML
- Research into international AML legislative reform
- Assisting with engagement assignment management
- Report writing and presentation

This is an interesting and challenging opportunity where your skills and knowledge will be tested. Our client has the resources to give successful applicants access to cutting edge methodologies and practices in the AML legislative arena together with outstanding career prospects.

If you think you have what it takes to make a contribution in this top tier consultative environment please email your resume to apply@curtispartnership.com.au quoting reference CPF02

Curtis Partnership Pty Ltd | Recruitment Specialists | www.curtispartnership.com.au
Reporting suspicions

Let’s ‘bust’ some myths

This review of suspicion reporting is the first of a regular column by Joe Garbutt. Joe is currently Senior Manager, Group Compliance Risk, at National Australia Bank, but he draws on his previous UK experience as a Money Laundering Reporting Officer and previous Australian AML experience for this column. Joe was a member of the British Bankers Association’s Money Laundering Advisory Panel from 2002-2004.

Myth: No Suspicions, no problem. As we have not reported any suspicions, we can’t have a money laundering problem. **Myth buster:** If you are a large firm you may well have a problem of non-reporting – go and check by doing a survey to see if your people know what a suspicion might look like, and if they know how to report one.

Myth: Too many suspicions, we have a problem. Being exactly opposite of the above (our people have been well trained and the numbers of our reports are growing) – we are concerned we have a problem. **Myth buster:** Don’t worry. Most people are not criminals but there is enough money laundering for large firms to have a number of suspicions – growing the number of reports complies with the law, may help fight financial crime and protects your stakeholders (including your genuine customers) and reputation – it is not a problem.

Myth: It is probably safer to over-report. We report any transactions that we consider unusual. **Myth buster:** Report only suspicions; it is not good to report transactions that are simply unusual. For example, firms that operate automated monitoring systems will typically report only a small minority of unusual transactions as suspicious. A single cash deposit of a few thousand dollars may be unusual for the profile of a particular customer but not of itself suspicious. If this turns into a series of deposits that look as if they are designed to avoid the $10,000 cash reporting limit, these transactions will be suspicious.

Myth: We don’t like ‘dobbing in’ our customers. We don’t like the idea of “dobbing them in” particularly our long term clients. **Myth buster:** Think this through. The law requires that you must report your suspicion. Think about what money laundering is. Money laundering derives from crimes with real victims. As to dobbing them in, don’t worry – it’s up to others to prove whether crime exists, you have done your job by reporting.

Myth: Well, we have reported the customers, let’s get rid of them to stop future problems. **Myth buster:** Be very very careful. It is an offence to ‘tip off’ the customer that a report has been made. You have to continue to treat the customer as you would any other in your dealings with them, but of course you may need to report subsequent transactions as suspicious. Closing the account simply because a suspicion has been reported, without clear reason, could alert the customer. Depending on the circumstances, this could be construed as ‘tipping off’. However, you could close the account if this is justified by normal business reasons, as you would for any other customer. An example would be if the customer had breached the terms and conditions of the product. Of course in rare circumstances, the authorities can subject individual accounts to freezing orders.

Myth: We don’t have to worry about tax evasion, it’s white collar crime – not like drugs trafficking and so on. **Myth buster:** The law requires you to report all suspicions of tax evasion so it is not up to you to pick and choose what to report and not report. Nevertheless, think this through – how do you know the customer is limiting their crimes to tax evasion anyway? Organised criminals probably don’t make the best taxpayers. Equally tax could be mis-represented to you as the reason to launder drugs money, for example. In any event, tax evasion is stealing from society.

Myth: We don’t have to worry about fraud, our fraud team have already dealt with the police. **Myth buster:** Wrong on a number of counts. Firstly the law requires it. Secondly, the report may help identify new or larger crimes, by being put onto the national intelligence computer systems, and may also link to other pieces of intelligence.

Joe Garbutt, Senior Manager, Group Compliance Risk, National Australia Bank
Thirdly, it is well documented that terrorists use fraud to finance their activities so you may be making a major contribution there. Protect your firm’s reputation and comply with legal requirements by reporting fraud.

**Myth: I am never going to recognise a terrorist or major organised crime ring, it’s all too hard. My firm’s not bothering too much with it.**

**Myth buster:** You don’t have to be a detective – all you have to do is to report suspicious transactions. You do not have to be aware of what the underlying crime is that may be generating the suspicion. In fact you will probably often not have any idea, though the scale of the drugs trade can lead to very large amounts of dirty cash being placed into the financial system, so that is an obvious one. There is no excuse not to train your people and report suspicions.

**Myth: Nothing seems to happen, it is a waste of time.**

**Myth buster:** Read the newspapers or do internet searches. There are plenty of successes. There is much public domain material to show success in the fight against financial crime. See for example the UK fortnightly newsletters on [www.assetsrecovery.gov.uk](http://www.assetsrecovery.gov.uk)

**No myth: I have had enough of this Pommie, tell me where I can get further information.**

**Answer:** Fine, see [www.austrac.gov.au](http://www.austrac.gov.au)

The views in the article represent Joe’s personal opinion and he is not speaking for National Australia Bank in this article. Where Joe refers to what the law requires, he is referring to current laws applying to cash dealers.
from overseas, which is why I would encourage Australian banks to reach out to their foreign subsidiaries and partners to ask them how they tackled the challenge of developing an AML program. Simple questions like, ‘when the legislation came out what were your first steps’, ‘what solutions proved a good investment’ and ‘what have you binned in the last year’, can prove invaluable.

