Money Laundering bulletin

The monthly briefing service for anti-laundering specialists

Relative calm

No, amended possibly to less news is good news could be the motto of the anti-money laundering (AML) profession, and compliance more widely. Delegates to the UK Financial Services Authority's fifth annual Financial Crime conference on 24 April may have had the adage in mind after the closing remarks. The day began with the customary reiteration of how seriously the regulator takes money laundering but the point was not laboured – recognition, perhaps, that the financial services industry is on board – and best of all for MLROs, there was no foretaste of any major new initiatives, rulebook changes, or hints of enforcement action to come. The guns have swivelled to data security, which in many firms is lamentable as all the morning sessions and the regulator's latest paper on the subject [1] emphasised. Loss of customer data through weak controls poses the risk of identity theft, fraud and so laundering of the proceeds, which means it has relevance for MLROs, but unless they also happen to be the data protection officer and hold responsibility for physical and IT security, it is primarily someone else's headache.

The main money laundering slots in the day's agenda were given over to US speakers, who were unable to offer any firm view on where regulation there is headed except towards reform, though not in this election year. In 2006 a reaction had started against the tide of legislation and rules introduced after September 11th and to address the scandals on Wall Street, said Jonathan Polk, Vice President of Bank Supervision, Federal Reserve Bank of New York. The prospect of rolling back uncompetitive elements of the *Sarbanes-Oxley Act*, which imposes burdensome internal controls to insure against financial misstatement and applies to all entities with a US listing, and the *USA Patriot Act* is now remote as the credit crunch has swung the argument towards greater, or at least more effective regulation. The focus is on protecting US consumers from predatory lending and as far as AML provisions are concerned, the status quo will obtain, Polk believes.

Rick Small, Global AML Leader for GE Money, agreed that there probably would not be any major changes this year. Asked if the risk of enforcement action was a deterrent to firms acting in a transparent and open way with US regulators, Small thought not but he said that trust had been damaged by the publication of bank transactions by former Governor of New York Eliot Spitzer, who resigned after it emerged that he had used an escort service. "The belief is that this disclosure came from the Government side, there's no way a bank would have [released the information]."

Small and Polk thought that industry confusion and anxiety surrounding the enforcement notices issued by US authorities was understandable since

May 2008
Issue 153

IN THIS ISSUE

1 **Relative calm**
Financial Services Authority conference report

3 **Wheel spin on the French Riviera**
Monaco – jurisdiction profile

4 **Foreign affairs – a lead on sanctions**
Interview with Mark Daws, UK Head of AML Services, KPMG

6 **Melted down into dollars**
FATF Terrorist Financing paper

9 **Beside the dragon: Taiwan**

11 **Seeking new ways to destroy**
Emerging terror funding methods

14 **Secrets in Singapore**

16 **Grey areas**
Unresolved aspects of the Money Laundering Regulations 2007

Money Laundering Bulletin is now part of Financial Crime on i-law.com. We hope you enjoy reading Fraud Intelligence, Financial Regulation International, Compliance Monitor and Lloyd's Law reports: Financial Crime (online) as part of this service.

informa
law

they do not always reflect the original drivers behind the actions. The uncertainty works against the risk based approach (RBA), Small noted. Bank examiners will refer to notices when they visit an institution; the AML compliance officer will answer that he or she has read it but is not really sure what happened and would like clear instruction on how to avoid making the same mistakes. In March this year, Small canvassed an audience of 1,300 AML professionals on their attitude to the RBA; over half said "just give me the rule, tell me what to do." The response suggested a lack of education and communication between industry and supervisors on interpretation of the RBA, that it is not about penalising an institution for each and every minor infraction, he remarked.

