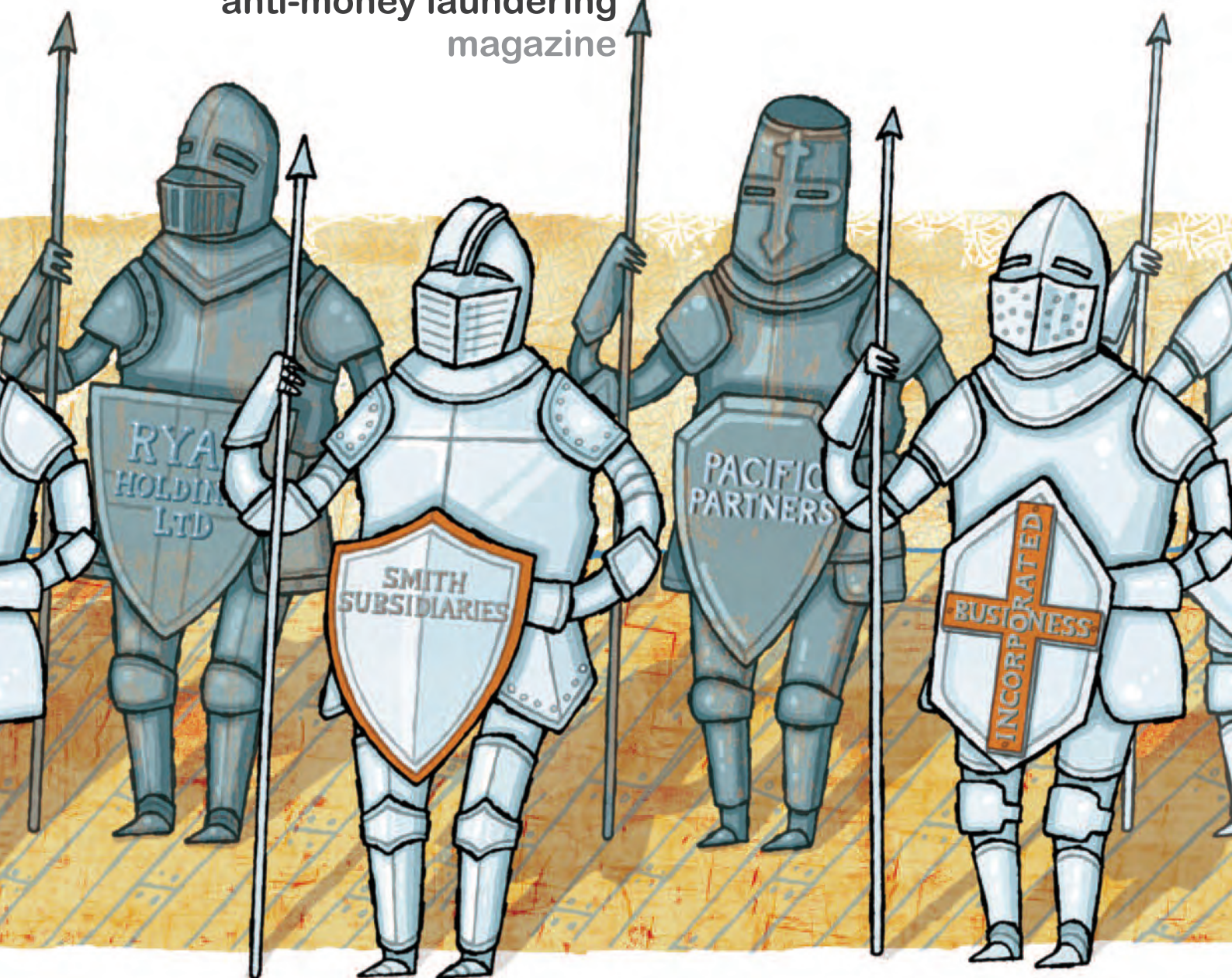


aml.

anti-money laundering
magazine

may 2010

combating money laundering
in financial services



Beneficial ownership

the great moral challenge of the regime

"Not happy Jan" says the FATF
Threat assessments – think global
and act local

Amendments to the AML/CTF Act close
alternative remitters' loophole
Up close and professional with the West



AML Refresh(er) 3 Regulation & Compliance CE Hours

This training course looks at the Australian and international anti-money laundering and counter-terrorism environment in 2010 and trends and issues in the key activities of governance, risk assessment, KYC and monitoring.

This **3 hour workshop** will explore:

- ✓ Governance & Oversight
- ✓ Customer identification procedures
- ✓ Monitoring strategies
- ✓ Case investigation and suspicious matter reporting

This workshop is designed for new and existing AML/CTF Compliance Officers who would benefit from re-cap training. It would also be suitable for senior management staff of smaller reporting entities who would like to further understand the legal, regulatory and compliance issues faced by their organisation with the implementation and ongoing maintenance of an AML Program.

Sydney 15 June 2010 | Melbourne 17 June 2010 | 9am – 12pm | \$869.00 inc GST

To register or for more information contact Jason Sheil 02 9776 7914 jsheil@afma.com.au

The great moral challenge of our regime

It is tempting to say that beneficial ownership is the great moral challenge of the Australian anti-money laundering/counter-terrorism financing regime, indeed of the global Financial Action Task Force regime. Ninety percent of FATF members are not compliant or only partially compliant with FATF Recommendation 5, and one of the main reasons is lack of compliance with the beneficial ownership requirements.



By Joy Geary
EDITOR

AML/CTF systems typically have negative responses to people using aliases, and proprietary companies are no more than avatars or aliases of their beneficial owners. ML/TF risks are unidentified and unmitigated when the beneficial owner has not been identified. As is well known, identification and mitigation of the ML/TF risk that a reporting entity reasonably faces is a required primary purpose of an AML/CTF program for any Australian reporting entity.

Identifying the beneficial owner down to the individual level is thus a fundamental control in any AML/CTF regime. And there is no escaping the FATF's stated expectation that reasonable steps will also be taken to verify the identity of the beneficial owner.

So where is Tranche II – still missing in action?

A small number of the members of the legal and accounting professions help criminals use legal entities and trust structures to launder money. A greater number of the members of those two professions may unwittingly provide this assistance without the benefit of conducting proper due diligence on their clients' activities. Government agencies with key responsibilities for defending the community against organised crime are on public record as saying that organised crime depends on the services of specialists such as lawyers and accountants to enjoy the benefits of their acquisitive crimes. The FATF recommendations relating to gatekeepers aim to make this partnership riskier and more difficult for the professional. So where is Tranche II – still missing in action?

The overseas experience provides little assistance, as other regimes also struggle to comply with the beneficial ownership elements of FATF Recommendation 5. US Senator Carl Levin, Chairman of the Senate Permanent Subcommittee on Homeland Security and Governmental Affairs, published a report in February 2010. This report shone a bright light on how proprietary companies home-grown in the US – together with the eager skills of lawyers, accountants, real estate agents and escrow agents – were put to work to launder hundreds of millions of dollars for overseas politically-exposed persons from Equatorial Guinea, Gabon, Nigeria and Angola, in part through lax practices regarding beneficial ownership.

Closer to home, a website which offers incorporation services for companies in New Zealand says the following about the nominee director services it is happy to provide:

A director whose function is passive in nature. The director receives a fee for lending his or her name to the organization. Nominee directors are subject to director responsibilities. Nominee directors are directors that [we] appoint for you. Each corporation or foundation must have a certain minimum number of directors appointed when registered. The directors' names and some of their personal details are on the public deed of the corporation (or foundation) and this information is publicly available. In many cases, [our] clients prefer NOT to be appointed as directors on the offshore entities due to either privacy reasons, or foreign public directorship reporting rules in their home countries. The nominee directors [we] appoint are only there to fill in the blanks at the public registry and they have no authority over the entity for any kind of decision making.

And the same website promotes the following:

New Zealand Tax Free Special Purpose Company: If the New Zealand company and Trust have no connection to New Zealand, the complete structure is non-taxable in New Zealand. The company owner and Trust beneficiary may be the same person. Once incorporated, the company is generally free to do business, open bank accounts, or invest anywhere in the world. In effect, it can operate as a tax-free offshore company but without the "tax haven" implications of the traditional offshore centres.

The implication of that last sentence is clear: New Zealand is regarded as low risk, it is a FATF member, it is not regarded as an important regional financial centre, and it scores well on the usual range of indicators used to measure ML/TF country risk. By using a NZ Tax Free Special Purpose Company, combined with nominee director services to "fill in the blanks at the public registry", it is possible to travel well under the radar of ML/TF country risk models used by financial institutions around the world.

There is a convergence of issues going on – opaque entities; low and easy incorporation standards; generous approaches to identifying beneficial owners by FATF members, including Australia; and lawyers, accountants and real estate agents outside the AML/CTF regime in many countries, also including Australia. The holes in the AML/CTF fishing net are big enough for all self-respecting criminals and their specialist advisers to swim through with ease.

continues page 8 ►



Who is hiding in your customer base?

Over 3 000 institutions worldwide rely on World-Check for their
KYC, AML and Enhanced Due Diligence (EDD) compliance requirements.

www.world-check.com

About World-Check

World-Check's risk intelligence on heightened-risk individuals and entities is updated daily in real-time by its international research team, and is derived from hundreds of thousands of public sources. Coverage includes money launderers, financial criminals, terrorists and sanctioned entities, as well as individuals and businesses from more than a dozen other high-risk categories. The database also covers Politically Exposed Persons (PEPs), their family members and associates worldwide. World-Check's intelligence and tools find direct application in financial compliance, Anti Money Laundering (AML), Know Your Customer (KYC), PEP screening, Enhanced Due Diligence (EDD), fraud prevention, government intelligence and other identity authentication, background screening and risk prevention practices. 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. If you are looking for results, look no further – with a 97% annual client renewal rate, the facts speak for themselves.



Features



6 Fees for IFTIs: AUSTRAC to introduce \$30m 'user pays' model

9 News

14 Letter to the Editor

BENEFICIAL OWNERSHIP

16 Part II – Who the bloody hell are you?

20 Part III – International approaches

24 Not happy, Jan! The FATF's view of Australia's AML/CTF regime

27 AUSTRAC's AML/CTF Compliance Officers survey

AUSTRAC COLUMN

Enhanced regulation of alternative remittance dealers

30 Lenders Beware!

32 National threat assessments – where would we be without them?

34 Australia's first Organised Crime Threat Assessment

38 Internal Fraud – Managing the fallout from the GFC

42 Catch up on the amendments to the AML/CTF Act

UP CLOSE AND PROFESSIONAL WITH THE WEST

Peter Robinson – Operations Manager, Patersons Securities, WA

46 India and the evolving, adaptable methods of terrorist financing

48 World-Check special crime and terrorism series:
illegal sports betting

EDITORIAL

EDITOR:

Joy Geary – jgeary@afma.com.au

SUB-EDITOR:

Roger Balch

CONTRIBUTORS:

Gordon Hook (APG), Dr. Hugh McDermott, Greg Standing (Wragge & Co. U.K.), Adam Courtenay, Dr. Nick Ridley (United Kingdom), BC Tan (World-Check).

PRODUCTION AND DESIGN

CREATIVE DIRECTOR:

Jo Fuller

COVER DESIGN:

Elly Walton Illustrations (UK)

ADVERTISING AND SUBSCRIPTIONS

MANAGER, MARKETING:

Jason Sheil –
Tel: + 61 2 9776 7914
jsheil@amlmagazine.com.au



ANTI-MONEY LAUNDERING MAGAZINE
IS PUBLISHED BY

AFMA – Level 3, 95 Pitt Street, Sydney NSW 2000.
GPO Box 3655, Sydney NSW 2001
Tel: + 61 2 9776 4411 Fax: + 61 2 9776 4488
www.afma.com.au

Disclaimer: This publication is designed to provide accurate and authoritative information in regard to the subjects covered. It is distributed with the understanding that the AFMA is not engaged in rendering legal, accounting or other professional service. If legal advice or other expert assistance is required, the services of competent professional persons should be sought. AFMA Anti-money laundering magazine presents the views of a range of commentators on AML issues for the benefit of readers and AFMA does not necessarily endorse these views.

This publication is copyright. Other than for the purposes of, and subject to the conditions prescribed under the Copyright Act 1968, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system, or transmitted without prior permission. Enquiries should be addressed to AFMA.

Fees for IFTIs:

AUSTRAC to introduce \$30m 'user pays' model

After almost two decades of resistance, the Australian anti-money laundering regulator has relented to government pressure and will begin charging reporting entities to register and file transaction reports from July next year. The funding bombshell was buried in this year's Budget papers, which state that AUSTRAC will levy around \$30m annually in fees to cover the cost of its regulatory activities. While the agency's intelligence function will continue to be underwritten by the government, the regulatory arm is expected to cover its costs from the 2012 financial year onwards.

Under the proposed fee structure AUSTRAC will charge reporting entities a flat fee of \$500 for registering with the regulator each year. Based on an estimated population of 17,000 reporting entities, this will raise around \$8.5m annually. AUSTRAC's budgeted revenue of \$29.6m in 2011 means that it will have to collect an additional \$21m from reporting entities for filing certain transaction reports.

At this stage AUSTRAC says it plans to target IFTIs and TTRs — international funds transfer instructions and threshold transaction reports. The proposed fee would be set at \$1.06 per transaction reported, generating the lion's share of its revenue over the initial three-year period from July 2011 onwards.

Since as far back as the early 1990s, AUSTRAC has resisted pressure from within the government to levy a fee to cover its services. In 1993 there was a proposal to charge AUSTRAC's partner agencies — those that use its data — for the financial intelligence unit's services. AUSTRAC said at the time that it was "decidedly opposed to its clients having to pay a money cost."

While the proposal pre-dated AUSTRAC's regulatory functions, it said then that its FIU role was "part of a program being promoted by government and the parliament to better focus law enforcement and revenue administrators

on issues concerning financial misbehaviour and certain types of tax evasion." As such, AUSTRAC said that to charge other government agencies for its data would be a "retrograde step in the promotion of that goal."

A decade later in 2003 the government revisited the idea of charging AUSTRAC's "clients" for the use of its data. Again, AUSTRAC rallied strongly against these proposals, arguing that they ran counter to the broader policy at stake. AUSTRAC argued — successfully — that the government should continue to fund its FIU efforts directly.

In its 2003/4 annual report AUSTRAC noted, rather obliquely: "As an outcome of the 2003/4 Budget process, AUSTRAC was asked to review whether a cost recovery regime could appropriately apply to its services and to provide cost recovery options for consideration in the 2004/5 Budget process. The government is not pursuing cost recovery arrangements for AUSTRAC."

In this year's Budget, things have changed. Instead of charging partner agencies for AUSTRAC's services the government has gone a step further and shifted the financial responsibility to reporting entities.

The outcome of this year's budget, if nothing else, is an indication of how much the fiscal landscape has changed in Australia with the latest Budget. After two decades of suc-

cessful resistance the government has now driven the agency part-way towards a "user pays" model. The government will continue to underwrite the \$31.5m cost of AUSTRAC's FIU work, but its regulatory function will be brought into line with other agencies — such as ASIC and APRA — that levy a fee on the regulated community to cover their services. (In the case of ASIC, of course, the government has gone further still and funnels almost \$300m annually into consolidated revenue, deftly turning regulation into a profit-making enterprise.)

In AUSTRAC's case, the government has argued that it is simply bringing AUSTRAC into line with the Department of Finance and Deregulation's cost recovery guidelines. The guidelines state that: "Agencies should set charges to recover all the costs of products or services where it is efficient to do so, with partial cost recovery to apply only where new arrangements are phased in, where there are government endorsed community service obligations, or for explicit government policy purposes."

The guidelines also state that in instances where the revenue from "cost recovery" is greater than \$5m per year, the regulator in question must consult stakeholders before

putting a framework in place. In view of this, AUSTRAC chief executive John Schmidt said that AUSTRAC would consult on the proposals between May and August this year. Following that consultation the government aims to introduce legislation in the Spring session of parliament.

Schmidt said that AUSTRAC had drafted the fee proposals to ensure that they were consistent with the DFD's cost recovery guidelines. He stressed that there would be no fee associated with suspicious matter reports, whereas income-generating transactions — IFTIs and TTRs — will incur a fee.

He added that most reporting entities would only incur the \$500 annual levy, as they did not handle international transfers or large transactions.

"Many reporting entities regulated by AUSTRAC do not undertake international funds transfer instructions — for instance, entities in the gambling, bullion and non-bank financial services sectors — and no longer accept cash over \$10,000. AUSTRAC would only expect to receive SMRs from these entities, not IFTIs or TTRs," Schmidt noted.

For the financial services sector AUSTRAC's fee announcement has come as a huge surprise. Both the Australian Financial Markets Association and the Australian Bankers' Association said that they were completely unaware that the government had any such plans in the pipeline. They acknowledged, however, that it was not government policy to consult on budget measures prior to their announcement.

The initial reaction from both AFMA and the ABA was that the decision to charge a "per transaction" fee for IFTIs and TTRs was an example of poor policy.

Duncan Fairweather, executive director of AFMA, said that the way the fees had been structured would place a significant burden on the financial sector. In particular, the cost will be concentrated on larger institutions that conduct cross-border transactions and on specialist remittance providers.

"Banks and other financial institutions have spent hundreds of millions of dollars in complying with the AML/CTF law. Now they are being asked to pay more and this extra cost will have to be passed on to customers and/or shareholders," Fairweather warned.

He also noted that the cost of recovery seemed extremely high, with AUSTRAC setting aside \$17m over three years to collect a total of \$80m in fees. Fairweather said that at first glance this raised significant concerns about the efficiency of the fee collection process.

At a broader policy level, AFMA will question whether it is appropriate to levy a fee on reporting entities when the AML/CTF regime is in fact an obligation that the government agreed to via its international commitments to the Financial Action Task Force.

"AUSTRAC is part of Australia's national security and crime prevention framework. This is an obligation on government and it can be questioned whether the cost of this should be imposed on financial institutions and their customers," Fairweather said.

Over at the ABA, the sentiment towards the proposed fee structure was equally pessimistic. Tony Burke, acting chief executive of the ABA, said that his organisation was particularly concerned about the focus of the fees on providers of international funds transfers and large (\$10,000-plus) transactions. He said the cost burden appeared to be designed to target banks and larger institutions rather than being spread across all reporting entities.

"We are concerned because there is scant detail available and there was no consultation on the new fee structure," Burke stated.



there was no consultation on the new fee structure

"It would appear from the information available that the heaviest burden of cost will be borne by a small number of reporting entities. We hope to soon receive more information from AUSTRAC on the changes."

On the other hand, the regulator has taken the view that it is unrealistic to divide the levy evenly between all reporting entities. Given that AUSTRAC needs to raise \$29.6m in the 2012 financial year, if it achieves full registration of 17,000 reporting entities the levy would average out at \$1741 per entity. If the regulator followed this path it would be accused of placing an unfair burden on smaller entities, such as the stereotypical one or two-person remittance provider.

In the AML community, meanwhile, consultants warned that firms at the "smaller end of town" would also find fault with the new flat fee structure for registrations. Although the big reporting entities occupy

a sizeable proportion of AUSTRAC's supervisory effort, consistent with their risk profiles as banks, they will pay the same flat fee as smaller reporting entities. Managed funds big and small will pay the same flat fee, as will superannuation funds of all sizes.

MSBs go underground

They also said the new policy risked driving some of the fringe elements of the "designated service provider" population even further underground. In the case of remittance providers, the new fee for submitting IFTIs would be compounded by the tighter regulatory regime announced by the government. The end result could be that underground operators are even less likely to register with AUSTRAC or submit all of their IFTI and TTR reports if there are cash costs involved.

One industry contact said that the tax on IFTIs would inevitably hit those who can least afford it. She said the proposed fee of \$1.06 per IFTI would inevitably be passed on to the entity or individual that makes the transaction.

In the case of the remittance sector, it would end up being a "tax on the poor, on the consumer, who use these services."

She also said that the flat registration fee failed to take into account the size of the reporting entity. While the reporting fees would target certain business sectors, the \$500 annual registration fee would be a disproportionate burden on smaller entities.

"A small 'cash in transit' business, for instance, will pay \$500, just like a large bank," she noted. "Many of these businesses almost do not make a profit out of carrying cash but do it to make their security services sufficient as a one stop shop."

"There will be an almighty battle between the big guys, who sub-contract a lot of their work down to the little guys in the cash in transit space and have been making them do

the reports for them. So that fee will be incurred again by the little guy who is also struggling under an extra piece of compliance — but may have little ability to pass on the cost,” she predicted.

Defensive reporting

Another interesting outcome could emerge for banks that have been taking a “defensive” approach to reporting all of their international funds transfers. Due to the complexity of determining whether transactions are reportable as IFTIs or not, some institutions have simply been reporting them all. The new fee structure may see these entities revisiting their reporting frameworks to avoid paying fees unnecessarily.