In terms of new trends, I think the risk based approach will continue to remain a buzzword in 2006. It will be interesting to see how Australian banks embrace the approach, building process and procedure around it. While conceptually it makes a lot of sense, there is still a long way to go until banks understand the full operational implications.

Another development I’ve witnessed first hand in the UK and Europe is a trend towards using third parties to verify customer identity. More and more financial institutions are looking to companies like credit rating agencies to confirm customer details. It makes perfect sense.

Why ask a customer for a copy of their gas bill if another company has already collected these details and has access to other sources of verification information, such as electoral roles?

What trends have you seen in the last five years?

While working to help firms build AML programs, I’ve been lucky enough to observe the implementation of anti-money laundering legislation around the globe. One area in which I’ve noticed a trend is development. What I mean by this is that nearly every country I’ve witnessed implementing AML legislation goes through the same process. Visiting clients here in Australia, it’s interesting to hear the same debates around customer identification, PEPs and monitoring that I heard in South Africa two years ago and, before that, in the UK.

The good news for Australia is that there are clear lessons that can be learned
What are some of the challenges you think Australian practitioners might face?

The main challenge facing all practitioners in anti-money laundering is that they still don’t know what they are dealing with. Until the legislation is finalised there is still a lot of guess work going on, which in my experience creates frustration.

What are the business benefits of an effective anti-money laundering program?

I was recently invited to address an audience of senior banking executives on the topic of AML. Before delivering my presentation I asked the audience to raise their hands if they wanted to known as the bank of al-Qaeda. No one raised a hand. I then asked delegates to raise their hands if they wanted to be known as the bank of the mafia. Again, no one raised their hand. The bank of arms dealers? Still no hands.

To me the business benefits of an anti-money laundering program are simple. It makes good business sense to know who you are dealing with. After all, why would you want to do business with criminals. The concepts of customer identification and risk assessment aren’t new. In fact, banks have been defining/developing and applying both for years. When a customer applies for a credit card they don’t just get handed one. The bank performs ‘Know Your Customer’ (KYC) checks to assess their ability to repay the loan. Now we are simply saying, let’s look at KYC not only in terms of credit risk, but as a tool to manage reputational risk.

By understanding who their customers are, banks can make informed decisions about whether they want to do business with them. When it comes down to it, no one wants to make the front pages of the newspapers as the preferred bank of terrorists.

Of course, banks can also benefit financially from more effective KYC. The better a bank knows its customer base, the more effectively it can target new or existing products, potentially increasing sales.

Can you give any examples of the cost of non-compliance?

World-Check has just commissioned a report on the Riggs Bank case, one of the first studies of its kind [see this month’s special report]. Together with David Carusso, the Executive Vice President of Compliance and Security at Riggs from June 2003 to May 2005, we have traced the history of the Riggs debacle and assessed the hard dollar cost of non-compliance.

Riggs Bank was one of the most prestigious financial institutions in the US. Often referred to as the ‘bank of presidents’ it held accounts for over twenty presidents, as well as 95% of all embassy accounts in Washington DC. Riggs was an important bank. Yet over a two year period the bank suffered huge reputational damage caused by a lack of proper AML controls.

If we look at the hard dollar cost of non-compliance, Riggs spent over $59 million in fines and settlements. This included a $25 million fine issued by the OCC for violation of the Bank Secrecy Act. The bank also ran up over $35 million in legal and consulting fees, settling numerous suits brought about by its own shareholders.

But the costs didn’t stop there. The true cost of reputational damage was reflected in the drop in share price. On July 15th 2004, the Riggs Board accepted a bid from PNC, comprising of a combination of cash and PNC common stock. The amount offered was US$24.25 per share. The very same day, a US Senate Committee issued a report concluding that Riggs had ignored directives by federal regulators to improve its anti-money laundering program.

Over the next eight months Riggs faced further shareholder suits, compelling PNC to renegotiate its proposed merger offer. On February 10th 2005, Riggs accepted a revised offer of $20 per share, a drop of approximately 20 percent in less than a year, at a cost of $160 million.

The total cost of non-compliance in the case of Riggs Bank totalled in excess of $250 million. That’s a compelling story for compliance managers to take to their board when developing their AML program.

What does the future hold for AML?

I think we’ll see AML become a true discipline within banks over the next couple of years, as governments develop legislation and financial institutions build internal expertise. This is a problem that is not going to just go away. A report recently estimated money laundering to represent in the region of USD 500 billion to USD 1 trillion annually. That’s almost four times Switzerland’s GDP. Imagine stealing that amount of money and hiding it! Clearly this isn’t happening and money is finding ways back into the banking system. We have to accept our social responsibility as a financial community and continue the good work that has already been started.

As World-Check celebrates its fifth birthday, what does the future hold for you?

Our passion continues to grow with our business. We are signing on average 50 new institutions a month and have some exciting plans in the pipeline to launch four new modules focused on the needs of smaller institutions. We look forward to showcasing some of these new products in the last quarter of 2006.