There may even be scope to apply the RBA in terrorist financing, according to Paul Newham, who manages teams working at the UK National Terrorist Finance Investigation Unit (NTFIU). If it is known that target groups use specific funding routes, these could be given priority attention. Very few documents deal comprehensively with terrorist financing, he observed: the recent FATF paper [2], while useful in giving a macro view, is too general if one wants to know about regional and local trends. Newham proceeded to fill in some of the missing detail by looking at how the threat profile has evolved in the UK. In the 1990s money was moving both in and out of the country but since September 11th it is rare to see inbound flows. "The UK is a net exporter of terrorist finance; the majority of terrorist funds circulating here originate in the UK." The sums comprise both "legitimate donations [diverted to violent ends] and fraudulent revenue streams." A similar pattern is apparent in North America and Europe. The risk of attack in the UK remains high though, said Newham; the "foreign footprint" is clear in terms of inspiration and direction and he urged the financial sector to work to keep the environment hostile to terrorist financiers. Collected funds are predominantly sent eastwards, he added, again the same is true for the Continent and the US. Amounts originating in the UK are channelled to Iraq, Pakistan, Afghanistan, also to North Africa and groups in South East Asia. Where the local economy is cash-based, the favoured means of transfer is by courier. Although there is clear evidence that both formal and alternative remittance systems and front companies are used by terrorists, the abuse of charities is limited, according to Newham.

The values involved in terrorist funding are very small when set against the activities of organised crime and law enforcement have not come across more sophisticated trade finance-based schemes that professional launderers might exploit. Instead, all the cells discovered in the UK so far have been self-financing, "There has not been a domestic or foreign financier." The reason, said Newham, is the low cost of mounting an attack, which removes the need even to resort to fraud or other crime. The range for the costs of the 7 July 2005 bombings in London lies between UK£4,000 and UK£10,000 – the lower value counts only the outlay in the weeks immediately preceding the events, which covered renting the premises where the explosives were prepared and purchase of the precursor chemicals. The larger figure includes the additional elements like flights to Pakistan. A further risk of attack lies in radicalisation of people who start off as sympathisers, supplying material support, whether funds or equipment like satellite phones; it happens frequently. Sums raised in the UK normally fall between UK£20,000 and UK£50,000. "It might not sound much but goes a long way in Iraq and Pakistan, where rocket-propelled grenades sell for a few hundred dollars." If funds are gathered regularly they quickly mount up, "I would estimate that millions every year leave the UK in terms of terrorist finance," said Newham. The figures have grown in the last 12 to 18 months as the terrorists have begun to experiment with VAT fraud, account takeovers and commercial mortgage fraud. There is no discernible trend due to the fragmented and disparate nature of the funding networks. "Terrorist financiers operate on the periphery of organised crime, they are not in the higher echelons."

One point on which there will soon be clarity is the composition of the list of non-EEA jurisdictions that may be regarded as having AML regimes equivalent to the standard of the EU Third Money Laundering Directive. Jane Kennedy, the Financial Secretary to the Treasury, announced that the European Commission had agreed the classification in mid April and that publication should follow before long.

Notes

1. Available for download at www.fsa.gov.uk/pubs/other/data_security.pdf
2. Download from www.fatf-gafi.org/dataoecd/28/43/40285899.pdf

***Timon Molloy**, Editor*

Wheel spin on the French Riviera

Playground of the super-rich, Monaco found favour with the Council of Europe when it first evaluated the Principality's money laundering controls in 2002 but a follow-up assessment, published this February, reveals that it is unimpressed by the lack of progress in the intervening six years. ***Chris Jones*** *reports from Paris.*

Monaco's casinos conjure an image of glamour and sophistication, where dinner-jacketed James Bonds sip cocktails around the Chemin de Fer table and where fortunes can be made, or lost, with just the turn of a card. For most visitors to the Principality's five casinos – Monte Carlo Casino, Café de Paris Casino, Sun Casino, Bay Casino and Summer Casino – the stakes are unlikely to be very high – a little holiday money spent at the roulette table or in the slot machines. But a small number of the gamblers gracing the tables are there for much less innocent reasons. For Monaco's reputation as a place that prefers hard cash to hard questions makes it a potential magnet for money launderers – and the casinos provide the ideal means to clean their 'dirty' money.

This other image of Monaco is clearly not one that the Principality's government, or the Société des Bains de Mer (SBM) – the company that owns the casinos – are keen to encourage. As a result, both have been eager to make visible efforts to show that they are committed to the fight against money laundering through the casino network.