At the same time, if fees are charged for TTRs (cash transactions of more than \$10,000), it could encourage some cash businesses to engage in structuring to avoid the fee. The end result for AUSTRAC would be less threshold reports and less financial intelligence.

“Structuring is a serious criminal offence but people might engage in it unknowingly because they, as a matter of principle, wish to avoid a fee which they take a philosophical objection to,” said the industry contact.

She said that a business that lodged more than \$10,000 in cash into its bank account daily could face around \$250 in additional bank charges. One response could be to bank twice daily instead of once.



“Imagine if the banks introduced a new annual fee of \$250 per annum just to place deposits in an account ... One would expect the government to robustly attack such a move on behalf of the community at large.”

“Imagine if the banks introduced a new annual fee of \$250 per annum just to place deposits in an account,” she mused. “One would expect the government to robustly attack such a move on behalf of the community at large.”

In addition, people using cash-in-transit services may be subject to two fees for a delivery to their bank of more than \$10,000 — one by the cash in transit dealer who has to make the TTR and then one by the bank who has to make the same report.

She concluded that this impost was a great pity, placing consolidated revenue well ahead of the overall quality of compliance with the AML/CTF regime.

“This new regime has a long way to go before it is effective across all sectors and these fees will do nothing to win the hearts and minds of reporting entities, particularly small business who remain somewhat confused by the legislation and its requirements,” she concluded.

From AUSTRAC’s perspective, the AML regime has real benefits for businesses. As such, the fees that they will be expected to pay from 2011 will be more than offset by the lower risk of fraud and the reputational benefits.

“Compliance with AUSTRAC’s regulatory requirements protects firms’ reputations by reducing the likelihood that criminals will use them for illicit purposes,” Schmidt noted.

He also warned that AUSTRAC would come down hard on any business that attempted to circumvent the new rules — via structuring or under-reporting, for example.

“Failure to report can trigger a range of enforcement actions by AUSTRAC, including remedial directions, the acceptance of enforceable undertakings, the appointment of an external auditor and civil penalty action in the Federal Court,” Schmidt said. ■

◀ from page 3 – editorial ...

The FATF is unhappy with the Australian AML/CTF regime and will not release Australia from annual reporting obligations, primarily because of problems with the way Australia has implemented Recommendation 5. Prepare for changes to beneficial ownership and the triggers, as well as the requirements of enhanced customer due diligence.

It is vital that the industry engages with AUSTRAC on how to meet the FATF objections and for AUSTRAC to manage this as a total issue and not in a piecemeal fashion. Issues are interlinked and changes in one place displace obligations already in play in other spaces. Pressure needs to be maintained on AUSTRAC and the Government for delivery on the commitment made to industry during the final stages of the consultation phase for the AML/CTF Act — that Tranche II will be introduced within

12 months of the passage of the legislation.

Earlier this month we conducted *AML Magazine’s* first webinar on assurance. It is part of AFMA’s drive to offer leading-edge information channels in an environmentally friendly manner. Neil Jeans, in the new role of General Manager Group Assurance at NAB, led the discussion on assurance and according to the feedback received, the webinar was a great success. The next webinar in the series will be in July, looking at getting ready for a visit from AUSTRAC.

Assurance delivers many benefits — in short it is the safety net for AML/CTF Compliance Officers. It provides among other things, traceable evidence of the degree of success of risk management; proof that controls are effective and efficient in design, and operation and data for performance measures.

Dates for your diaries — *AML Magazine’s* annual conference will be held on 15th and

16th November in Sydney. The theme is “Partnership — the DNA of combating financial crime and money laundering” and we will be hosting a number of guests from overseas, together with local experts.

This is the twenty-fourth issue of the magazine and my twelfth as editor. We are conducting a survey of readers to better align the magazine to your needs. If you wish to respond to the survey before the next issue please contact jsheil@amlmagazine.com.au. If we don’t hear from you, then we don’t know what you want!

And finally, the breaking news that AUSTRAC will start charging reporting entities a \$500 annual fee plus \$1.06 per international fund transfer instruction and threshold transaction report lodged is disappointing. There are a range of objections to the proposal, from the way the fee is calculated to its disincentive quality. We will focus on these matters in our next issue. ■

Breaking news as we went to print

THE FORMER ABN AMRO Bank N.V., now named the Royal Bank of Scotland N.V., has agreed to forfeit \$500 million to the United States in connection with a conspiracy to defraud the United States, to violate the International Emergency Economic Powers Act (IEEPA) and to violate the Trading with the Enemy Act (TWEA), as well as a violation of the Bank Secrecy Act (BSA), announced Assistant Attorney General Lanny A. Breuer of the Criminal Division and U.S. Attorney Ronald C. Machen Jr., for the District of Columbia.

RBS, part of a trio of banks that bought ABN in 2007, said the consortium had agreed to a \$500 million fine as part of a final settlement with U.S. authorities. The payment was covered by the provision made before ABN was bought.

"ABN AMRO facilitated the movement of illegal money through the U.S. financial system by stripping information from transactions and turning a blind eye to its compliance obligations," said Assistant Attorney General Breuer. "It is essential that financial institutions both large and small properly monitor the origins of funds flowing into our financial system. When financial institutions fail to do so, and, even worse, manipulate information in order to profit from prohibited transactions, they will be held accountable."

"Over the course of a decade, ABN AMRO assisted sanctioned countries and entities in evading U.S. laws by facilitating hundreds of millions of U.S. dollar transactions," said U.S. Attorney Machen.

According to court documents, ABN AMRO used similar stripping procedures when processing U.S. dollar checks, traveler's checks, letters of credit and foreign exchange transactions related to sanctioned countries. ABN AMRO and the sanctioned entities knew and discussed the fact that, without such alterations, amendments and code words, the automated OFAC filters at banks in the United States would likely halt the payment messages and other transactions, and, in many cases, the banks would reject or block the sanctions-related transactions and report the same to OFAC. By removing or altering material information, these payments and other transactions would pass undetected through filters at U.S. financial institutions. This scheme allowed U.S. sanctioned countries and entities to move hundreds of millions of dollars through the U.S. financial system.

"If global banks and businesses wish to conduct financial transactions in America, they are welcome to do so as long as they abide by our laws that govern those transactions," said Victor S. O. Song, Chief, IRS Criminal Investigation. "The IRS is proud to share its hallmark financial investigative expertise in this and other increasingly sophisticated financial investigations. Indeed, creating new strategies and models of cooperation among governments on international financial compliance is a top priority for the IRS."

Last year, British bank Lloyds was fined \$350 million by U.S. authorities on similar charges it faked records so clients from Iran, Sudan and elsewhere could do business within the U.S. banking system. Credit Suisse paid \$538 million in fines in December.

FATF public statements start to bite

REMEMBER the February statements made by the Financial Action Task Force that identified eight countries with strategic AML/CTF deficiencies? In March 2010, the US Financial Crimes Enforcement Network (FINCEN) issued an advisory to regulated businesses stipulating its expectations regarding the levels of due diligence to be applied to customers and transactions involving the countries named.

PayPal competitor Payoneer is an online payment distribution solution established in 2005 which has delivered millions of payments to hundreds of thousands of people around the world using a prepaid MasterCard. Payoneer is headquartered in New York and is a registered MasterCard merchant service provider, partnering with MetaBank and Choice Bank to deliver services.

Payoneer has just advised its customers that, due to a change in requirements from regulators, as of June 1, 2010, Payoneer cards will be blocked for transactions in the countries listed by the US Government as having strategic AML deficiencies. This change will affect card usage in Angola, Ecuador, Ethiopia, Pakistan, Turkmenistan and Sao Tome and Principe (six of the eight covered by the FATF February Statement and backed up by the FINCEN Statement).

Payoneer's response appears to have been to regard these countries as excessive risk for its business model. Of the countries named in the FATF Statement, Payoneer's competitor, PayPal, still allows customers

to send international fund transfers only to Ecuador according to its website.

Operation Goldfinger

SIR SEAN CONNERY has been ordered to give evidence at a court in Spain in regard to an alleged money-laundering scam. The actor, his wife, and members of a law firm based in Marbella, on the Costa del Sol, have been summoned to appear before the court in Marbella later this month.

The former James Bond star and his French artist wife, Micheline Roquebrune, have not been charged with any offence nor arrested. Sir Sean's wife told *The Times*: "These allegations of money laundering are nonsense. We have nothing to do with this. We sold the property and that's it."

Under the codename Operation Goldfinger, police raided the offices of the Díaz-Bastien & Truán law firm in Marbella and Madrid on Wednesday and removed 30,000 documents. No arrests were made. The case centres on the star's former mansion Casa Malibu, according to sources cited by *El Mundo* newspaper yesterday. There is no suggestion that Sir Sean or his wife were involved in any wrongdoing.

JMLSG new draft Guidance

THE JOINT Money Laundering Steering Group (JMLSG) has published a proposed new Part III to its guidance. The draft guidance is open for public consultation until 9 July 2010. It proposes to give guidance in the following areas:

1. Transparency in electronic payments (Wire Transfers)
2. Equivalent jurisdictions
3. Equivalent markets
4. Compliance with the UK financial sanctions regime
5. Directions under the Counter Terrorism Act 2008
6. Proliferation financing

The sections on wire transfers and sanctions provide useful insight into what is considered best practice in these areas.

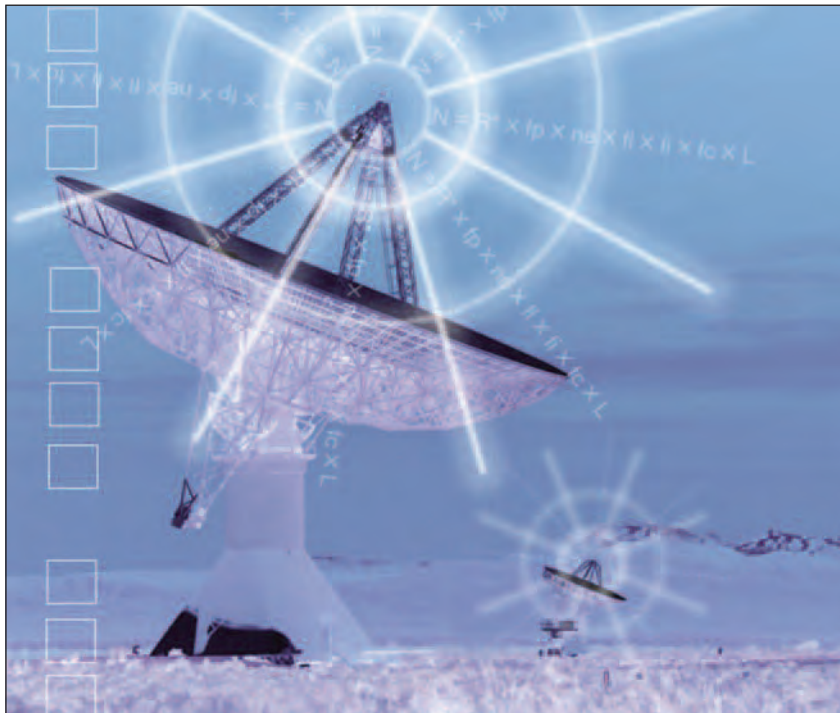
Canberra boosts oversight of remittance sector

INDUSTRY FIGURES have backed the Australian government's efforts to crack down on the remittance sector, saying that the reforms need to address a long-standing area of weakness in the anti-money laundering (AML) regime. Commentators such as Neil Jensen, the former head of AUSTRAC, have indicated that remittance providers have been a concern for the Australian money laundering regulator for many years. He said the new tools that the government had proposed would give AUSTRAC the power to provide much tighter oversight of the sector, including the power to refuse registration to the "illegitimate" operators in the industry. At the same time, he warned that the new regime risked driving these elements even further underground. As such it would need to be accompanied by a strong law-enforcement presence to be successful in preventing launderers and terrorist financiers from misusing the sector.

From the regulator's perspective, the remittance sector has proven difficult since the first days of the AML regime. In terms of registrations, remittance dealers have persistently fallen below the industry average. As of February this year, 5891 remittance providers had registered with AUSTRAC, which is a significant improvement from the year before. Yet despite the increase in registrations, the regulator believes there are around 600 providers of designated remittance services that have failed to register. In policy terms, these 600-odd under the radar remittance dealers constitute a huge AML risk.

Under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 as it currently stands, providing remittance services without registering with AUSTRAC is an offence punishable by two years' jail and/or a \$55,000 fine. Policymakers believe that not only are these sanctions inadequate but the laws as they are drafted are far too loose. As an example, anyone can register to be a provider of remittance services – there are no professional standards or suitability criteria that must be met. Any business that registers can provide money transfers and there are no conditions on the way a remitter operates.

One of the biggest problems at present is that AUSTRAC lacks the power to refuse to register a remitter, even if it suspects that the business is non-compliant. Registration is



The view that many have espoused at industry events is that it makes a mockery of the efforts of the compliant if some remitters are seen to be flying beneath the radar.

automatic, provided a remitter can successfully fill out some paperwork, spell their name and lodge an application.

Under the proposed changes to the AML regime, AUSTRAC would be able to assess the suitability of entities that seek to provide remittance services. Applicants would be required to disclose information on the beneficial ownership and control of the business. They would have to declare any criminal convictions, insolvencies, or "history of regulatory non-compliance". They would also have to renew their application every three years, or more frequently if required by AUSTRAC. Those on the register would have to report any changes in their circumstances or the circumstances of their associates.

According to Brendan O'Connor, the Home Affairs Minister, the government accepts that the remittance sector has a valid role to play in providing a low-cost, fast

money transfer service to many locations around the world. However, it also believes that the remittance sector is vulnerable to money laundering and terrorist finance. Australian law enforcement authorities are also well aware that alternative remittance services – such as hawala – are being used to pay the operators of people smuggling ventures, O'Connor said.

Within the AML community there has been strong support for the government's plans to tighten up the remittance sector. The adage that the AML regime is only ever as strong as its weakest link holds true, and many AML practitioners have been concerned about apparent lack of compliance among some remittance dealers, especially small, community based remitters. The view that many have espoused at industry events is that it makes a mockery of the efforts of the compliant if some remitters are seen to be flying beneath the radar. ■

Warning bell chimes on foreign bribery offences

THE REVELATION in April that BHP Billiton is facing possible regulatory action in the US for alleged bribery of officials in Cambodia has underlined the importance of understanding the brutal sanctions regime that exists in that country. Australia's anti-bribery regime, it must be said, is relatively supine. Yet for any entity that has a US listing or extensive operations in the country, the regulatory consequences of breaching the anti-bribery laws are another matter entirely.

In the US it is not uncommon to see overseas companies with a secondary NYSE listing paying hundreds of millions of dollars in penalties for their transgressions in a country that is completely outside the US's jurisdiction. As banks with US-dollar clearing operations

are all too aware, the long arm of the US regulators is lengthy indeed when it comes to bribery, corruption and AML/CFT breaches.

In March, for instance, there was a multimillion-dollar settlement with the US Department of Justice that highlighted the reach of US regulators – and the quantum of penalties that apply. Daimler, the German car maker, agreed to pay US\$93.6 million and enter into a deferred prosecution agreement to settle claims that it breached the Foreign Corrupt Practices Act (FCPA). According to the DoJ and the Securities and Exchange Commission, Daimler paid tens of millions of dollars in bribes to officials around the world over a ten-year period between 1998 and January 2008. In addition to its payment to the DoJ, Daimler is expected to pay

US\$91.4 million to the SEC, bringing its total penalties to US\$185 million.

For companies in the mining and manufacturing sectors, in particular, these risks are difficult to negotiate. Bribery is an entrenched practice in many developing countries, where “tea money” is the simplest way to ensure the expeditious passage of a project and prevent obstacles from arising at the hands of local officials.

The risks of doing business in this manner in the modern era, however, are extreme. For financial services firms the reputational and legal exposure to FCPA cases is a matter of major significance. Any institution that has facilitated such payments could also find itself hauled before the US regulators – and even more so if the bribery has occurred in a country subject to US sanctions.

The FCPA essentially outlaws the corrupt payment – or offer of payment – of “anything of value” to a foreign official to obtain or retain business. This could include attempting to reduce taxes, avoid duties or obtain licences and permits for minerals exploration, for example. ■

MITIGATE YOUR *financial* CRIME RISKS

Financial crime is constantly evolving and so are the laws enacted in response. Sustainable corporations need to understand international financial crime trends and their legal obligations to ensure financial integrity.

Deakin University's off-campus **Graduate Certificate of Commercial Law (Financial Crime Control)** is designed to provide an in-depth understanding of international financial crime and its impact on the law and on regulatory and corporate practices.

Study areas include international financial crime, AML/CTF, corporate governance and enterprise risk management. The course is designed to benefit in particular, compliance and risk officers, regulators and law enforcement officials.

Graduates of this course may receive credit towards our Master of Commercial Law.

Applications are now open for study in Trimester 1 2010.
For further information please call 1800 624 316.

deakin.edu.au/law



DEAKIN
UNIVERSITY AUSTRALIA

MELBOURNE GEELONG WARRNAMBOOL

AUSTRAC clears up definition of 'agent' for industry

THE AUSTRALIAN AML regulator has confirmed that any agents of reporting entities will need to ensure that they have a watertight agency agreement in place to avoid becoming reporting entities themselves under the AML regime. The regulator set out its views on the definition of an "agent" and "agency" to address the industry's concerns about relying on third parties to provide AML services – for instance, in relation to customer identification processes and suspicious matter reporting.

Reporting entities have voiced concerns that there is no definition in the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 of what constitutes an agent. As such, there was some confusion as to whether AUSTRAC would rely on the common law principles of agency when implementing the AML/CTF regime. Early versions of the AML/CTF Bill in 2006 had various definitions of agents and these were discarded before the final bill entered parliament because of the confusion they created.

Under common law, an agent is a person who is "able, by virtue of the authority conferred upon him or her, to create or affect legal rights and duties as between another person, who is called a principal, and third parties." Under this model the principal is still responsible for the services provided by the agent, which confirms the commonly accepted principle in compliance that you can outsource processes to an agent but you cannot outsource the ultimate responsibility. It also means that if an agent forms a suspicion in relation to a transaction, for example, then the principal has an obligation to ensure that a report is lodged with AUSTRAC.

AUSTRAC says in its latest Public Legal Interpretation (PLI): "A defining feature of the agency power is that contracts entered into within the scope of the agent's authority become binding on the principal and the principal will be held liable for the acts of his or her agent where they are within the implied authority of an agent. The implied authority of an agent extends to all acts which are necessary or ordinarily incidental to the exercise of his or her express authority."

AUSTRAC stresses that, where a reporting entity provides a designated service through an agent, the "reporting entity retains

its status as reporting entity and is deemed to have provided the service." The agent will not become a reporting entity by virtue of the agency agreement. This definition of agency is distinct from an "independent contractor" who is engaged to provide a designated service to a reporting entity and would therefore be treated as a reporting entity in its own right under the AML/CTF Act.

An industry commentator said it was a welcome development that AUSTRAC had set out its views on agency in black and white. She said that the PLI was consistent with the position set out in the AML/CTF Act

ensure the agents are contractually bound to report any suspicious activities to them or to AUSTRAC. The reporting entity needs to ensure that it has an AML/CTF program in place that requires employees and agents to recognise and report suspicions. The industry commentator observed that it would be a confident principal that would allow its agents to make these reports directly to AUSTRAC. The more prudent path would be to handle the reporting obligation itself, receiving unusual activity alerts from the agent and conducting its own investigation, with the help of the agent.

it would be a confident principal that would allow its agents to make these reports directly to AUSTRAC

explanatory memorandum and agreed to by the Attorney-General's Department during the final stages of the consultation period, but that this was the first time it had been set out following the passing of the legislation.

The PLI was a salutary warning to businesses performing activities for others relevant to compliance with the AML/CTF Act. These businesses need to have a proper agency agreement in place to ensure that they will not inadvertently become reporting entities under the legislation.

A classic example provided was the small cash-in-transit businesses that subcontract to the bigger players like Brambles, Armaguard or Chubb. If those small businesses are not appointed as agents, then they are a reporting entity for any cash deliveries they do for the big players and they will have to duplicate everything that the principal does in terms of AML compliance. If they do have a formal agency agreement in place, however, then only one entity has to be responsible for establishing the procedures for compliance, even though the agent may then be required to follow those procedures to the standard required by the principal. So this PLI has a lot of relevance for both the agent and the principal.

AUSTRAC's interpretation means any reporting entities that use agents should

The regulator notes: "An agent may report [suspicious] matters to AUSTRAC on behalf of the principal under the principles of agency. The obligation to provide the report to AUSTRAC, and any penalty for breach of this obligation, would however remain with the principal under the AML/CTF Act."

The principles of agency will also apply to any reporting entities that outsource their customer identification procedures. Under Subsection 37(2) of the AML/CTF Act a reporting entity can authorise another person to act as its agent and carry out customer identification procedures. Based on the premise that a reporting entity cannot contract out of its statutory obligations, however, the principal would still have full responsibility for the customer ID processes.

AUSTRAC's publication of its latest PLI has also resolved some confusion within the industry as to why there was a "missing PLI" on its website. Prior to its release, the web site featured PLIs one to nine and then 11 to 12. That numerical mystery, we are happy to report, has now been solved.

In keeping with the regulator's new position on agency, it has updated its sixth PLI on suspicious matter reports. It will also republish its third PLI on designated remittance services in the near future. ■

Chinese banks struggle to manage AML risks

As Chinese regulators seek to stamp out money laundering in the country's growing financial services industry, Chinese financial institutions are facing challenges meeting new AML requirements laid down by the People's Bank of China.

WITH Chinese domestic financial institutions expanding their geographical presence and product portfolios, they have increasingly been facing greater money laundering and sanctions risks, according to a recent Deloitte & Touche survey. The study, on the key challenges faced by Chinese financial institutions in meeting Chinese AML requirements, began in December 2009 and was completed in January 2010.

In the survey, Chinese financial institutions identified several challenges with meeting the PBOC's new AML requirements. The lack of a clear interpretation of AML requirements by the PBOC's various branches at the provincial, county and centre level, as well as its operation management offices across the country, had been one of the main problems, according to the survey respondents.

"The PBOC should have detailed guidelines on the AML requirements so that its officers can give consistent answers to the questions raised by industry participants, rather than letting the officers figure out the various AML requirements from their

own interpretations, and then distribute the answers to the industry participants," said Rachel Layburn, associate director at Deloitte in Beijing.

Chinese institutions should also have in place a proper communications channel allowing AML officers at headquarters to communicate with the PBOC, she suggested.

The central bank's prescribed AML requirements had also forced banks to reassess their compliance duties, while securities, asset management and insurance companies were just beginning to be confronted with the lack of skilled and experienced AML staff, according to the survey.

One of the important changes that financial institutions were expected to undertake would be on the operational and technology front. Ten percent of the executives interviewed for the survey said their institutions did not use any software for sanctions screening purposes. Fifty percent of the respondents said their institutions used internally-developed software for sanctions screening, 8 percent depended on external vendor applications, and 31 percent used a combination of vendor applications and software developed internally.



To most Chinese institutions, words such as "AML" and "compliance" were new terms, and this sometimes meant that commercial interests took precedence over complying with regulations, the survey results showed. The pressure to bring in more revenue had made those on the frontline of business in firms reluctant to contribute towards building a more robust compliance framework, according to 62 percent of the compliance officers interviewed for the survey.

In a similar survey, conducted by Deloitte in 2008 with 11 global financial institutions, respondents also indicated some challenges in meeting China's AML requirements, particularly with respect to customer information monitoring – especially for large corporate customers – and tracking and updating KYC information. As the sanctions regime continues to develop in China, respondents said they expected to see more requirements in terms of due diligence, screening and filtering of customers' names, as well as in the processes for resolving domestic hits and monitoring and screening arrangements. ■

Singapore increases focus on AML compliance



ANTI-MONEY LAUNDERING and the financing of terrorism has risen up the Singaporean government's agenda as it seeks to establish the city-state as Asia's leading financial centre. To help firms in their fight against money laundering, Singapore's Commercial Affairs Department recently published the third edition of its AML/CTF Handbook.

Ong Hian Sun, director of the CAD and co-chairman of the Asia-Pacific Group on

Money Laundering from 2008 to 2010, said the CAD had continued to monitor international and regional best practice, making sure that internationally accepted AML standards were enforced in Singapore.

To strengthen Singapore's AML/CFT regime, it has reviewed the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (the CDSA), particularly the list of predicate offences in the Second Schedule of the CDSA, the CAD said. Its aim is to extend the crime of money laundering to cover a wider range of predicate offences. Additional predicate offences were added to the Second Schedule of the CDSA in January this year, bringing the total number of such offences to 368. ■

Letter to the Editor

I applaud the article published in the February 2010 edition of *AML Magazine*: “Would the real beneficial owners please stand up and identify themselves”. This article, along with the article published in the same edition by Martin Woods: “The exposed nominee”, highlights the confusion and lack of clarity provided by AUSTRAC and the AML/CTF Act and Rules with regard to what level of beneficial ownership is to be identified by banks and financial institutions. The articles also highlight the need for AUSTRAC and the corporate regulator, ASIC, to be working closer together.

While both articles note the fact that there is inconsistency and confusion across the industry on how banks meet this requirement, companies who have relationships with more than one bank or financial institution have also questioned why there is a difference in the standard of identification and verification.

Regardless of how far we dig into the company’s structure to identify the beneficial owner, the real issue is: how reliable is the information obtained and used to verify the company and its ownership? This became apparent with the uncovering by the police and corporate regulators of an Australian crime syndicate as reported by Michael West for *The Age* on April 20, 2010 (“Major banks linked to crime ring’s money laundering”). The article reports how the crime syndicate was believed to have garnered trading tips from several sources, and traded in a range of shares on the stock exchange.

Where this article draws relevance to the discussion on beneficial ownership is that the share trading was conducted through what have been reported as false company names, along with false names of individuals behind them. So the questions that begs to be asked is: what checks are done by ASIC when a company applies to register its name? Would it not make sense that ASIC – as Australia’s corporate, markets and financial services regulator, whose role it is to ensure that company directors and officers carry out their duties honestly, diligently and in the best interests of their company – should be carrying out some form of identification and verification to ensure that the company and its directors are who they say they are.

As noted earlier, banks can only go by the information that is available to them and verified by the corporate regulator. If this information is false, then what chance have the banks got in knowing who they are really dealing with, when the regulator has allowed a company and its directors to be registered without themselves having done any form of due diligence.



At the end of the day, money launderers will continue to pursue their craft while Australia has a corporate watchdog that does not perform any form of due diligence on the legitimacies of either companies or their directors.

Donna Jones
May 2010

How to Tell Your Best Customer from Your Worst Nightmare



Win the battle against fraud, money laundering
and terrorist financing with Dow Jones

Dow Jones **Watchlist**

Doing business with just one wrong customer can result in steep financial penalties for your business or, worse, cause irreparable damage to your reputation.

Dow Jones Watchlist helps you easily and accurately identify high risk clients with detailed, up to date profiles on more than 500,000 entities. Coverage includes national and international

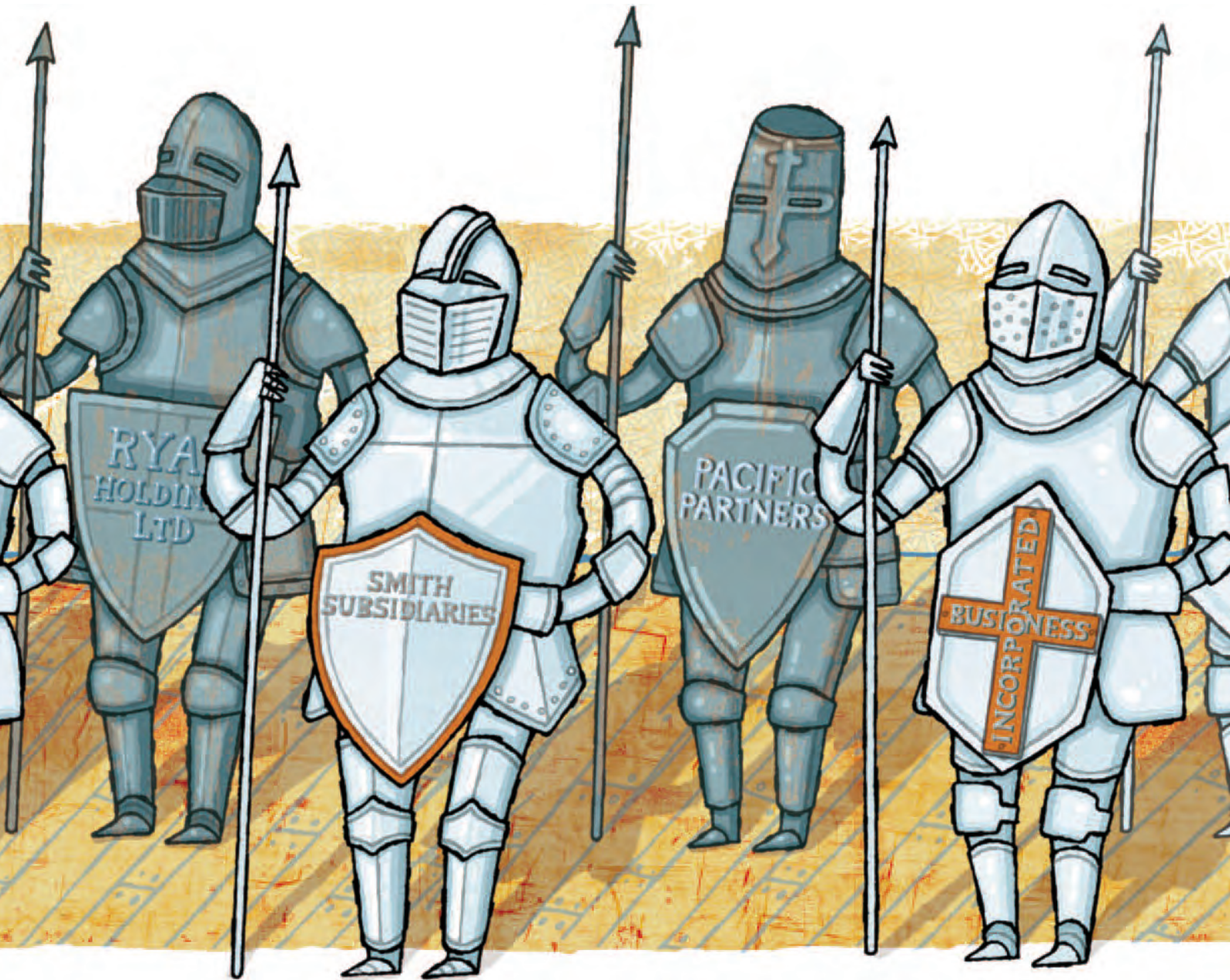
government sanction lists; persons linked to high profile crime; and senior foreign political figures, their relatives, and close associates.

To learn more about Dow Jones Watchlist, contact Richard Butler at richard.butler@dowjones.com or at +61 (0)2 82724600.

DOWJONES

Beneficial Ownership

Part II – Who the bloody hell are you?



Indeed, there are two questions – who are you and where are you from?

Just like attracting the elusive overseas tourist to a destination (Australia) that thinks it has everything, reporting entities struggle to find the essential link (the beneficial owner or “BO”) in customer due diligence on proprietary companies.

The reasons can be any of the following:

- clients themselves do not understand the question when asked;
- the BOs are intentionally making themselves hard to be found;
- company registry information is unavailable or unreliable; or
- the cost of completing the necessary searches is regarded as disproportionate to the revenue stream from the client.

In this article, the term BO refers to individuals who are the beneficial owners of the issued capital of proprietary companies. This ownership may be held directly as shareholders or indirectly as shareholders of other companies which are the direct shareholders. There may be a number of tiers of shareholdings involved. By definition, a BO is always an individual. BOs are not necessarily the shareholders of a proprietary company.

Why is the identity of the beneficial owner of critical importance to identification and mitigation of ML/TF risk?

The identity of a BO, and where they are located or domiciled, are pivotal to the assessment and mitigation of money laundering and terrorism financing risk (ML/TF risk). There is no argument that the overwhelming majority of corporate vehicles operate for genuine and legitimate purposes. This is a version of the well-worn statement that most people are not money launderers. However, the ugly reality is that proprietary companies are very useful in the process of laundering money and yes, the 'bad guys' do know this (and if they don't, they're sure to know a company formation agent, adviser or lawyer who does).

Proprietary companies provide useful blinds behind which money launderers and their associates can easily disguise themselves, using complex ownership chains to make identification difficult. Money launderers can pass ownership of proceeds of crime to a proprietary company which they retain control of, thus distancing themselves from the money being laundered without losing ultimate control. This reduces their need to trust others to handle their criminal assets on their behalf, which in turn reduces the need to have private enforcement methods at their disposal to protect these assets. It is difficult to seek the assistance of law enforcement agencies and legal systems to recover assets from associates that have become uncooperative if those assets have dubious parentage.

Some European FIU experience has been that ML events have invariably involved a proprietary company where the BO is not known, or a trust of some sort.

This article contends that ML/TF risks are unidentified and unmitigated where the beneficial owner has not been identified. As is well known, identification and mitigation of the

ML/TF risk that a reporting entity reasonably faces is a required primary purpose of an AML/CTF program for an Australian reporting entity. Beneficiaries of trusts throw up similar issues, made more complex through the absence of registration systems for trusts and open classes for beneficiaries.

The Australian Rules go too far in one sense, in that they do not permit a reporting entity to take comfort in a shareholding of a reporting entity which is, for example, composed of 33 percent by a public listed company on the ASX; 33 percent owned by a regulated financial institution, and 33 percent owned by the European Central Bank. A literalist tick-the-box approach would dictate that searches stop when no individual can be found to hold shares in any of the ASX, the regulated financial institution or the European Central Bank. And that is a step too far in the wrong direction. The FATF Recommendation 5 does contemplate certain categories where a simplified approach is permitted.

The enquiry process is not easy but necessary

In 2009, the Global Witness *Undue Diligence* report launched a penetrating dissection of "How Banks do business with corrupt regimes"¹. The report shows a catalogue of risk management failures within some of the biggest names in financial services; it also demonstrates the damage that *one* single client

provide nominee services in Anguilla. The company is assumed to be a shell company because of the place of its incorporation and the identity of the shareholders. Anguilla is not a major place of economic activity and in all likelihood there were prohibitions on the company carrying on actual business in Anguilla.

The Guideline on the Prevention of Money Laundering, issued by the Hong Kong Monetary Authority (HKMA) clearly states the following:

*"An Authorised Institution should exercise special care in initiating business transactions with companies that have nominee shareholders. Satisfactory evidence of the identity of beneficial owners of such companies should be obtained"*².

Anguilla is generally seen as a secrecy jurisdiction where details of shareholders, directors and beneficial owners are not available from the Government agency responsible for the incorporation of companies. So a relationship with a shell company from Anguilla, complete with nominee shareholders, would normally be placed in the risky basket from a know your client (KYC) perspective.

To add to the risks involved with opening an account for a shell company incorporated in Anguilla with nominee shareholders, the

ML/TF risks are unidentified and unmitigated where the beneficial owner has not been identified

relationship can inflict on a financial institution's reputation. But most of all the report shows how customer due diligence, if completed properly, would have in *all* cases identified high-risk beneficial owners, or revealed a level of opacity such that the accounts should not have been opened because the bank involved had no idea who their customer really was and where they came from.

One of the case studies described in the *Undue Diligence* report relates to Bank of East Asia's relationship with a little shell company named Long Beach. Long Beach was incorporated in Anguilla; its *shareholders* (emphasis added) were companies which

bank did ascertain that the main business activities of Long Beach were "trading crude oil, gas, and products (mogas, jet, gasoil, kerosene) in Congo".

The intermediary introducing Long Beach to the Bank was a Hong Kong company formation service and its subsidiaries were the nominee shareholders.

The operation of this account (receipt of proceeds that appear to be the sale of Congo oil and the payment of the credit card bills of the son of the President of the Republic of Congo) are secondary to the purpose of this article.

¹ http://www.globalwitness.org/media_library_detail.php/735/en/undue_diligence_how_banks_do_business_with_corrupt

² http://www.info.gov.hk/hkma/eng/guide/circu_date/attach/20071113e2a2.pdf

Conduct of proper KYC before acceptance of this client should have addressed the red flags the customer presented that have been described above:

- **Secrecy jurisdiction** – the appropriate response to the high risk presented by an Anguilla incorporated company would be to use independent means to secure satisfactory evidence of the identity of the beneficial owners of Long Beach. Failure to secure satisfactory evidence of identity should have resulted in refusal of the account. Securing satisfactory evidence would have produced a further red flag because the beneficial owner was the son of the President of the Republic Congo (son of a politically exposed person of a country ranked 113 out of 133 countries for corruption in the year this account was opened).
- **Secrecy jurisdiction** – information would be sought about the purpose of the structure and the choice of Anguilla and the reason for nominee shareholders. Failure to secure satisfactory information on these matters should have resulted in refusal of the account. Securing satisfactory evidence would have produced the PEP red flag referred to above.
- **Source of funds** – the appropriate response to the source of funds disclosed would be to deploy the bank's country ML/TF risk model which should have provided background information on the Republic of Congo. These facts would have included learning that all Congo oil is owned by the Government so any person claiming to have funds from trading crude oil, gas, and products (mogas, jet, gasoil, kerosene) in Congo must therefore be connected with the Government. This information, coupled with the PEP information about the BO, would raise further red flags about potential corrupt flow of funds.

It is not known whether the Bank did conduct all of this due diligence. If it did, then it proceeded to conduct a high risk account to perform high risk transactions which on publicly available information, appear to be excessively risky. If it did not conduct the due diligence then the transactions conducted on the account succeeded because of the lack of response to unambiguous red flags presented in support of account opening.

In the case of Long Beach, ascertaining the BO revealed other material red flags. Now, before we all pat ourselves on the back that we would *obviously* have found out who the BO is of a company from *Anguilla*, and seen every red flag, let's move onto the next case study...

It turns out money laundering does happen in the US, after all

Despite the trenchant criticism from the United States towards little Caribbean islands, for their unacceptably low levels of transparency and activity as 'tax havens and secrecy jurisdictions', one of the best places to launder money turns out to be, America.

The US Senate Permanent Subcommittee on Investigations released a revelatory report³ (revelatory to the US financial sector and its regulators at least) which examines how corrupt government officials have been "*circumventing or undermining PEP controls*" within US financial institutions.

One of the report case studies focuses on the son of the President of Equatorial Guinea, Teodoro Nguema Obiang Mangue (TNO). There are now multiple reports (and indeed investigations) into how TNO has managed to circumvent AML controls to further his extraordinarily lavish lifestyle. Just to give you an idea, TNO owns a US\$35 million mansion in Malibu; a US\$33 million private plane; a Bugatti Veyron and a Ferrari 550 Marinello, all on his official salary of a few

TNO laundered USD\$110 million within four years. He did this using one key resource: lawyers. Two lawyers *actively helped* TNO to get around the controls within US banks, sadly, this wasn't hard to do – all it takes is a couple of shell companies in California. TNO was actually the signatory for one of the accounts of one of these shell companies which suggests that there was no process in place to identify account signatories and screen such persons against PEP lists. The existence of TNO as a signatory creates a red flag which is directly connected to opaque ownership and the true identity of the UBO.

The Levin report rightly observes, that "*since 2001, U.S. financial institutions have been required to set up AML programs ... to know their customers*".

The problem is, US Banks appear to have fallen into a risk-based trap, where beneficial ownership is not part of *standard* customer due diligence. In relation to the companies formed by TNO's lawyers, US banks apparently thought it's possible to know their client, a shell company, without knowing who sat behind it. Which does beg the question – what else is there to know about a shell company that's meaningful?

The KYC analysis is no different to the first case.

Until the BO is known the totality of ML/TF risk presented by an unregulated proprietary company cannot be understood. This is not a risk-based proposition.

TNO owns a US\$35 million mansion in Malibu; a US\$33 million private plane; a Bugatti Veyron and a Ferrari 550 Marinello, all on his official salary of a few thousand dollars a month

thousand dollars a month – amazing. In the mean time, most people in Equatorial Guinea live on a meagre US\$1 a day.

But how can these government officials outwit the Compliance frameworks of some of the largest Banks in the world? The answer is simple – the failure by banks to identify BO is exploited to the hilt by professional advisers.

Discovering the presence of nominee shareholders (perhaps these may have been the lawyers) is an additional red flag. An account signatory who is a PEP is a further red flag. Combining knowledge of the identity of the BO, knowledge of the signatory with the stated source of funds for the account may

³ "Keeping Foreign Corruption out of the United States: Four Case Histories" 3rd February, 2010.

produce even more red flags. Comparing this information with incoming funds and transactions should have produced more red flags.

US banks had considered that BO inquiries should not be mandatory for 'low risk' customers, and that other controls such as transaction monitoring were more proportionate ways to flag otherwise low risk customers for additional scrutiny. There are two problems with such an approach:

- These additional controls weren't working effectively in most of these case studies; and
- The best prevention is to ensure that such companies do not gain access to the financial sector in the first instance.

Here are a few things we can take away from this latest report from the US Senate:

- An effective AML/CTF regime cannot be operated under the assumption that the misuse of corporate vehicles only happens outside the US;
- Such an assumption leaves glaring gaps within the U.S. financial sector that are being exploited;
- No one seems to be planning on regulating US Lawyers (or accountants, or trust company service providers, or financial planners et cetera) despite the demining information in the Levin Report.

The elephant in the room

The case studies highlighted by the Undue Diligence report and the latest Levin report are damning reminders of how the proceeds of corruption are still making their way (apparently without much difficulty) into the global financial sector through opaque entities.

Read for "proceeds of corruption" in the above statement "proceeds of crime" and also "funds for the financing of terrorism". If it works this easily at this gross level of Congo and TBO with red flags of the dimensions noted, then the more modest money launderer or terrorism financier is on Easy Street. In the two cases cited, there was no major piece of additional work that the bank needed to conduct which would take it out of its way or cost significant amounts of money. The banks did not need to leave home to understand the ML/TF risks involved.



the proceeds of corruption are still making their way (apparently without much difficulty) into the global financial sector through opaque entities

The social costs of corruption and bribery are immense, the World Bank estimates approximately US\$1 trillion of bribes are exchanged annually. However, there is another pool of illicit assets, which equally impacts the citizens of developing nations, that is prevalent across the financial services sector – that is, the proceeds of tax evasion.

Due to the nature of the subject, it is difficult to obtain definitive figures of how much money the proceeds of tax evasion amounts to, though it certainly doesn't seem to be peanuts:

"Current total deposits by non-residents in offshore and secrecy jurisdictions are just under US\$10 trillion"

There is an ever increasing focus on tax evasion following the G20 summit in 2009 and the investigations into the activities of UBS and LGT Group.⁵ The two major themes of these investigations are:

- The setting up of offshore accounts; and
- Hiding the beneficial ownership of offshore funds through 'asset protection' companies in offshore tax havens.

Within Australia, the reporting and analysis of international funds transfers has been a dominant driver of the AML/CTF regime for many years. The problem is that 'bad guys' know this, including their lawyers, consequently, the easiest way to circumvent this reporting is to make use of corporate vehicles to transfer funds in and out of Australia anonymously. The effectiveness of IFTI reporting is undermined if neither the public nor private sector finds out who the BO's are of corporate vehicles, particularly asset protection vehicles.

AUSTRAC recognises that its role as Australia's Financial Intelligence Unit is impacted by the quality and extent of information collected by the private sector:

"The more high quality data AUSTRAC receives, the better positioned we are to assist our partner agencies with valuable financial intelligence to combat money laundering, crime and tax evasion".

Tax evasion has damaging social and economic implications, which are equally as harmful as the corruption of government officials. The recent case studies of UBS and LGT, as well as Project Wickenby are placing tax evasion as a priority and clearly highlight the role of beneficial ownership in identifying potential tax evasion. In short, beneficial ownership is a jackpot for tax regulators and law enforcement bodies.

The way forward?

The case studies discussed above (rightly) lament the failure of banks to know who their customers are. The failure flows from failure to identify BOs and follow the facts from there.

We opened this article by contending that ML/TF risks of corporate vehicles are unidentified and unmitigated where the beneficial owner has not been identified. The above cases are evidence for this view. A reporting entity that does not identify the BO of a proprietary company does not know who they are dealing with.

Global Witness and Senator Levin both ask 'Why is this still happening?' This is a good question, but it needs to be directed at a broader range of players with responsibilities at key control points in our economies than just the banks. ■

⁴ http://www.taxjustice.net/cms/front_content.php?idcat=103. ⁵ LGT Group is the private banking, wealth management and asset management group of the princely House of Liechtenstein. LGT, originally known as **The Liechtenstein Global Trust**, is the largest family-owned private wealth and asset manager in Europe, wholly-owned by the Prince of Liechtenstein Foundation.



Beneficial Ownership

Part III – International approaches

In the previous edition of AML magazine we discussed difficulties in determining the ultimate beneficial owner (UBO) of proprietary companies in Australia. In this month's article, Dr McDermott looks at two key jurisdictions which influence future trends in AML; namely, the US and UK. You will see from the analysis below that problems faced by Australian institutions and the lack of transparency of UBOs are yet to be tackled in a successful way by these jurisdictions.

United States – over-reliance on US company registration

In general, American AML laws don't require a financial institution to look through a corporate customer and identify its beneficial owners.

The Bank Secrecy Act 1970 and its implementing regulation, 31 CFR 103, require financial institutions to identify and verify those companies not deemed to be high risk. This involves establishing a company's principal place of business and collecting a govern-

ment-issued identifier (such as an ABN for an Australian company), and verifying by obtaining documents such as certified articles of incorporation or a government issued business license [31 CFR 103.121(b)(4)(ii)(A)]. There is no specific reference in this provision to the concept of beneficial ownership.

However, the Department of Treasury Final Rule (68 Fed. Reg. 25090) implementing section 326 of the USA Patriot Act 2001 provides that, based on a bank's risk assessment, a bank may need to take additional steps to verify the identity of the customer by seeking

information about individuals with ownership or control over the account. The Final Rule also states a bank may need to look through an account as part of its ongoing customer due diligence procedures under its Bank Secrecy Act compliance program.

While US laws promote a risk-based approach to identifying beneficial owners at the point of establishing a relationship, in practice, US banks tend not to identify beneficial owners of domestic corporate customers at this point. This is due to the weighting banks

apply to country risk, where they tend to apply a blanket 'low-risk' status for US companies and a higher risk classification for all foreign companies (with countries declared by the Secretary of the Treasury to be of primary money laundering concern given the highest risk rating). Banks generally only identify beneficial owners for domestic companies as part of their ongoing customer due diligence.

The 2006 FATF mutual evaluation noted this as a deficiency against FATF recommendation 5 and recommended a primary obligation to identify beneficial owners be introduced.

The approach taken by US banks results in a nonsensical situation where enhanced customer due diligence is not undertaken on a corporate customer simply because the company is registered in the US. For example, beneficial owners are usually not identified for a company registered in Delaware (a State known for its lack of transparency in company registration), but are sought for recognised legitimate foreign businesses (such as Barclays Bank or Westpac).

While material changes to legislation have not occurred since the mutual evaluation, there are moves afoot among US lawmakers and regulators to focus more on beneficial ownership.

Movement by US lawmakers

Legislation is currently before Congress to strengthen disclosure of beneficial owners of companies.

Currently, new business entities including corporations, limited liability companies, limited liability partnerships, non-profit organisations and other entities file formation documents with a State. States compete for business creation through innovative business entity laws. While many State laws require business entities to nominate a contact officer for the serving of notices, State laws often do not require disclosure of all current owners of the entity.

The Incorporation Transparency and Law Enforcement Assistance Bill was introduced by Senator Carl Levin in March 2009 and would require beneficial owners to identify themselves, and States to collect and maintain beneficial ownership information on corporations and limited liability companies.

In the March 2010 issue of *Anti-Money Laundering Magazine*, we published the article 'Beneficial ownership Part 1: Would the real beneficial owners please stand up and identify themselves'. In this article, we considered whether it was more reasonable to put the onus of identification on beneficial owners at the point of company registration, rather than on banks at the point of establishing a relationship. The Levin Bill proposes this type of self identification by beneficial

claiming that legitimate businesses have important interests in maintaining the privacy of the ownership structures they use to invest in new projects. They claim that public disclosure of beneficial owners not only impacts purchase prices for target companies, but also purchase prices for target assets, particularly real estate.

The Bill is currently under review by the Committee on Homeland Security.



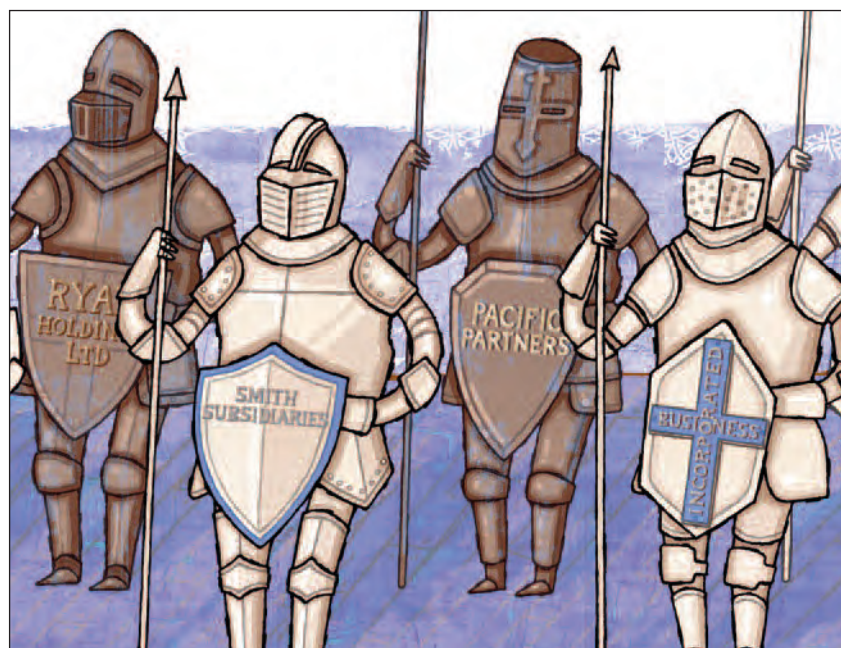
The approach taken by US banks results in a nonsensical situation where enhanced customer due diligence is not undertaken on a corporate customer simply because the company is registered in the US

owners, with corporate regulators collecting and maintaining the information. While the Bill does not propose removing the requirement for banks to also identify beneficial owners, in the event the Bill passed, some might ask whether this duplication of identification is necessary.

The strongest critique of the Bill is that it relies on individuals voluntarily reporting their beneficial ownership information, so the burden will fall most strongly on the companies least likely to break the law. Opposition has also come from business lobby groups,

Movement by US regulators

An interagency "Guidance on Obtaining and Retaining Beneficial Ownership Information" was issued on March 5, 2010, by FinCEN (jointly with the SEC and each bank regulatory agency). While the Guidance purports only to "clarify and consolidate" existing regulatory expectations regarding the identification of beneficial owners of accounts, it provides a clear indication that this has now become a priority for the regulators.



The Guidance expressly singles out accounts maintained for various types of entities, such as unincorporated associations, private investment companies (PICs), trusts and foundations. It specifically points out the heightened risk posed by these accounts because of the ease with which their unidentified beneficial owners can engage in illicit activity anonymously through them.

The Guidance specifically highlights companies that are not publicly traded in the US, and risks associated with foreign politically exposed persons (PEPs). As such, the Guidance breaks no new ground in resolving banks' misplaced over-reliance on US companies as being of lower risk. However, the primary significance is that beneficial ownership is the new "hot button" for US regulators.

United Kingdom – gaps pre 2007

Prior to the UK's implementation of the 3rd EU Money Laundering Directive in December 2007, financial institutions in the UK were not legally required to identify beneficial owners of corporate customers.

Despite the lack of legal requirements, most UK banks were identifying beneficial owners in line with JMLSG Guidance which stated that "the firm's objective must be to know who has control over the funds which form or otherwise relate to the relationship, and/or form the controlling mind and/or

management of any legal entity involved in the funds". Identification standards were set out in the Guidance and were applied in a fairly standard way across industry. However, the Guidance on verification was vague ("the firm may feel it appropriate to verify the identity of appropriate beneficial owners holding 25% or more") and applied in a haphazard way across financial institutions.

Gaps in verification, and the FATF's refusal to accept JMLSG Guidance as 'other enforceable means', led to a rating of 'partially compliant' against recommendation 5 in the FATF's 2007 mutual evaluation.

UK implementation of Third EU ML Directive

The Money Laundering Regulations 2007 address these concerns by requiring financial institutions to identify and verify beneficial owners, as defined in box below.

The requirement to identify and verify beneficial owners applies before or during the

the Guidance on verification was vague and applied in a haphazard way across financial institutions

course of establishing a business relationship and when conducting transactions for occasional customers. Regulation 7 requires a bank to identifying and verifying beneficial owners when it:

- establishes a business relation;
- carries out an occasional transaction (which is defined as a transaction outside of a business relationship amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked);
- suspects money laundering or terrorist financing;
- doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

In practice, the company's identity comprises its constitution, its business and its legal ownership structure. The key

UK Money Laundering Regulations 2007, Regulation 6, definition of beneficial owner

For a body corporate, any individual who owns or controls (directly or indirectly) more than 25% of the shares or voting rights in the body, or otherwise exercises control over the management of the body.

For a partnership, any individual who is ultimately entitled to or controls (whether directly or indirectly) more than 25% share of the capital or profits or more than 5% of the voting rights, or otherwise exercises control over the management of the partnership.

For a trust, any individual who is entitled to a specific interest in at least 25% of the capital of the trust property, or any individual who has control over the trust. (Specific interest is further defined to include a vested interest which is in possession or in remainder or reversion; control means a power under the trust instrument to dispose of, advance, lend, invest, pay or apply trust property; vary the trust, add or remove a person as a beneficiary; appoint or remove trustees; direct, or withhold consent to or veto the exercise of power).

In any cases outside of a body corporate, partnership or trust, beneficial ownership means the individual who ultimately owns or controls the customer or on whose behalf a transaction is being conducted.



The third round of FATF mutual evaluations identified systemic non-compliance by jurisdictions with recommendation 5



identification particulars are the company's name and business address, although the registration number and names of directors may also be relevant.

Customer due diligence includes understanding the purpose and intended nature of the business relationship as well as the ownership and control structure of the company.

Public companies listed in the UK

Where a company is listed and its securities are admitted to trading on a regulated market, or where it is a majority-owned and consolidated subsidiary of such a company, simplified due diligence applies.

For a listed company, this may simply be confirmation of the company's listing on the regulated market. Such evidence may be a copy of the dated page of the website of the relevant stock exchange showing the listing, a photocopy of the listing in a reputable daily newspaper, or information from a reputable electronic verification service provider or online registry. For a subsidiary of a listed company, evidence of the parent/subsidiary relationship is required.

Public overseas companies

If a regulated market is located within the European Economic Area, banks may adopt a risk based approach to identifying and verifying beneficial owners. HM Treasury have released a list of countries that the UK government accepts have anti-money laundering requirements equivalent to the money laundering directive and can be used as a basis for a bank's country risk assessment.

While this list is seen by some as a useful tool for banks in determining country risk, it

has been criticised as the product of a political process rather than a clinical assessment of the equivalence of ML regulation and enforcement within a jurisdiction. The inclusion of countries like Switzerland and Russia on this list do little to instil confidence that the list truly indicates countries that meet the 'equivalence test'. One should be extremely wary of banks that blindly rely on this list as their basis for assessing country risk.

Systemic global non-compliance

The third round of FATF mutual evaluations identified systemic non-compliance by jurisdictions with recommendation 5, primarily due to deficiencies in identifying and verifying beneficial owners of non-natural persons.

One response has been law reform, with new laws introduced in Australia, the UK, and draft laws proposed in the US.

Some are calling for corporate regulators such as ASIC to take responsibility for identifying beneficial owners



Another response has been debate about whether recommendation 5 is achievable. Not a single country has been rated compliant with recommendation 5. Could this be because it is simply not realistic to expect a bank to look through its corporate customers to the UBOs?

A new way?

Some are calling for corporate regulators such as ASIC to take responsibility for identifying beneficial owners of the companies it registers. With the imminent incorporation of market regulatory functions into ASIC, perhaps ASIC is best placed to work with share registries to identify the shareholders of listed companies at any point in time.

On the surface, this appears to be a sensible solution.

However, this shift in responsibility would strip a rich source of KYC information from a bank's ongoing customer due diligence program. FIUs tell us that much of the most useful financial intelligence is gleaned from high quality suspicious activity reports, where those reports are the result of effective OCDD involving transaction monitoring against expected customer behaviour. A dual model would see ASIC possessing information about beneficial owners and banks possessing information about transactions.

For ASIC to make this information public could compromise a company's ability to invest in new projects without distorting market pricing, as raised by opponents of the Levin Bill.

Multi-layered corporate structures present real problems for financial institutions, regulators and law enforcement – that's why they are used so pervasively by serious money launderers. While transaction monitoring software has improved our ability to spot placement and structuring, pattern recognition depends on identifying the UBO. Revealing the identity of criminals is the ultimate goal in AML. Without being able to determine the UBO of propriety companies we are unlikely to be able to achieve this aim. ■

By Dr Hugh McDermott, Barrister-at-Law, CAMS and Director of Invictus, a consultancy which advises clients on financial regulation, white-collar crime and AML. He was formerly the Senior Manager, Major Fraud and International at ASIC, Sydney, and a Litigation Attorney in the Cayman Islands.

Not happy, Jan!

The **FATF's** view of Australia's AML/CTF regime



It must be with considerable disquiet that many anti-money laundering/counter-terrorism financing (AML/CTF) compliance officers and their reporting entities learn for the first time that the Financial Action Task Force (FATF) is unhappy with the AML/CTF regime that Australia implemented in 2006 after three long years of consultation. Australia has been on annual report to the FATF since its mutual evaluation in October 2005, reporting in October of 2007, 2008 and 2009.

The **FATF** has recently refused to remove Australia from the annual follow-up process and allow it to report on a biennial basis. The reason for the refusal is the FATF's concern with the nature and extent of Australia's implementation of the risk-based approach in relation to customer due-diligence (CDD) requirements.

FATF considers that what Australia has done for CDD (the FATF Recommendation 5) is too risk-based and insufficiently prescriptive, and so has rated Australia as only partially compliant with Recommendation 5. When we look at the other members of the FATF to find out their level of compliance, we find that in the last round of mutual evaluation, 90 percent of the FATF membership are either non-compliant or partially compliant with Recommendation 5. Only Belgium, Portugal and Singapore were rated in the last round of mutual evaluations as largely compliant with

recommendation 5. Twenty-one members were rated as partially compliant and five as non-compliant during that round. NO FATF member was rated as compliant.

The implications of the FATF objections are serious because Australia may introduce changes to its regime in order to overcome them. These changes would lead to changes in processes and procedures – in short, more money will need to be spent on work completed in anticipation of a stable regime. It is not so much that the FATF has moved the target, rather that the FATF believes Australia has missed the target.

AUSTRAC has released a discussion paper to industry groups that raises a number of issues on which it is seeking input in order to respond to the FATF. Not since the passage of the AML/CTF Act has there been a more important time for your industry association to

be engaging directly with AUSTRAC on these issues and acting as a channel for your views.

And all of this is taking place at the same time that the FATF is reviewing the FATF 40 + 9 recommendations, and its own mandate is under review. Choppy waters indeed!

What is AUSTRAC interested in hearing about regarding customer due diligence?

The FATF objects to the following areas in Australia's CDD requirements:

- The definition of "beneficial ownership" is regarded as inadequate because it does not cover the concept of control. The Glossary to the FATF Methodology defines beneficial owner as "the natural

person(s) who ultimately owns or controls a customer and/or the persons who exercise ultimate effective control over a legal person or arrangement". In contrast, the Australian definition is that beneficial owner, in respect of a company, means any individual who owns through one or more shareholdings more than 25 percent of the issued capital in the company.¹ AUSTRAC points to an additional reference to beneficial ownership appears in the definition of know your customer (KYC) information in Chapter 1 of the AML/CTF Rules, but this definition applies only to individuals and not to legal persons. This is just one inconsistency within the definition of KYC information which has always been somewhat of a puzzle.

- Exceeding the FATF's view on risk-based approach for certain CDD measures, which appears to be an objection to the risk-based approach to verification of the identity of beneficial ownership. The FATF expects the standard to be to take reasonable measures to verify the identity of the beneficial owner. Australia permits the use of appropriate risk-based systems and control to verify the identity of beneficial owners, which is not the same as taking reasonable steps.
- Lack of a legal obligation to apply specific enhanced customer due diligence (ECDD) measures in high-risk situations.
- The range of ECDD measures in the AML/CTF Rules is too limited.
- AUSTRAC's examples of high ML/TF risk in the Regulatory Guide do not cover the high-risk categories in the FATF Methodology or the Basel Committee for Banking Supervision's CDD paper.

Enhanced customer due diligence

In response to the issues on enhanced customer due diligence (ECDD), AUSTRAC has released draft amendments to Chapter 15 for discussion. The main proposed changes are:

- Recanting on a hard-fought subject during the AML/CTF Rules consultation phase by changing the operation of the ECDD rule from one where a reporting entity needed to "give consideration" as to whether any of the ECDD measures apply to a requirement where action *must* be taken. Under these changes, a reporting entity must now take at least one or more of the actions in 15.10.

- Expand on the nature of further information and analysis that should be undertaken, depending on which step the reporting entity has elected applies. These include source of wealth and funds, as well as the ultimate beneficial ownership of personal assets and shares held by the customer (if a non-individual).
- Introducing the option of a new control – senior management approval – for establishing or continuing certain relationships, processing certain transactions, providing a designated service to a customer and any other reasonable action responsive to the identified ML/TF risk or suspicion.

Close examination of these changes reveals that the changes will significantly upgrade what a reporting entity will need to

An objectionable change is the reference to "the ultimate beneficial ownership of personal assets and shares held by the customer (if a non-individual)". Ultimate beneficial ownership seems to imply that there is a state of beneficial ownership that is not ultimate, a kind of halfway house of beneficial ownership. Use of the word "ultimate" adds to the confusion around identifying the beneficial ownership of proprietary companies. A beneficial owner is either a beneficial owner or not.

This proposed change to Rule 15.10 adds to the problems around the operation of Rule 4.3.10. There should be no need to add these words into Rule 15.10 if the requirements on proprietary companies and on trusts were followed by Australian reporting entities.



do at the point of establishing a relationship with a customer in a high-risk category. Reporting entities will be forced into capturing further information about source of wealth and funds and ultimate beneficial ownership of personal assets and shares if the customer is not an individual, because the other steps under Rule 15.10 do not apply at the start of a relationship. Reporting entities are unlikely to expose their senior management to approval of high-risk customers without placing sufficient information before them on these matters.

These changes encroach on the operation of the rules for companies and trusts, which will lead reporting entities to wonder what less they can do under the requirements in Chapter 4 – or indeed to contemplate what Chapter 4 did require them to do in the area of beneficial ownership and beneficiaries of trusts.

The proposed changes to Rule 15.10 have been promulgated for discussion in somewhat of a vacuum. The beneficial

¹ See also the article by Dr. Hugh McDermott in this issue which sets out the definition used in the United Kingdom.

ownership challenge in Chapter 4 needs to be addressed in tandem, so that Rule 15.10 does not start to encroach on broader minimum requirements. Piecemeal amendments which may undermine other obligations may not be the best approach.

The beauty of proposed changes that the FATF is considering making to the Glossary of the FATF Methodology for evaluation regarding ECDD is that it specifically refers

Included in the list of specialist facilitators are those that would captured under Tranche II of the AML/CTF regime, were it ever to be enacted.

Beneficial ownership

The problems in this area are the subject of a two-part series that started in the previous issue of *AML Magazine* and conclude with this issue. Australia is not the only FATF member appearing to be reluctant to come to grips with beneficial ownership. If the



to the designated non-financial businesses and professions (DNFBPs) – those lawyers, accountants and real estate agents still missing from the Australian AML/CTF Act. The proposed changes are to require reporting entities, including the DNFBPs, to conduct ECDD for PEPs, correspondent banking relationships, new or developing technologies that favour anonymity and other higher ML/TF risks. For Australia this means that discretion will be replaced by prescription for higher ML/TF risk circumstances and ECDD and will introduce further pressure to implement Tranche II.

On the pressure for Tranche II progress, it is noted that only the FATF is expecting a Tranche II in Australia but DNFBPs are shown as higher risk in the Organised Crime Threat Assessment (OCTA) released by the Australian Crime Commission in a report entitled “Organised Crime in Australia 2009”. On page 9 of the OCTA, the report states that “more and more organised crime groups are becoming involved in money laundering, either directly or by employing the services of facilitators with specialist knowledge.”

requirements of FATF Recommendation 5, the Evaluation Methodology, the Basel CDD paper and the AML/CTF Rules are put to one side, and the ML/TF risk is analysed in pure terms, then the solution is obvious.

AML/CTF systems typically have negative responses to people using aliases. Proprietary companies are avatars or aliases of their beneficial owners. ML/TF risks are unidentified and unmitigated where the beneficial owner has not been identified. As is well known, identification and mitigation of the ML/TF risk that a reporting entity reasonably faces is a required primary purpose of an AML/CTF program for an Australian reporting entity.

Identifying the beneficial owner down to the individual level is thus a fundamental control in any AML/CTF regime. And there is no escaping the FATF’s stated expectation that reasonable steps will also be taken to verify the identity of the beneficial owner except in the limited categories where FATF has recognised that “simplified due diligence” is appropriate.

The battle on beneficial ownership in Australia is coming down to a contest between, on the one hand, processes that have been put in place relying on informal interpretations of the AML/CTF Rules accompanied by generous approaches to identifying ML/TF risks; and on the other, the obvious perils of dealing with opaque entities and the standards set by the FATF. This battle of wills also seems to be in play in other FATF member jurisdictions. If the FATF members are not prepared to step up to compliance with this area of Recommendation 5, then the huge investment in AML/CTF regimes globally could be regarded by the cynical as a complete whitewash. The very fact that identifying beneficial owners in some cases is difficult is itself an indicator of higher ML/TF risk; it is not a reason to seek relief from compliance with FATF Recommendation 5.

Accurate and current information on beneficial ownership of legal arrangements including trusts

AUSTRAC would like industry to comment on what could be done to improve their access to accurate and current information on beneficial owners of proprietary companies and beneficiaries of trusts. The answer must be – “a lot could be done”.

It is inefficient for every reporting entity that provides services to a trust (for example a self-managed superannuation fund or a family trust) to go through the ponderous process of identifying and verifying the trust without the assistance of a national trust registration system.

It is a large gap in accountability for the Australian Securities and Investments Commission not to be required to identify and verify those that are the beneficial owners of proprietary companies, or acquire interests in those companies after incorporation. ASIC should be subject to the full weight of the AML/CTF regime. Creating companies without proper identification processes is anachronistic in these times. Currently, financial institutions are often the only defence in the detection and mitigation of ML/TF risks rather than being one of many defences spread across key points in the economic system.

Your next steps

Engage with AUSTRAC via your industry association on these important issues! Otherwise changes may take you by surprise. ■

AUSTRAC's AML/CTF Compliance Officers survey

Anti-money laundering/counter-terrorism financing (AML/CTF) programs are entering their third year of operation for most reporting entities – assuming that they were put in place by December 2007. The ML/TF risk assessments that are the backbone of these AML/CTF programs are thus around three years old. If you have not already done so, it is time for you to overhaul and review these first-generation assessments. In that process, there is some new information to take on board.

The survey was sent to 356 reporting entities and 150 replied. Of the 150 that replied, not all answered every question. The responses were anonymous.

Ninety-eight percent of the 150 respondents thought their position was set at a sufficiently senior level to identify major deficiencies in the AML/CTF program and to effect changes where required.

On the bright side

Ninety-two AML/CTF Compliance Officers (62.6 percent of the 150 respondents) had more than six years' experience in compliance and risk management.

About one-third said they had an intermediate knowledge of their business and just over a further one-third said they had a basic knowledge of their business.

Ninety-four AML/CTF Compliance Officers had a bachelor's degree or a graduate certificate or diploma.

There has been an increase in resources applied to AML/CTF in the 12 months to September 2009 and the rate of turnover in the role has been very low, with most being the original AML/CTF Compliance Officer or the second AML/CTF Compliance Officer in their reporting entity.

Just over half of AML/CTF Compliance Officers were conducting assurance activities to assess compliance with the AML/CTF Compliance Team Act and Rules.

On the odd side

AUSTRAC noted in its executive summary that reporting entities were well placed

through their AML/CTF Compliance Officer to understand and comply with their obligations under the AML/CTF Act and AML/CTF Rules. Yet, when looking at the data contained in the report:

- 67 AML/CTF Compliance Officers (45.6 percent of the 150 respondents) spent 10 percent or less of their time on AML/CTF matters (including one bank and 17 credit unions);
- 40 AML/CTF Compliance Officers (27.2 percent of the 150 respondents) spent 11 to 25 percent or less of their time on AML/CTF matters (including three banks and 16 credit unions);
- 19 reporting AML/CTF Compliance Officers did not know about AUSTRAC's e-learning courses;
- 25 reporting AML/CTF Compliance Officers did not know about AUSTRAC's typology reports;
- seven reporting AML/CTF Compliance Officers did not know about AUSTRAC's Regulatory Guide;
- four reporting AML/CTF Compliance Officers did not know about AUSTRAC's Guidance Notes;
- 23 reporting AML/CTF Compliance Officers did not know about AUSTRAC's Public Legal Interpretation;
- 16 reporting AML/CTF Compliance Officers did not know about AUSTRAC's Information Circulars; and
- 30 reporting AML/CTF Compliance Officers did not know about AUSTRAC's monthly newsletter.

Among the common issues raised, were the difficulties that the AML/CTF Compliance Officers had in maintaining their own knowledge about AML/CTF and keeping up to date with legislative change. If 72 percent of the

AML/CTF Compliance Officers that responded spend less than 25 percent of their time on AML/CTF, then this might be one reason for understanding why key AUSTRAC publications were not known to them. AUSTRAC urged reporting entities to review the amount of time that AML/CTF Compliance Officers spent on AML/CTF – especially now that all arrangements are in place.

Fifty-two percent of AML/CTF Compliance Officers received some form of performance bonus. Looking at their spread of knowledge about materials issued by AUSTRAC, it is possible to conclude that their appraisals might not include AML/CTF as a predominant assessment factor.

Resource issues were raised by a small number of respondents in all sectors. But, elsewhere in the survey, 91 percent were of the view that they *did* have enough resources. But the fact that only a small number raised resourcing as an issue suggests that the majority of the 72 percent spending less than 25 percent of their time on AML/CTF are doing so not because they are under-resourced, but because they see no need to.

Slightly under one-third of respondents did not think that their membership of a professional association helped them with AML/CTF. It would have been helpful in hindsight if this question had also focused on industry associations, because they are key to AUSTRAC's communication with the different industry sectors (see the AUSTRAC Supervisory Strategy 2009-10).

Upon releasing the report, AUSTRAC Chief Executive Officer John Schmidt said: 'The information presents a snapshot of how those surveyed have interpreted and implemented the obligation to designate an AML/CTF compliance officer.' 'The ultimate aim of the 'AUSTRAC survey series', Mr Schmidt added when asked to comment for this article, 'is to help reporting entities understand and comply with their obligations under Australia's anti-money laundering and counter-terrorism financing legislation. Our plan for the next four years includes building our strategic research capability in regulatory and intelligence matters, as a key way of continuing to bolster the AML/CTF regime.' ■

Enhanced regulation of alternative remittance dealers

Many people rely on remittance dealers to send money overseas to family and friends. It is important that this legitimate service is not misused for criminal activity.

On 9 April 2010, the Government announced it would strengthen the existing regulatory regime for remittance dealers to reduce the risk of money transfers being used to fund people-smuggling ventures and other serious crime.

The vulnerability of remittance services to criminal misuse – including money laundering, terrorism financing and people smuggling – is well recognised by the international anti-money laundering/counter-terrorism financing (AML/CTF) community. Australian law enforcement and national security agencies are also acutely aware of this problem. Strengthening the regulation of the remittance sector will ensure authorities are better able to take appropriate action against remitters who do not comply with their obligations under the regulatory framework.

On 16 April 2010, as a first step in bolstering the regulation of remitters, the

Government announced new AML/CTF Rules to provide the AUSTRAC Chief Executive Officer with the power to deregister remittance dealers who pose a significant money laundering or terrorism financing risk.

On 23 April 2010, the Minister for Home Affairs released a discussion paper, *Enhanced regulation of alternative remittance dealers*, as the start of a consultation process with the remittance sector about the Government's proposals for a more comprehensive regime.

Existing regulation of remittance dealers

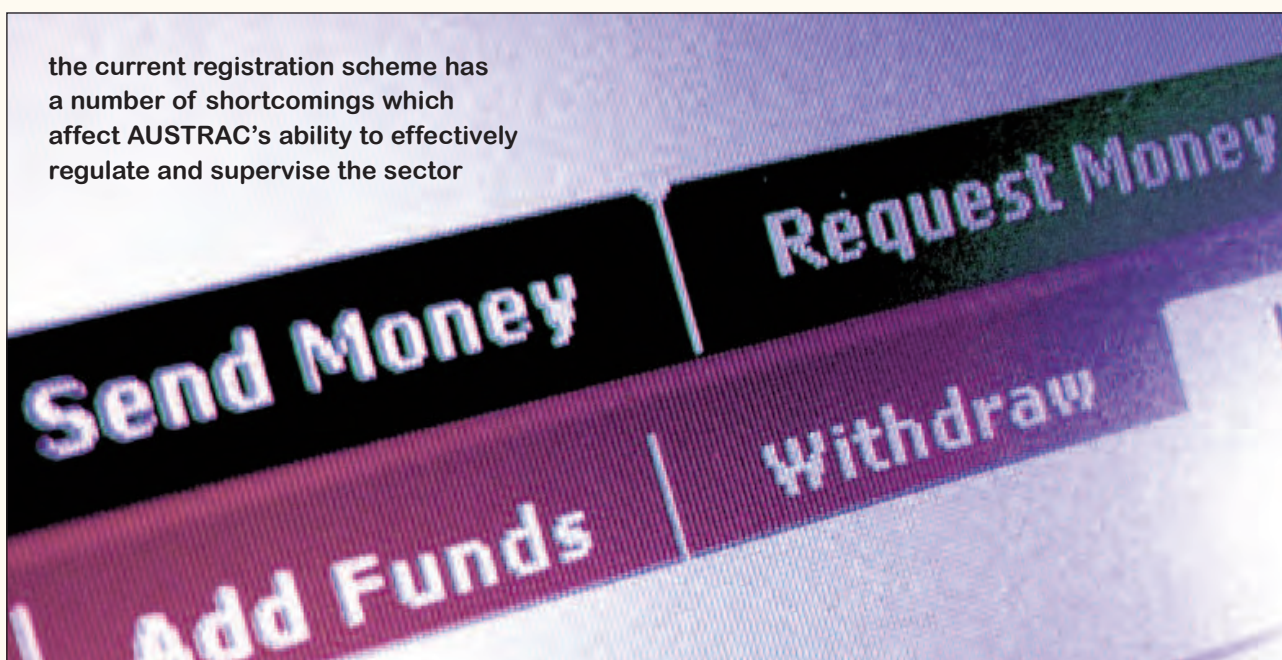
Remittance dealers accept cash, cheques and other forms of payment in one location and arrange the payment of an equivalent amount of cash or value to someone in another location, often overseas. Remitters range from global money transfer businesses, such as Western Union, to smaller remittance businesses operated by a single individual.

Providers of remittance services have a variety of obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act (2006) (AML/CTF Act), including the requirement to register with AUSTRAC before providing funds transfer services, to identify their customers and to establish AML/CTF programs. Providing remittance services without registering with AUSTRAC is an offence which carries a penalty of two years' imprisonment or a fine of \$55,000 or both.

As the discussion paper *Enhanced regulation of alternative remittance dealers* states, the current registration scheme has a number of shortcomings which affect AUSTRAC's ability to effectively regulate and supervise the sector, including:

- anyone can register – there is no suitability criteria that must be met;
- any business can be a remitter – there are no conditions on the way a remitter operates;
- there is no explicit authority to refuse registration or remove or deregister a remitter;

the current registration scheme has a number of shortcomings which affect AUSTRAC's ability to effectively regulate and supervise the sector



- registered remitters are not obliged to update their information or identify their business associates; and
- there are limited sanctions available.

Enhancements to existing regulation

While the AML/CTF Act has always required AUSTRAC to create and maintain a register of providers of designated remittance services, until recently the Act has not provided the AUSTRAC CEO with the power to remove remitters from the register.

The new AML/CTF Rules, effective from 16 April 2010, do provide for this. The Rules make it possible for AUSTRAC to deregister remittance dealers where the CEO considers the remittance dealer poses an unacceptable money laundering or terrorism financing risk.

In relation to registration of remittance dealers, the new regulatory arrangements being proposed include:

- powers for the AUSTRAC CEO to refuse, suspend, cancel or impose conditions on registration;
- obligations on applicants to disclose matters relevant to beneficial ownership and control; and
- obligations on applicants to disclose matters relevant to character, such as criminal convictions or a history of regulatory non-compliance.

Other proposed measures include:

- publication of a list of registered remitters;
- publication of a list of deregistered remitters; and
- obligation on reporting entities to provide a suspicious matter report to AUSTRAC when they suspect they are dealing with an unregistered remitter.

Maintaining a secure remittance sector

The remittance sector offers a valuable and important service and must be kept safe from criminal misuse.

The enhanced AUSTRAC powers will further help to identify those remittance dealers who pose a significant risk, in particular with links to money laundering, terrorism financing or people smuggling.

How remittance services can be misused

The typology and case studies reports published by AUSTRAC each year are important tools to assist reporting entities in understanding various money laundering and terrorism financing risks.

Descriptions of some of the ways in which remittance services can be used for illegal pursuits can be found within these reports.

The *AUSTRAC typologies and case studies report 2010*, which is due to be released shortly, contains a significant number of cases related to remittance services, including the following example:

Gambling debts drove drug couriers to smuggle heroin

Law enforcement officers commenced a joint agency investigation into a Vietnamese syndicate suspected of using drug couriers ingesting heroin to smuggle it into Australia.

The main suspect of the syndicate came to the attention of law enforcement officers during a previous law enforcement operation against her associates. These associates had been charged with drug trafficking and importation after also using couriers who had ingested drugs.

The heroin was purchased in Vietnam with funds remitted via Vietnamese remittance dealers serving Vietnamese communities in Australia. The couriers were then flown to Vietnam to make the return journey, with the drugs concealed internally.

The joint law enforcement investigation led to the arrest of the main suspect, as well as six couriers recruited in Melbourne – it is suspected that some of the couriers may have been coerced into trafficking drugs because they owed gambling debts.

The main suspect was a partner in a business that used a cheque-cashing service to pay staff wages, and she had been using the cheque-cashing service to help fund the heroin purchases.

The suspect was charged with importing and trafficking commercial quantities of heroin and crystal methamphetamine hydrochloride (ice). ■

EDITORS' NOTE:

IN THE AUSTRAC'S Annual Report, 2008-2009, it was stated that as at 30 June 2009 a total of 5,401 remittance dealers (about 83 percent of the estimated population) were registered with AUSTRAC. This compares favourably to 30 June 2008, at which time 2,590 remittance dealers had registered. AUSTRAC estimates that there are about 6,500 remittance dealers operating in Australia – around 38% of the total population of reporting entities (AUSTRAC recently advised that there were 16,783 reporting entities).

The Government's discussion paper raises many interesting issues, including:

- Provision of a downloadable list of the names of remittance dealers, adding to the lists that reporting entities may use for screening customers;
- Whether a downloadable list of names should also include beneficial ownership information;
- How a bank, building society or credit union should be monitoring and managing the ML/TF risks posed by their remittance dealer customers;
- Whether providers of remittance networks (for example those that franchise their systems to agents) should be required to provide compliance systems to their agents;
- Whether remittance customers should be subject to an appropriate level of regulation from an APRA or ASIC style body rather than relying solely on anti money laundering laws to govern their conduct;
- The difficulties low capacity entities have with the amount of information generated by AUSTRAC regarding the AML/CTF regime;
- The untapped power of the interposed person provision in Division 4 of Part 5 of the AML/CTF Act. ■

Lenders Beware!

By Greg Standing

The decision of the Court of Appeal in *Shah & another v HSBC Private Bank (UK) Ltd* (HSBC) will give lenders cause for concern. The court has held that a customer whose instructions were not initially complied with due to money laundering concerns is not bound to fail in a subsequent claim against the lender for losses suffered as an alleged result of the subsequent delay in carrying out those instructions.

The facts of the case

The claimants held accounts with HSBC and instructed it to transfer several large sums of money from various accounts held with it and to make some payments out. Suspecting that the funds were criminal property, HSBC disclosed its suspicions in relation to a number of transactions to the appropriate authorities, as it was required to do, so as to avoid criminal liability under the Proceeds of Crime Act 2002 (POCA). It then had to await the appropriate consents under POCA before being able to fulfil the claimants' instructions in the usual way.

Consents were subsequently given and the transfers were made. The claimants sought reasons why their instructions had not been complied with. HSBC's response was that it was complying with its UK statutory obligations, but gave no further information once the transactions had been completed.

The claimants contended that HSBC's failure to carry out their instructions or to properly explain the reasons for not doing so had caused their affairs elsewhere to be scrutinised, as a result of which they had suffered substantial loss. They brought a claim for breach of duty against HSBC for failing to take reasonable care in maintaining the account and for failing to provide information

about the disclosures made to the authorities. They further alleged that HSBC had failed to take reasonable care by not making those disclosures as soon as reasonably practicable. They also argued that there were no rational grounds to suspect the claimants of money laundering and if its "suspicion" was induced by irrationality, negligent self-induced suspicion, mistake or automatically by, for instance, a mechanical error, then it would not be a relevant suspicion.

HSBC applied to strike out the claim.

First instance decision

The judge dismissed the claims based on irrationality, negligent self-induced suspicion and mistake on the basis that the relevant suspicion need not be based on reasonable grounds. The suspicion need only be based on a possibility which was more than fanciful that the relevant facts existed. HSBC's evidence showed that employees had been involved in the decision-making process so the "suspicion" had not been mechanically generated either. The judge held that for a customer to impugn the decision to make an authorised disclosure it had to challenge the good faith of the lender's suspicions. The claimants had not challenged HSBC's or its employees' good faith and the claim for breach of duty therefore had to be struck out.

The decision on appeal

The Court of Appeal agreed with the judge's findings on the issues of irrationality, negligent self-induced suspicion, mistake and mechanically generated suspicion.

However, most importantly, it held that there was no reason why the claimants could not require HSBC to prove its case that it had the relevant suspicion. The claimants' claim was not fanciful; HSBC was not bound to win. Any claim by a customer that their bank had not executed their instructions is, on the face of it a strong case, if indeed the instructions have not been complied with. It is only when the bank says it suspects money-laundering that a defence begins to emerge. There was no reason why HSBC should not be required to prove the important fact of suspicion in the ordinary way at trial, by first giving relevant disclosure and then by way of witness evidence. There was a danger of injustice without this.

The court appreciated that tipping-off under s333 POCA was highly relevant and could determine what evidence was admissible and who could give it. However, by the

time this action came to trial it would be unlikely that there would be any issue regarding tipping-off as any investigation would likely be over by then; and if it wasn't, the court could be informed of that in an admissible manner. To find otherwise would, in effect, be giving carte blanche to banks to decline to execute their customer's instructions without any court investigation.

The court did not accept either that disclosure of relevant documents, including those reporting a bank's suspicions to the relevant authority, would not or should not be ordered by a court as that would lead to the dispute being completely unjusticiable with the bank inevitably winning. There might be good argument for concealing part of a document or (more doubtfully) declining to disclose all of the documents but a judge in chambers could make that decision.

The court accepted that banks have been placed in an unenviable position by POCA.

Any claim by a customer that their bank had not executed their instructions is, on the face of it a strong case

They are at risk of criminal prosecution if they don't report their suspicions, or report them but carry out their customer's instructions without authorisation. If they act as instructed by the authorities, their customers may become incensed and commence proceedings. However, that does not mean that litigation should be dismissed without any appropriate inquiry of any kind. The court's procedures should not be sidestepped unless there is an express statutory provision to that effect.

The order striking out the claim would be set aside.

The court also went on to confirm that a bank's duty of care is not completely excluded by POCA and, in principle, delay in making a relevant disclosure under POCA might be a breach of duty. There was no delay here though and so no breach. Additionally, there was no requirement for a bank to seek advanced consent under POCA in respect of future payments as the claimants argued. The authorities would be unlikely to give consent in the abstract before any payment instruction was given. Neither should disclosure have been made when the money was first paid into the claimants' account as no question of seeking authority to execute a payment instruction can arise until a payment instruction is made.

The court further held that there was an arguable breach of agency duty. An agent (the bank) is (arguably) obliged to keep his principal (the customer) informed as to the state of his principal's affairs, especially when the principal requests information. The tipping-off provisions are highly relevant here but there must come a time when, after tipping-off is no longer relevant, a principal is entitled to have more information about his affairs than the claimants had yet been given here. When that would be would be a matter of evidence.

Comment

Although the claimants get to fight on, on both the "suspicion" and provision of information points, it does not mean that they are bound to win. It is not a high threshold that HSBC has to meet – the suspicion has to be just a possibility, which is more than fanciful, that the relevant facts existed. The statute

does not require the suspicion to be "clear" or "firmly grounded and targeted on specific facts" or based on "reasonable grounds", although a vague feeling of unease would not suffice.

Lenders should go through a human process of looking at the facts, establishing a possibility that is more than a vague feeling of unease and having the decision checked by someone else. The more people involved in the decision-making process as to whether there is enough evidence to raise a suspicion, the more likely it is that the basis of that suspicion will be justified. A clear audit trail of such steps should be maintained in case the decision is ever challenged. ■

Greg Standing is a Partner in Wragge & Co LLP's Banking and Finance Litigation Team specialising in contentious disputes for banks and lenders. He has a particular interest and specialism in financial crime cases. Wragge & Co LLP. Wragge & Co is a major UK law firm providing a full service to clients worldwide, including 27 FTSE 100s, 22 FTSE 250s, hundreds of public sector organisations and thousands of large private companies, from its offices in Birmingham, Brussels, Guangzhou, London and Munich. http://www.wragge.com/lawyersearch_greg_standing.asp

National threat assessments

– where would we be without them?

*By Gordon Hook, Executive
Secretary Asia Pacific Group on
Money Laundering Secretariat*



Introduction

Responding to many demands from the international community, the Financial Action Task Force is poised to release a *Global Threat Assessment* report in June or July 2010 summarising its concerns over the worldwide risks of, and systemic vulnerabilities in relation to, money laundering (ML) and terrorist financing (TF). The report will contain a broad outline of ML and TF risks and sketch consequent harms in three ascending groups:

- harms at the individual/local level;
- harms at the community/regional level, and;
- harms at the national and international level.

Drawing on previous research (in 2008 and 2009) the FATF report will consolidate a variety of statistics and country reports. It is anticipated the report will provide an invaluable tool for policy development in countries committed to implementing the FATF standards.

Background

Not so long ago, the major risk of money laundering was reflected in the stereo-typical image of a money launderer who took bags of cash to a bank for deposit looking satisfied when leaving. Unbelievable in today's environment, in a 1982 United States case over \$US242 million in cash was deposited at one Florida bank over the course of a few months by untidy-looking individuals carrying paper bags and suitcases full of cash – up to \$US2 million at a time in small denomination notes (United States v \$4,255,625.39, 551 F Supp 314 (S.D. Fla. 1982)). Bank tellers were struck by an “actual narcotics smell” when counting the cash.

A similar string of cases occurred in Canada at about the same time and into the 1990s, when members of the Caruana-Cuntrera mafia family placed bags of cash in pick-up trucks, backed the trucks up to a bank's front door and threw the bags to the bank staff inside to empty, count and deposit. Once deposited, the money was quickly wire-transferred to offshore accounts (Nicaso and Lamothe, *Bloodlines: Rise and Fall of Mafia's Royal Family* (Toronto: Harper Collins 2000)).

While the unkempt drug dealer rarely fronts the bank with dirty money today, the funds still make it there, one way or another. Laundering money has taken on global proportions involving sophisticated methods such as over and under-invoicing of goods shipped through the international trade system, over-funding life insurance policies, discounting electronic stored-value cards and sophisticated casino transactions (including intentional losses), as well as the engagement of intermediaries such as lawyers, accountants and front companies. The infestation of criminal proceeds in the international financial system via weak domestic

anti-money laundering counter-terrorism financing (AML/CTF) systems has been a concern of the United Nations for many years – at least since the 1988 Convention Against the Illicit Trafficking in Narcotics – but with greater focus since 1999, with the UN Convention Against Transnational Organised Crime. But no comprehensive study of the risks and vulnerabilities inherent in the international system has been undertaken.

This new FATF report will therefore be welcomed by many governments as a policy tool for greater efforts to tighten their systems and deal with sophisticated white-collar money launderers – not just the scruffy looking criminals with bags of loot who have disappeared from view.

FATF standards

While the “general interpretation and guidance” section in FATF's methodology handbook states that a country may decide not to apply some or all of the FATF Recommendations where there is a “proven low risk” of ML or TF, the rest of the handbook (including the

While the unkempt drug dealer rarely fronts the bank with dirty money today, the funds still make it there, one way or another.



Recommendations themselves and the Interpretative Notes accompanying them) provides no guidance or suggestions on how to do this; nor do the Recommendations explicitly require that a national risk assessment be conducted by any particular country, either before or after implementing the measures contained in the international standards.

However, from a policy perspective it is difficult to see how a comprehensive and well-developed AML/CTF strategy, including the exemption of some sector activities, could exist without such an assessment. Common policy-sense strongly suggests that this kind of analysis should be undertaken in order to better understand the environment within which a country will implement, or better refine, its systems to combat financial crime.

The process and use of assessment

"A national ML/TF risk assessment is an organised and systematic effort to identify and evaluate the sources and methods of money laundering and terrorist financing and weakness in the AML/CTF systems and other vulnerabilities that have an impact, either direct or indirect, on the country conducting the assessment" (FATF 2008).

An effective assessment should bring together the public and private sectors. Public authorities (including law enforcement and prosecution agencies, regulators and supervisors) have privileged access to information that can assist financial institutions to reach informed judgments when pursuing a risk-based approach to counter ML and TF. The private sector, in particular financial institutions, understands its business geography and its clients better than government.



Once completed, the national risk assessment will have value for:

- government: to assist in formulating and implementing a national strategy to combat serious crime, and to establish AML/CTF priorities;
- law enforcement/prosecution agencies: to assist in focusing investigative, prosecutorial and judicial resources;
- the private sector: to assist financial and non-financial institutions to implement and operate a risk-based approach;
- technical assistance providers: to assist bilateral and multilateral technical experts in delivering programs and assistance to jurisdictions in need; and
- academics: to better inform the academic community of the reasons and rationale for FATF and the activities of FATF-style regional bodies such as the Asia Pacific Group on Money Laundering (APG).

The FATF report will cover these points in detail, and in doing so will better inform

which includes two other templates to assist countries to prioritise ML and TF risks and to develop and implement a national AML/CTF action plan.

The National Risk Template is designed to assist jurisdictions to understand the sources and methods of ML and TF; to identify vulnerabilities and risks across various sectors; and to evaluate weakness in their legal, judicial and institutional systems. It does this by focusing their attention on a number of domestic information sources:

- prevailing crime type;
- legal/jurisdictional /institutional framework;
- economic and geographical, environment; and
- reporting institutions (financial and non-financial).

Some of the factors under the economic and geographical environment include considerations of whether the economy is highly dollarised; the degree of international financial system integration; whether there is a large number of alternative remittance systems; and whether there is an off-shore financial centre within the jurisdiction. These and other factors are critical to a comprehensive assessment and are also factors incorporated into the FATF report to be released.

A copy of the SIP framework document is publically available on the APG website at www.apgml.org and is already being used by many countries outside the APG region.

Feedback from APG member countries that have used the SIP framework in their AML/CFT policy development is very positive. The new FATF report will add value to these already existing SIP plans and will place them within a broader international, as opposed to a local, domestic, context. In this regard, APG membership fully endorses this FATF product.

Conclusion

The upcoming FATF *Global Threat Assessment* will be a welcome document for many countries in the APG region. Financial institutions, as well as national policymakers, should pay close attention to this document. It will assist countries and institutions to develop their own assessments. And it will help countries to prepare for another round of FATF and APG mutual evaluations which will commence after 2012. ■

An effective assessment should bring together the public and private sectors

Once relevant sectors are on board for the exercise, the question becomes: how is a risk assessment to be undertaken? For this purpose, the FATF has suggested an overarching methodological framework which identifies:

- 1) the features that are used by money launderers and those who fund terrorists and their activities. Features include: cash and bearer-negotiable instruments, transfer of value, assets/stores of value, gatekeepers and environmental/jurisdictional issues;
- 2) the main harms that are caused by the abuse of these features;
- 3) the reasons (or what FATF says are drivers and enablers) why criminals and terrorists use certain features; and
- 4) how the harms can be reduced or mitigated through the application of various measures.

the international financial sector, as well as domestic financial systems, of key factors to address to mitigate the identified risks.

APG's strategic implementation planning framework

It was noted in the APG a few years ago that many of the risk assessments seen during mutual evaluations of APG members were light on the assessment of risk and heavy on the perception of it. In response, the APG, in consultation and collaboration with the World Bank, decided to develop a risk-assessment template to assist countries to finalise more analytical, and thus more helpful, assessments. The template is part of a document referred to as the Strategic Implementation Planning (SIP) Framework,



Catch up on the amendments to the AML/CTF Act

The Anti-Money Laundering and Counter-Terrorism Financing Act (AML/CTF Act) received its first substantive round of amendments in February, addressing a loophole in the definition of a designated remittance arrangement.

The amendments came into effect on 20 February 2010, when the Crimes Legislation Amendment (Serious and Organised Crime) Act (No. 2) 2010 was passed. A current consolidated version of the AML/CTF Act is available from the Government's legislative website (www.comlaw.gov.au) or from Austlii (www.austlii.edu.au).

The loophole

Before the amendments, a designated remittance arrangement required two persons, both of whom were not authorised deposit-taking institutions, banks, building societies or credit unions (see section 10 of the AML/CTF Act). This allowed any alternative remittance dealer who sent their transactions through, or to, an authorised deposit-taking institution, bank, building society or credit union which then became the releasing party of the funds to fall outside the reach of the AML/CTF Act. There are several such models in operation in Australia:

- Those that send funds to banks in overseas countries and the recipients of those funds (who will invariably not hold an account with that bank) physically go to the bank, and on supply of the matching PIN and identification information, receive the funds in physical currency; and

- Those that receive funds by telegraphic transfer to their bank account and then create fresh instructions to send the funds via telegraphic transfer through the banking system to banks overseas for deposit into a bank account.



The cure

A category of "non-financier" has been created in the definitions section of the legislation. All persons who are not authorised deposit-taking institutions, banks, building societies or credit unions are defined now as "non-financiers". Section 10 has then been amended to define a designated remittance arrangement as only requiring that one of the persons in the transaction flow be a non-financier.

The designated services in items 31 and 32 of Table 1 of Section 6 of the AML/CTF Act have then been amended to catch those that carry on a business of giving effect to designated remittance arrangements. Without the amendments to items 31 and 32, the

introduction of the non-financier definition and the changes to Section 10 would have caught many people in circumstances where it was not so intended. Flow-on changes dealing with the new term of "non-financier" appear in Section 46, which also closes loopholes in the international funds transfer instruction obligations for alternative remittance dealers. Section 64(2) of the AML/CTF Act has not been amended because any person (including authorised deposit taking institutions, banks, building societies or credit unions and a non-financier) may be an interposed person. Section 64(2) may well apply to those that receive funds by telegraphic transfer to their bank account, and then create fresh instructions to send the funds via telegraphic transfer through the banking system to banks overseas for deposit into a bank account.

Other changes

The definition of stored-value card has been changed to exclude debit and credit cards and to include not only the capability to store value but also to be used to gain access to monetary value stored on the card. Flow-on amendments have been made to items 21-24 in Table 1 of Section 6 by expanding the nature of what storage means: from being stored on, to being stored in connection with.

Section 123 has received some technical amendments around the prohibition on disclosing to anyone that information or documents have been provided to a person under section 49(1) of the AML/CTF Act. Section 49(1) provides AUSTRAC and certain other agencies the power to seek further information if a suspicious matter, threshold transaction or international fund transfer instruction report has been lodged.

Criminal Code amendments

The money laundering provisions in the Criminal Code Act have also been amended in a variety of ways. Reporting entities would be unlikely to be directly considering the application of these sections unless they were considering circumstances where it was unclear if there were grounds for making a suspicious report under Section 41. ■



Australia's first **Organised Crime Threat Assessment**

A risk-based anti-money laundering/counter-terrorism financing (AML/CTF) regime assumes that a money laundering and terrorism financing (ML/TF) risk assessment will be undertaken by regulated entities. These regulated entities, left to their own devices, do not have access to the kind of information needed for such risk assessments. Government, law enforcement and criminal intelligence agencies on the other hand, hold or have access to this information to the extent that it has been captured. Regulated entities are thus dependent on their governments, law enforcement and criminal intelligence agencies to package this information into official risk assessments and make it available to them.

Issues of quality of data, quality of analysis and confidentiality all impede the ability for this kind of information to be released into what is essentially the public domain. These issues also impede on the capability of organisations to critique what is released for its adequacy and completeness. Incomplete or inaccurate risk assessments at the national level can see AML/CTF efforts skewed in the wrong direction and potentially increase ML/TF risk rather than mitigate it.

In a sister article in this issue of the magazine, Gordon Hook of the Asia Pacific Group on Money Laundering discusses a soon to be published *Global Threat Assessment* by the Financial Action Task Force. So where is Australia in terms of developing this much-needed national threat assessment?

In 2009, the Government released a Strategic Framework setting out its response to organised crime. A key component of the Strategic Framework is the first Organised Crime Threat Assessment (OCTA) released by the Australian Crime Commission in a report entitled "*Organised Crime in Australia 2009*".

AML/CTF programs are entering their third year of operation for most reporting entities, assuming that they were put in place by December 2007. The ML/TF risk assessments that are the backbone of these AML/CTF programs are thus around three years old. If you have not already done so, it is time for you to overhaul and review these first-generation assessments.

The OCTA is one piece of new information you should be taking on board in that review.

The Strategic Framework

There are five challenges set out in the Strategic Framework, which might be also seen as vulnerabilities Australia has in respect of the threats posed by organised crime.

The five challenges are:

- 1) The level of knowledge of organised criminal networks and their flexibility, dynamic nature, level of innovation and resilience to traditional organised crime interventions;
- 2) The opportunities presented by the acquisitive crimes of illicit commodities (predominantly drugs and firearms), fraud, high-tech crime, environmental crime, piracy, counterfeiting, people trafficking, identity crime, public sector corruption and labour exploitation, and money laundering associated with these predicate offences;
- 3) The successful reliance of organised crime on infiltration of information technology, accountants, lawyers,² bankers, law enforcement, public sector agencies and industry, as well as significant footholds in certain industry sectors;
- 4) The continued existence of a clandestine black market economy out of view, and functioning with strong competitive advantage through non-compliance with regulatory and fiscal processes; and
- 5) Possession of well-developed capacity to operate across multiple domestic and overseas jurisdictions.



The Australian Crime Commission's OCTA

The stated purpose of the OCTA is to provide a shared picture among stakeholders of the most significant threats and harms arising from organised criminal activity. The FATF Guidance on the Risk Based Approach released in 2007 noted that, in a risk-based model, countries will need to identify the main vulnerabilities to ML and TF and address them accordingly.

The need for a national risk assessment was enshrined in the first of the five principles in the Guidance and was seen as fundamental to a successful implementation of a risk-based approach within a country.³ Reporting entities

Reporting entities should be counting themselves in as key stakeholders in the OCTA

should be counting themselves in as key stakeholders in the OCTA, given the objects of the AML/CTF Act.⁴ The FATF Guidance also states that the private sector should be involved in discussion about how best to allocate resources and responsibilities to respond to identified threats.

Clearly it follows that those reporting entities that consider relevant aspects of the OCTA in their ML/TF risk assessment place themselves in a strong position to defend its adequacy to AUSTRAC.

The OCTA will be produced biannually, so the next OCTA is expected in 2011. Of relevance to ML/TF risk assessments are the following characteristics of high-threat organised crime groups. The risk indicator column has been added in the course of

preparing this article, suggesting ways in which the characteristic might be detected through AML/CTF systems operated by reporting entities. A number of the characteristics are clearly not able to be identified or treated within an ML/TF risk assessment used by a reporting entity in the financial services sector.

Crime markets

The OCTA identifies the high-risk crime markets as involving illicit drugs such as the production and supply of amphetamines, MDMA (ecstasy) and cannabis, and the importation and supply of cocaine and heroin. Add to that list financial-sector crime (including fraud and market manipulation) and money laundering. On page 9 of the OCTA, the report states that

**OCTA is a
greyhound
version by
comparison
at 16 pages**

“more and more organised crime groups are becoming involved in money laundering, either directly or by employing the services of facilitators with specialist knowledge.”

These are the specialist facilitators that would captured under Tranche II of the AML/CTF regime, were it ever to be enacted.

Threat assessments overseas

The United Kingdom is the most relevant regime to look at when considering the relative maturity of risk assessments. The 2009/10 UK Threat Assessment weighs in at 82 pages, including covers and introductions, and the OCTA is a greyhound version by comparison at 16 pages including covers and introductions. The stated purpose of the UK Threat Assessment is to help public and private organisations develop “target hardening” measures. Threats are broken into five main categories and then broken down into further specific threats.



Characteristic:	Suggested risk indicators:
Having transnational connections.	Connections with overseas countries through place of birth, establishment, incorporation, operation. Location of beneficial owners or controllers. Location of nominee directors and shareholders. Source of funds. Source of wealth. Source or destination of transactions.
Having proven capabilities and involvement in serious crime of high harm levels including illicit drugs, large-scale money laundering and financial crimes.	This will be hidden from the reporting entity and might only be detected through monitoring for suspicious activity or through due diligence processes responding to red flags.
Having a broader geographical presence and will generally operate in two or more jurisdictions.	Same indicators as transnational connections, and also applied similarly at the domestic level.
Operating in multiple crime markets.	See intermingling of legitimate and criminal enterprises.
Engaging in financial crimes such as fraud and money laundering.	This will be hidden from the reporting entity and might only be detected through monitoring for suspicious activity or through due diligence processes responding to red flags.
Intermingling legitimate and criminal enterprises.	Overly profitable businesses. Cash intensive businesses in high-risk sectors. Participation in sectors infiltrated by organised crime such as finance, entertainment, telecommunications, building, transport, private security).
Being fluid and adaptable, and able to adjust activities to new opportunities or respond to pressures from law enforcement or competitors.	This will be hidden from the reporting entity and might only be detected through monitoring for suspicious activity or through due diligence processes responding to red flags.
Being able to withstand law enforcement interventions and rebuild quickly following disruption.	This will be hidden from the reporting entity and might only be detected through monitoring for suspicious activity or through due diligence processes responding to red flags.
Increasingly using new technologies.	
Using specialist advice and professional facilitators.	Involvement of intermediaries. Due diligence on intermediaries Complex structures without reasonable explanation.

Although the annual threat assessment in the U.K. has been published for a number of years, it has now been enhanced by the use of a Harm Framework, which is designed to help drive decision-making and to underpin the control strategy responding to the threat assessment. This concept of harm appears as a constant thread in Hook's article on National Threat Assessments in this issue.

Broad estimates of the economic and social costs of organised crime, including the cost of combating, are upwards of \$33 billion a year for a population of 65 million people. Australia's estimates are at least \$10 billion, for a population of 21.5 million. There is an uncanny similarity in those two figures, despite Australia's location being far from the crime markets of the United Kingdom, Europe and Africa.

The multiple references in the UK Threat Assessment to the involvement of "specialists" reinforces the need already noted for Tranche II to be introduced in Australia. In the wide range of specialists discussed are the usual suspects of lawyers, accountants and company formation services. Serviced offices receive a mention, perhaps to the surprise of this sector in Australia.

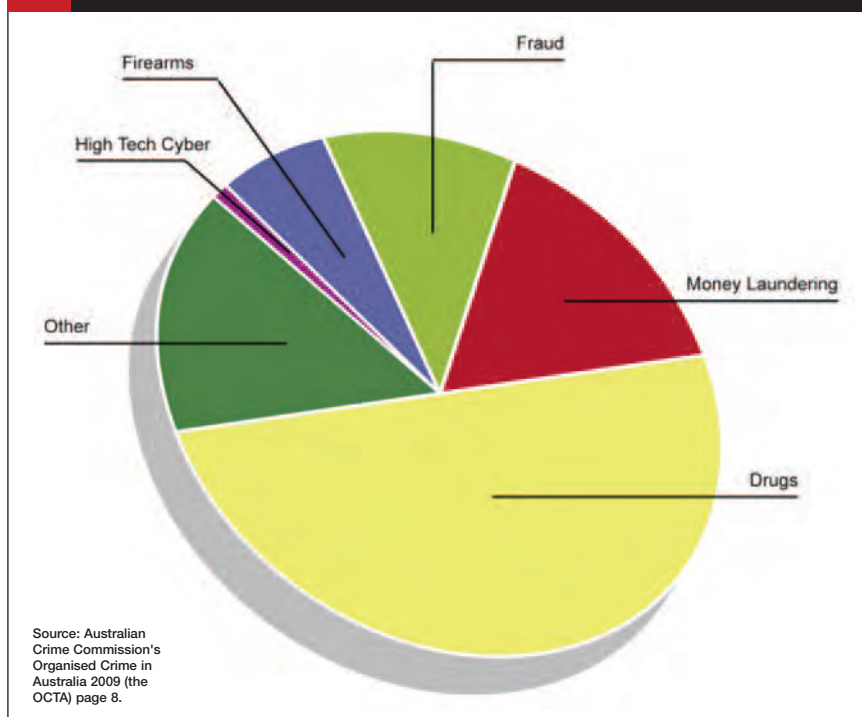


The UK Threat Assessment reflects the state of evolution of the UK approach to organised crime and includes a strong consultation process with regulated entities.

The UK Threat Assessment reflects the state of evolution of the UK approach to organised crime and includes a strong consultation process with regulated entities. It is a step forward that, within three years of introducing the AML/CTF Act, the Government has embarked on the Strategic Framework and the Australian Crime Commission has published the first OCTA. A gap of two years until the next edition of the OCTA is unfortunate, given the room for natural maturing of the process and its importance to reporting entities and their ML/TF risk assessments. The OCTA's focus on organised crime is not explained by reference to other threats relegated to lower priorities. It is not transparent how much the major reporting entities were included in its development.

AML/CTF Compliance Officers may find it useful to read the UK Threat Assessment and identify relevant indicators for their business and then lobby the regulator for more information in areas which are not covered by the OCTA as well as for greater involvement in the development of the next version. An area ripe for research is the use that regulated firms and reporting entities make of the UK Threat Assessment and of the OCTA, and to what extent these reports fall short of their needs.

Organised criminal involvement in criminal activities in Australia



¹ AUSTRAC has made a significant contribution through the publication of its annual typology reports and these deserve consideration in any review of ML/TF risk assessments.

² It is interesting to note these observations in the Framework against the ongoing silence as to the implementation of Tranche II, widening the scope of the AML/CTF Act to accountants and lawyers.

³ Paragraph 1.9 on page 2 and Principle One set out on page 11 of the FATF Guidance on the Risk-Based Approach to combating Money Laundering and Terrorist Financing.

⁴ See section 3 of the AML/CTF Act and the Objectives outlined in the Amended Explanatory memorandum at the time the Act was introduced into the Australian Parliament in 2006 as a Bill (Page 7).

Internal Fraud

Managing the fallout from the GFC

By Adam Courtenay

There is one oblique area of financial services which tends to proliferate during a financial crisis, and the world never hears about it. Accountants are reporting an unprecedented boom for their forensics departments, because the period after a downturn is when the fallout from fraud tends to unhappily manifest itself.



Deloitte Australia claims it has undertaken as much as five times its normal work in this area over the past 12 to 18 months and there is no sign of it slacking off. KPMG has also reported a considerable increase in its forensics business, and the need to take on new personnel to cope with the upsurge.

Anti-Money Laundering Magazine asked Australia's big four accountancy firms where the frauds are coming from, their extent and what can be done to keep them in check. One thing emerged across all four service providers – their forensic departments are no longer the quiet achievers – the global financial crisis has catapulted them into a major revenue line.

Secrecy

Internal as well as “close to home” fraud is the corporate stain which dare not speak its name. While the media tends to hype up the proliferation of external, web-based fraud – the problems with cloud computing, cyber-hackers, criminal gangs and the potential penetration of susceptible social media – internal fraud remains by far the biggest problem for corporate Australia.

“It is the people within – not to mention the major relationships with customers and suppliers that are struck from close quarters –

It has long been believed that banks – and most other financial services firms – are more susceptible to external fraud than internal employee-related fraud, but not all agree.

Gill says the financial services sector is necessarily outwardly focused on external attacks but that it is becoming increasingly concerned about the threat from within.

“Who is more likely to have access to client details and personal information about customers – people without or people within?” asks Gill. “If you can steal that information – use their names to apply for loans or credit cards, or be able to get into another person's account and either forge or misuse their ID documents, you're already there,” he says.

Impact of GFC

It is the GFC which has tipped the scales on employee fraud. Paul Fontanot, Ernst & Young's head of fraud investigations, mentions one case where an employee of a superannuation provider was nearing retirement but unhappy with his super portfolio. Having seen the impact of the GFC, he used available company information for his own benefit, not thinking that he would be noticed.

The employee was able to find out the pricing of all share deals before they were officially stated and accrued to portfolios, and arbitrated his fund accordingly.

Look more closely at the rot within thyself, say the forensics experts, not to external, unspecified forces supposedly doing you harm from afar

which count here,” says KPMG's most senior forensic expert, Gary Gill. KPMG says its fraud surveys show that around 65 per cent of frauds perpetrated on companies are internal.

Steve Ingram, head of PricewaterhouseCoopers' risk practice in Melbourne, says over a third of organisations in Australia will have lost \$1 million or more in economic crime during the worst part of the financial crisis. “That beats the average globally and regionally,” Ingram asserts.

The scope of internal fraud relates as much to financial services companies as it does to any Australian corporate. Look more closely at the rot within thyself, say the forensics experts, not to external, unspecified forces supposedly doing you harm from afar.

“He was able to buy the right shares in his plan when the market went up and switch to cash when the market went down, thereby avoiding losing money,” says Fontanot.

“He was caught because, lo and behold, when everyone else's super portfolio went down, his went up, thereby bucking the predicted trend.”

Outsourcing

There are unique risks in the financial services arena, and one of the most critical is outsourcing arrangements. More than any other sector, its managers need to outsource to other firms – either to sell upfront to clients or to do back-office processing – and yet financial

services firms rarely consider what risk these outside connections pose, says Gill.

“Once you have given the outsourcer access to your information, you have to ask whether they monitor their staff,” asks Gill. “What controls do they have in place – do custodians and administrators have equal access to your information, and how do they monitor and control risk?”

Analytics tools

Also, do big firms have the right to audit and review a third party? All four forensic accountants have what they term “continuous” monitoring and analytics tools – capable of generating reports to clients about red flags, which could be used by the main product provider to analyse information coming in and out of its administrators and custodians.

“There's no reason why a bank couldn't have analytics tools provided for use by itself and for other suppliers and administrators – another layer of monitoring,” says Gill.

This kind of back-end analytics may be an expense, but it could be a critical one. On the front-end side, firms transacting through a broker or financial adviser should know whom they're dealing with from a fraud risk perspective.

If the company is providing a super product to a customer through a financial adviser and yet never sees the customer, how does the company guarantee that the adviser is not wrongfully accessing – and even abusing – customer information and/or data?

In the end it is about monitoring the back and front ends – both the data coming in and going out – using forensic tools to discern anomalies.

The big four – and other forensically inclined accountancy firms – are being brought in to insurance companies, banks and brokers often with both a covert and an overt role: overtly as auditors to check accounts; and then covertly to dig deep inside company data to check for forced and unforced errors.

Segregation of roles

Fraud tends to be found at the lines where employees, suppliers and customers intersect, and specialists never tire of saying that companies which fail to segregate authorisation and custodial duties will always be more susceptible. They also point to the need to regularly test internal controls for weaknesses and ensure they are operating as intended.

“What many firms don’t seem to realise is that they can use their own data to understand what’s happening inside themselves – companies are data-rich whether they have one large system or a stock of disparate sys-

Forensic experts say they are often amazed at the simplicity of so many of the frauds. It’s not so much new-fangled smart frauds but the same old favourites – payroll fraud, online payment fraud, procurement fraud and supplier fraud – just perpetrated more efficiently using modern technology.



Forensic experts say they are often amazed at the simplicity of so many of the frauds

tems – all this can be used for self-compliance,” says Kelvin Kenney, a partner in Deloitte’s forensic practice.

As Kenney explains, it’s the inefficiencies of data collection and processing, the ability (or not) to flag and amend errors and mistakes that crop up, which provide continuous proof of corporate vulnerability.

Whistleblowers

Last but not least, a whistleblower process – which may incorporate a number of lines of access to report suspicions anonymously, is deemed essential. Deloitte Forensic research found that around 70 percent of frauds are identified by someone else in the organisation, and over 80 percent of staff who will not report fraud cite a fear of retribution as the reason.

False Invoicing

On the accounts payable side, all four accountants are seeing a lot of false invoicing – the setting up of bogus vendors and then the processing of false invoices. There is also a lot of simple online payment fraud, much of which is barely disguised. “Sometimes fraudsters just transfer money straight out of the company account into their personal accounts,” says Gill.

There is also collusion with suppliers, whereby invoices are inflated for the benefit of both parties. Expenses fraud is also escalating, they tend to be around the \$10,000 or \$15,000 mark but there have been cases of up to \$1 million.

Ingram at PwC says companies have become better focused on supplier fraud since the advent of the GFC. “They tended not be

looking at a process so closely when they were not concerned where every dollar was going, but now that they are cutting costs, they’re finding that suddenly find there is 1000 metres of concrete being delivered, not the 2000 metres they ordered,” he says.

Insurers even say that without good lines of access to report suspicions, a company will not be considered for fidelity insurance which covers corporates for internal fraud (see box below).

Monitoring

A recent development has been the growth of data analytics techniques and technology to monitor suspicious electronic transactions among thousands of pieces of information. Document-management systems are also becoming critical to support complex legal cases stemming from the misdeed.

Deloitte has its own proprietary system – Dtect, while KPMG has K-Trace. Ernst & Young has Oversight while PwC has its own analytics tool – and declines to give it a name.

All are constructed to analyse the million pieces of data in everyday business systems, such as comparing vendor master files to employee records. They can uncover real frauds as well as operational mistakes.

What kinds of things can they flag? You can run a comparison between accounts of employees on the payroll system against your vendor bank account numbers. If an employee has the same number, you know there’s a problem.

FRAUD INSURANCE

In the case of a small or medium-sized business whose cash flow may even at the best of times be precarious, a loss caused by fraud, even a relatively small one, can be fatal.

An all risks policy, even one that covers consequential loss, will be of no help. Consequential loss protects the insured against the knock-on effects of a serious event such as fire or flood but not fraud.

However, protection against fraud loss is possible and few businesses are aware of it, says Aon’s head of risk services, Shane Boyd.

Policies tend to come in two types. Fidelity guarantees cover dishonesty by

employees and can be extended to every employee. There is also third-party fraudulent loss cover.

These policies are rare, for two reasons. An insurance company would have to know a great deal about a business’s activities – perhaps more than the insurer’s client would like them to know.

To pay out, an insurer would need to be completely satisfied that the company had all the correct internal controls and the proper segregations between custody and authorisation. As well as this, a highly developed whistleblower system would need to be in place.

“Sometimes the insurance company takes the client at their word that they’ve done all these things. But then the insurer

finds that the client hadn’t and refuses the claim,” says Boyd.

A company will also have to show a rigorous audit trail after the fraud, providing detailed evidence of the loss.

Premiums will vary with circumstances, but in the case of a business whose activities place it at particular risk, they will be higher. Boyd says often there is an excess available. Premiums for a \$1 million policy will be less if the company pays the first \$100,000 fraud loss.

Fidelity insurance is developing. There are policies addressing things like identity fraud and fraudulent online transfers and payments. “There are even policies which will allow the policyholder to engage PR people to limit reputation damage,” he says.

You can look for duplicate payments – one legitimate, one false. They also look for round sum payments – very few invoices are for round sums. It's a good idea to have them checked, as well as any payments processed outside normal business hours.

Red flags

The tools cite a number of red flags that the technology is most likely to throw up, which includes things such as short-term changes to employee or supplier accounts.

Another giveaway that fraud may be occurring is the repeated structuring of transactions just under the delegated authority limit. Five payments of \$9,999 authorised by a staff member with the authority to approve costs up to \$10,000 would certainly be subject to close investigation in any organisation if detected.

A company can spend millions trying to get to the bottom of its problems, but huge frauds have been discovered quickly – and at low cost

“You might get an invoice number which is correct but a customer number on the invoice number which is incorrect,” says E&Y's Fontanot.

“Then you have to ask, is the right amount going to the right customer?”
“There may be round amounts paid on Sunday night. Instead of waiting for Monday, the system shouldn't process it until someone's looked at it.”

EFT risks

Transactions conducted directly through the electronic funds transfer system rather than the accounting system are also subject to scrutiny. Typically, instances of EFT fraud appear to be linked to issues involving access to computer log-ons and inappropriate use of passwords.

Is the cost worth it? A company can spend millions trying to get to the bottom of its problems, but huge frauds have been discovered quickly – and at low cost.

“We have known firms to spend as little as \$20,000 only to see the technology uncover multi-million dollar frauds,” says one forensic expert. ■

Fraud and AML/CTF Obligations

Reporting entities that experience external and internal fraud need to consider the anti-money laundering/counter-terrorism financing (AML/CTF) issues that these crimes present. Where the fraud involves movement of funds or value through the provision of designated services to the fraudster or his or her associates, then a reportable event has arisen under Section 41 of the AML/CTF Act.

IF THE FRAUD does not involve the provision of designated services, then there is no reportable obligation because the first required element in Section 41(1), namely that the reporting entity is providing a designated service or has been requested to provide a designated service, is absent.

Assuming that the fraud does involve a designated service, the reporting entity should then consider what other actions it should take, from enhanced customer due diligence all the way through to amendment of its ML/TF risk assessment and changes in monitoring controls for staff accounts.

Reporting entities may become aware of internal fraud involving their business customers which have utilised the designated services provided by the reporting entity. Such matters are reportable under Section 41 because a designated service has been provided and information that the reporting entity holds about the provision of the designated service may be relevant to the investigation of, or prosecution of, a person for an offence against a law of the Commonwealth or of a state or territory.

For example, an employee of a business customer of a bank may have transferred money from the business customer's account using internet banking facilities to their own account with a different bank. This fraud involved the supply of designated services (the transaction on the customer's account) and is thus reportable under Section 41. Frauds involving employee's bank accounts with their employer bank will give rise to Section 41 reporting obligations. Insider trading and market manipulation events may involve a range of reporting entities, and in addition to their obligations to the market regulators they also have Section 41 reporting obligations.

Reporting entities may become aware of a fraud involving a supplier. Depending on how the value has moved to perfect the fraud, there may have been provision of a designated service within the meaning of Section 6, giving rise to reporting obligations under Section 41.

The example in the accompanying article involving an employee of a superannuation provider is illustrative of the intricacy of these questions. If the provider was not a reporting entity, then the provider has no reporting obligations. Those that provided share acquisition services to the employee are likely to be providing designated services and, on learning of the employee's activities, would be subject to a reporting obligation under Section 41.

Payroll frauds will inevitably involve reporting entities preparing the payroll or providing payment services. So if a business customer of a bank discusses payroll fraud with its bank, a reporting obligation has arisen under Section 41.

External frauds perpetrated on reporting entities, for example phishing attacks, are also reportable under Section 41 because they meet the criteria in Section 41(1). Phishing attacks occur on legitimate accounts held by genuine account holders and, although they do not perpetrate the fraud, the designated service is the provision of an account to the genuine account holder. ■

UP CLOSE AND PROFESSIONAL WITH THE WEST

Peter Robinson

Operations Manager, Patersons Securities,
Perth, Western Australia

What are your professional background and qualifications?

I have a BSc in Computer Science and Electronic Engineering from the University of Birmingham in the United Kingdom. I emigrated to Australia in 1991 and worked as an IT Project Manager in the financial service sector up until 2005, latterly for Perth-based online securities broker JDV. In 2005, I made the move from Project Manager to Operations Manager for JDV. This also entailed taking on the position of Responsible Executive for the back-office side of the business, having first passed the necessary examination in accordance with the requirements of the ASX.

What is your role with Patersons Securities?

I joined Patersons Securities as Operations Manager in 2007 and I continue to hold that position with the firm. The Operations area is split into the following departments:

- scrip (stock) settlement;
- cash settlement;
- on-boarding of new clients;
- and
- our Accolade portfolio management service.

I am also the Anti-Money Laundering/Counter-Terrorism Financing Compliance Officer for the firm and have been involved with the AML/CTF implementation since I joined the firm.



Peter Robinson

We found that engaging an external person for the independent review was very useful

Where did you get your AML/CTF knowledge?

I had to teach myself most of what I know. Perth does not have access to many AML/CTF events or courses, so it was a question of reading my way in. We found that engaging an external person for the independent review was very useful, because

good position to monitor activity. On a daily basis, my AML/CTF involvement would consist of:

- answering identification-related questions posed by Client Advisers and their Dealer Assistants. This interaction often involves providing background in the regulatory and policy requirements, as well as providing ongoing training on Patersons' AML/CTF policy and procedures;

If our clients understood the reasons behind the requirements we have to impose on them, then we face less opposition from them in meeting those. It is difficult for a firm such as ours to be fulfilling that educative role

that helped clarify that we had proceeded in the right direction on most aspects of the implementation.

How well does the AML/CTF Compliance Officer fit with that role?

My role involves managing a number of key operation processes. Since AML/CTF requirements touch each of these, I am well placed to be able to design and implement operational responses embedded within our usual activities. Having been closely involved in the development of Patersons' AML/CTF policy and procedures, I was able to ensure that these were then integrated into the procedure manuals for each of departments described above.

How much of your day do you spend on AML/CTF?

I see myself as being one step back from the coalface in terms of the operation of our AML/CTF program, and this puts me in a

- responding to queries from Operations staff relating to the application of Patersons' AML/CTF policy and procedures. These would generally relate to less-common scenarios that only arise on the odd occasion;
- monitoring the on-boarding of new clients and other key AML/CTF processes;
- checking the output from our ongoing customer due diligence reports; and
- keeping up to date with AML/CTF-related press releases and notifications. This would take perhaps 15 to 20 percent of my time in any given day.

What would you change about the AML/CTF regime if you could?

If I was in AUSTRAC's shoes, I would undertake an education program aimed at improving wider community knowledge of the objectives and requirements of the AML/CTF Act. If our clients understood the reasons behind the requirements we have to impose on them, then we face less

opposition from them in meeting those. It is difficult for a firm such as ours to be fulfilling that educative role.

What do you think are the hardest things to manage in your AML/CTF program?

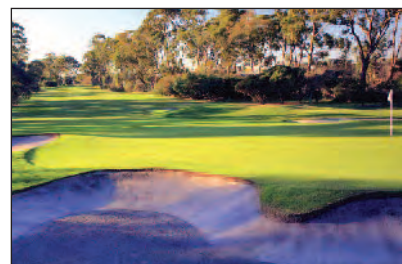
The wider community does not appreciate the rationale of the nature of the requirements imposed by the AML/CTF Act. This leads to some frustration among our client base and also frustration from their accountants and lawyers, who do not always understand the requirements.

What do you think are the easiest things to manage in your AML/CTF program?

The Patersons Operations staff who apply the procedures are well trained and are diligent in applying the procedures, so the internal quality of compliance is not an issue for me. Once the procedures are put in place, my experience is that we have a fairly smooth operation with procedures being followed. Of course, the challenge is to put the procedures in place in the first place which suit the business and the systems we have, and also meet the requirements.

In your spare time, what are your favourite things to do?

Two young children and a golfing addiction keep me busy. ■



Write to the Editor and tell us what is on your mind, and what questions you are working on in your AML/CTF Program.

Email: jgeary@afma.com.au

aml.
anti-money laundering
magazine





India and the **evolving, adaptable methods** of terrorist financing

by Dr Nick Ridley
Senior Lecturer in Policing and Security,
John Grieve Centre, Dept of Applied Social
Sciences, London Metropolitan University

In 1978, Paresh Baruah was given employment as a porter of Indian railway company North East Railways at Tinsuki railway station. In early 1980, Baruah absconded from the district and joined regional terrorist liberationist group the United Liberation Front of Asom (ULFA) and, as part of the group, committed numerous sabotage raids and killings of law enforcement officials in Assam. He is now one of the leaders of the ULFA and the subject of several Indian National Police wanted notices.

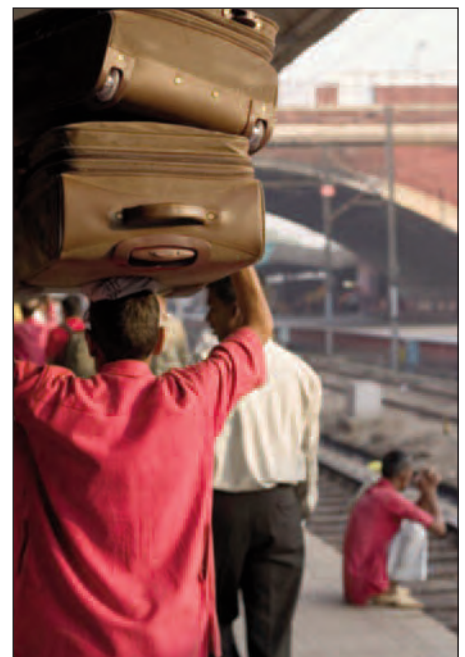
Nearly 20 years after he joined the group, in December 2009, it was discovered he was still officially employed by North East

Railways and payments were still being made to him. The Indian Railway Ministry then took action. According to an Indian railways spokesperson, he was summoned to an internal railway employment hearing, then:

"Two dates were fixed, first for a hearing and then, after two weeks when no one turned up to claim the post, Paresh Baruah was sacked as per government procedures."

The dismissal took effect from 8 January 2010.

However it is not only the Indian railways that are cumbersome and have to suffer a negligent bureaucracy. The Indian banking system is also an extensive network, in both urban and rural areas.



All large banks are nationalised and all financial institutions are in the public sector. However, despite the wide-reaching network over the subcontinent, banks have not outreached to a large part of the population. In 2007 it was estimated that between 60 percent and 70 percent of the Indian population did not participate in banking activity. Rather than traditional banks, many use the hawala and other underground banking systems, well out of sight of regulators. An estimated 60 percent to 70 percent of the Indian economy is therefore unofficial or underground.

Such unofficial methods of money transfer – because they are so widespread in legitimate and genuine use by such a large proportion of the population – are conducive to and exploited by terrorist groups based in and targeting India. India has a variety of such domestic and transnational terrorist groups.

Terrorism by liberationist struggle is conducive to high-profile attention because of the ease of popular comprehension. There is an identifiable geographical area of “liberationist” or disputed territory, usually equated with an ethnic minority. Ideological motivated terrorist groups tend to have less-tangible objectives. Compared to the Kashmiri liberation groups and the al-Qaeda affiliated groups, which are partially linked to elements of claimed territoriality, the Maoist groups operating in India have attracted less international attention.

Yet in one year, 2006, over one-quarter of all deaths from terrorist attacks in India were due to left-wing extremist groups. The main group is that of the Communist Party of India-Maoist (CPI-Maoist). All such groups espouse the ideology of Maoist communism, whose economic ideals have been adapted for the rural conditions and the interplay between urban conurbations and the countryside in India.

It is estimated that 14 states in India are significantly affected by Maoist groups. Nine states have sustained intense activity from the main group, the CPI Maoists: namely Andhra Pradesh, Bihar, Jharkhand, Orissa, West Bengal, Uttar Pradesh and Karnataka.

In 2008, the Indian Prime Minister said that the threat from extreme left groups was “the single largest internal security challenge to the Indian state”.

In August 2009, the Indian Home Affairs Minister, P. Chidambaram, publicly cautioned all states against losing focus about internal security, saying that the nation continues to face challenges from terrorism and Maoism.

Maoist rebels in February 2008 attacked a regional police station in Orissa state, killing all 17 officers and one civilian worker; in July 2009 killed in a single attack 27 police in the district of Raj Nandgaon, Chhattisgarh state; and in January 2010 an attack in Ghumla, Jharkhand state, killed six police officers and a police civilian worker.

Such unofficial methods of money transfer are conducive to and exploited by terrorist groups



In terms of financing, they have evolved systems, particularly in the rural areas from tradesmen and farmers of graded tributes – not always paid under duress, as they enjoy considerable local sympathies – and a system of moving monies through organised cash couriers.

This involves a network of trusted and paid individuals constantly on the move, and static individuals entrusted to store and hoard sums of monies. The latter, usually lower paid workers in the service sector or agricultural labourers, have revealed much ingenuity in methods of concealing the monies and have proven themselves scrupulously meticulous in clandestine record-keeping of the incoming and outgoing sums, the records being as detailed as they are coded.

The Maoist groups have also raised revenue, showing pragmatic adaptation by cashing on the change in post-2008 drug cultivation trends whereby marijuana cultivation has increased in the states of Andhra Pradesh, Madhya Pradesh and Chhattisgarh. In Andhra Pradesh, where police seizures have indicated to strategic analysts in 2009 an exponential growth in marijuana cultivation, the Maoist groups have acted as brokers and facilitators to the cultivators and purchasers by providing at comparatively modest fees (thereby maintaining their empathy with the local lower rural classes) guards and drug couriers for transporting the crop cultivation to the border regions for export.

In 2001, the Financial Action Task Force passed the eight (later nine) Special

Recommendations against terrorist financing. Some of them have fallen short in their practical implementation, including those under Special Recommendation VI dealing with international wire transfers. In operational intelligence terms, what is achieved is transaction frequency assessment and destination profiling, as opposed to full transaction analysis.

However, in 2009 Italian police, through tenacious investigations, identified transactions sent from a money transfer agency in Brescia, which eventually led to correspon-

ding sums paying for certain aspects of the December 2008 terrorist attacks in Mumbai. The funds were transmitted by several stages and via individuals in an EU jurisdiction. In investigative terms, it was a pragmatic advance in intelligence work in terrorist fund transfer by wire transfers. It was of additional significance of the extent and complexity – and international links – of the financing if terrorist groups in, and impacting upon, the Indian subcontinent.

In 2009, US Assistant Secretary of State Christopher Glaser, responsible in the US administration for combating the financing of terrorism, in an official visit to India spoke at an anti-terrorist conference. While he was fully supportive and positive of Indian efforts against terrorist financing, he discreetly noted the delay in such effort development, significantly concluding his address with the words:

“In conclusion, India is beginning to recognise the importance of counter-terrorist financing as a central component to the fight against terrorism.”

In the area of financing and financial services, the Indian subcontinent has engendered wide and diverse methods of moving sums of money. Such methods have been successfully adapted and exploited by differing terrorist groups based in and targeting India. A decade after 9/11 the full significance of these methods is becoming more apparent. For international efforts in anti-terrorist financing, there remains much to achieve to successfully counter them. ■



World-Check special crime and terrorism series:

illegal sports betting

By: BC Tan, Head of Organised Crime Research, World-Check

South Africa is racing to complete its preparations to host the 2010 FIFA World Cup in June, and more than 450,000 sports fans are expected to attend the event. While concerns about South Africa's high crime rates continue to be a talking point of the World Cup, the external criminal influences that plague major international sporting events must also be factored into its security planning and arrangement.

Bookmaking has always been a major income avenue for organised crime syndicates. While organised crime groups have significantly evolved and expanded their lucrative illicit activities in recent decades, illegal gambling operations remain one of the largest revenue components for most traditional organised crime groups.

To quantify how lucrative the illegal gambling industry is to organised crime, it is estimated that legal sports betting in the US constitutes a mere 1 percent of the sports betting market. As such, approximately \$US380 billion of illegal sports bets are made in the US each year. Based on these estimates by the 2005 National Gambling Impact Study Commission, approximately 92 percent of earnings from sports betting finds its way into the pockets of traditional organised crime groups.

The unfortunately reality of bookmaking and other lucrative illicit activities linked to organised crime is that they serve as a foundation to perpetuate other criminal activities. For instance, loan sharking, corruption and money laundering are key criminal activities intertwined with illegal gambling operations.

When criminal groups are able to secure this illicit income, it finances ventures into other criminal operations; further solidifying the continuity of these illicit organisations. The transnational nature of these organisations and their border-transcending operations pose a challenge to security planners and present severe risks to financial institutions.

How bookmaking operations work

Bookmaking is a complex operation in which organised crime elements participate at varying levels. The bookmaking operation could either be bankrolled by organised crime groups, directly operated by organised crime groups or portions of the operation outsourced to organised crime groups; or it could simply obtain security from organised crime groups through protection-fee arrangements. Either way, virtually no bookmaker can operate without financially benefiting an organised crime group for the privilege of conducting business. In operations not controlled by organised crime groups, independent bookmakers have been known to pay up to 50 percent of their profits in protection fees.

The reason behind the high level of organised crime involvement in bookmaking is simple – bookmaking requires substantial up-front capital. A decent-sized bookmaking operation has a capital requirement of at least \$600,000 and must maintain a healthy cash reserve of between \$500,000 and \$1 million dollars to be able to settle up losses. This cash-intensive requirement serves as a major barrier to entry.

Certain characteristics of illegal sports betting ensure its continued popularity. For one, illegal betting operators normally offer better odds than legal outlets. The underground nature of bookmaking means winnings are not reported or audited, and are therefore not taxable. Another key factor is that illegal betting operators normally extend generous credit to their clients. The credit extensions provided by bookmakers are a particularly important component of bookmaking operations that opens up for organised crime participation. At times, bookmakers may have to outsource debt collection to organised crime elements, which can either be compensated

through the protection-fee arrangement or obtain a cut of the debt interest. In many cases organised crime groups are directly involved in the loan-sharking business and extend the loans directly – at exuberant interest rates. Invariably, the threat of violence will be used to reclaim a debt.

The issue of match-fixing touches every sport at almost every level, and illegal betting syndicates are often the key external force seeking to influence match outcomes. As bookmakers profit only from the gamblers who lose rather than win, they find themselves in a position of substantially higher profit margins by betting against ideal odds.

Often match-fixing involves organised crime elements seeking a personal relationship with players, direct bribery, or simply the extortion of officials and players. The participation of organised crime elements in match-fixing is so prominent that an FBI special agent once said that “most of our major mob cases start out as gambling investigations”. One such example would be the case former National Basketball Association referee Tim Donaghy, who was convicted in 2005 for his part in influencing the outcome of numerous NBA matches. The discovery of his participation was actually the result of an investigation into a mob-operated bookmaking operation. Finally, in 2007, Donaghy publicly admitted his match-fixing was linked to a bookmaking operation associated with the Gambino crime family of Brooklyn.

With over \$148 billion placed on football bets annually, football in particular has a long and tainted history of corruption. In 2005, former German referee Robert Hoyzer confessed to an allegation of match-fixing. Unsurprisingly, investigation into Hoyzer’s match-fixing activities uncovered links to Croat organised crime elements. The outcome of the investigation identified at least five German Cup matches where Hoyzer either attempted to, or successfully managed to, influence the outcome. And also in 2005, Brazilian Edilson Pereira de Carvalho, who also happened to be on the FIFA referee staff, was found to have accepted bribes to influence over 11 matches. The Union of European Football Associations (UEFA) is currently investigating at least 40 alleged cases of match-fixing.

In 2007, UEFA issued a 96-page dossier addressed to Europol that identified 26 cases of high-profile European matches alleged to

have been influenced by Asian betting syndicates. However, organised crime syndicates’ involvement in match-fixing is actually a far more complex phenomenon. Often match-fixing incidents can involve multiple actors acting across borders. For example, there have been many occasions where non-European betting syndicates have been linked to match-fixing incidents in Europe.

Betting syndicates that operate out of Asia in particular have been singled out as key players in the international illegal sports betting industry. Specialists in this field say this is because in Asia it is common for bets to be uncapped (meaning bets are placed without any value limits), while this is much less the case in Europe. This equates to higher stakes in sports betting in Asia.

An expected 3 million football fans will arrive in South Africa during the World Cup and a cumulative total of 40 billion fans are

these illegal betting syndicates worldwide. In continuation to Operation Soga in 2007; in 2008, Interpol coordinated another similar operation in Asia. At its completion, Operation Soga II successfully disrupted over 1000 illegal gambling operations estimated to have managed some \$1.5 billion in bets.

Conclusion

The 2010 World Cup will be the first FIFA event at which an early warning system will be implemented to monitor the games for anomalies and identify possible match-fixing. This system was tested during the 2006 World Cup in Germany and introduced to FIFA tournament matches in July 2007. Along with procedural changes – such as the FIFA code of ethics amended in 2006 that bars officials and players from participating in betting, gambling, lotteries and similar events or transactions connected with football matches – officials are taking no chances in



The 2010 World Cup will be the first FIFA event at which an early warning system will be implemented to monitor the games for anomalies and identify possible match-fixing

expected to follow the game through global telecasts. The transnational element of illegal sports betting poses a grave risk to global financial institutions because the operational requirement of illegal betting syndicates to move finances around the globe is usually done using the global financial system. Besides the obvious regulatory risks involved with illicit finances from illegal sports betting, these illicit finances are often linked to other criminal activities. In 2007, Interpol coordinated Operation Soga in cooperation with eight national law enforcement agencies in Asia that targeted illegal betting syndicates. A particular betting syndicate uncovered during this operation was one led by Tien Dung Ngo: a particularly successful betting syndicate that operated in Canada, Europe and Asia. Investigations revealed that, besides the lucrative betting operation that brought in an average of \$1.5 million per major international football game, the syndicate was involved in narcotics trafficking and laundering the proceeds from its criminal ventures.

As we get closer to the World Cup finals in South Africa, it will be expected that officials will step up their efforts in disrupting

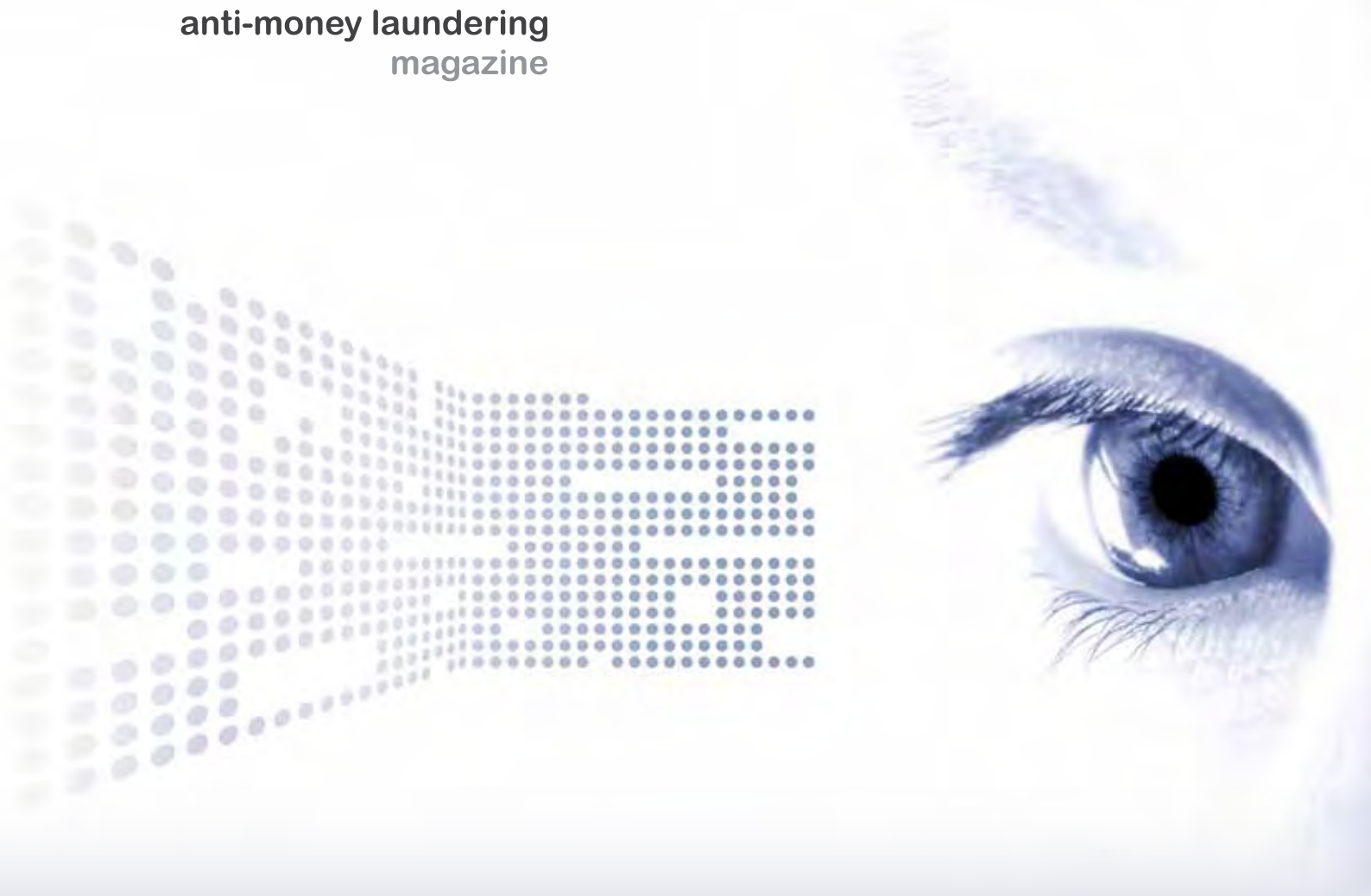
preventing the influences of illicit external forces and making certain that perpetrators will be identified.

During this period, financial institutions, foreign exchange houses, betting facilities and law enforcement agencies must install heightened controls to identify and prevent abuse by criminal elements in the movement and laundering of criminal proceeds during this period of increased liquidity and spike in cash based transactions. With the obvious increase of transactions involving betting placements that is to be expected during such massive international sporting events, the zero tolerance approach adopted by FIFA and law enforcement agencies will likely result in further identification and disruption of these transnational criminal syndicates. Financial institutions must take the highest precautions to ensure they do not risk their reputations by being associated in any manner with these criminal organisations. ■





anti-money laundering
magazine



SUBSCRIBE TO AML MAGAZINE TODAY!

SUBSCRIBE TODAY and gain access to the full version of Anti-Money Laundering Magazine.

Contact jsheil@amlmagazine.com.au for pricing and a subscription order form.

www.amlmagazine.com.au

Join the Anti-Money Laundering Magazine Experience!