Monaco acceded to the Council of Europe convention on money laundering in May 2002 – an indication, perhaps, of how the world was no longer prepared to turn a blind eye to allegations of money laundering in the Principality after the terrorist attacks of 11 September 2001. A detailed assessment by the Council of Europe's select committee of experts on the evaluation of anti-money laundering measures (the MONEYVAL committee) of the Principality's anti-money laundering (AML) measures at that time followed and it suggested that far from being a haven for black market activities, Monaco already had an "extensive and thorough regime" in place. Nonetheless, comparing Monegasque policies and legislation with international AML standards, it stressed that there were still numerous areas where improvements could be made.

The committee's latest evaluation by the Strasbourg-based body has just been published (in February) and notes that "several changes to the legislation and regulations to supplement the Principality's anti-money laundering system" have indeed been made since 2002. These include "amending the provision of the Criminal Code criminalising money laundering, introducing additional customer identification measures, adopting new legislation regulating electronic transfers, relations with politically exposed persons and the activity of correspondent banks, and ratifying a number of international conventions."

But the government of His Most Serene Highness Albert II could still do better: "The legal provisions are [still] not very detailed or otherwise supplemented by more precise secondary legislation or instructions," according to the report, adding that this is evident from the lack of concrete progress since 2002. "Since the last evaluation, there was only one final conviction and 24 cases were pending investigation."

As for the specific measures in place in casinos, MONEYVAL's experts were for the most part happy. "Monegasque casinos are all subject to the Principality's anti-money laundering laws, and it should be noted that the frequency of controls carried out in casinos by [financial regulator Service d'Information et de Contrôle sur les Circuits Financiers] SICCFIN (two in the last three years) is far higher than the number carried out on other financial or legal institutions covered by the laws," the report says. "The controls carried out by SICCFIN complement those already undertaken by the Service du Contrôle des Jeux", the Monegasque gambling regulator.

But the assessors bemoaned the fact that in Monaco, "law enforcement activities are primarily reactive and the police and prosecution service do not appear to conduct proactive inquiries on money laundering offences". They also rued the lack of specific rules obliging casinos to check whether their clients were acting for themselves or a third party - or indeed to identify who that third party might be – a loophole that needed to be closed. Casinos should "be obliged to implement measures that would allow them to tell which of their clients were politically connected and to ensure that these clients are monitored," the report adds.

The sanctions against financial institutions found guilty of money laundering in the Principality are not applicable to casinos, the assessors noted. Casinos can only be sanctioned for failing to notify suspect transactions – and they are under no obligation to do that if no transaction actually took place (either because the casino refused to carry it out or because it failed to be completed, for whatever reason). In

addition, employees, not the casino, are considered responsible for any failure to notify a suspect transaction, effectively keeping the casino management (SBM, whose main shareholder is the Monegasque state) free from any risk.

Monaco government spokesman Jean-Pierre Doria said that there was nothing improper about the state holding such a large stake in the casino, and that there was no risk of anti-money laundering measures not being carried out effectively as a result. "On the contrary, the presence of the state as a shareholder guarantees that the activity of the Monegasque casinos is closely scrutinised, and ensures that the casinos cannot be taken over by companies or individuals of suspect intentions," he said.

The MONEYVAL report also notes that there are no rules in place obliging individual staff members within the casinos to watch for suspect transactions; nor are there any requirements to maintain a permanent staff responsible for verifying suspect transactions or even to ensure that staff are properly trained in how to spot such transactions. And provided they have a valid work permit, anyone can apply to work at one of the casinos, which are not obliged to carry out any further enquiries into the integrity of their staff.

Mr Doria stressed, however, that "the various control measures examined by the assessors highlighted no particular shortcomings in the current system of training for casino staff" – simply that there was no legal requirement on casinos to carry out such training.

On the positive side, the report also notes that there are monthly reports drawn up by the Service du Contrôle des Jeux detailing cash transactions in the casinos, which allow SICCFIN to keep track of any potentially suspect payments. All visitors to the casinos are clearly identified using passports or other identification, the report says, but recommendations that all clients buying or exchanging chips worth more than €1,000 should be subject to further identity checks have been ignored by the Monegasque casinos, which set this limit at €3,000.

The spokesman said that the Monegasque government had "heard" the recommendations of the MONEYVAL committee and was "preparing a new piece of legislation that would amend the current rules to take these recommendations into account". But, he said, it should be noted that many of the recommended actions "are already taking place, even if they are not expressly required by law."

The next assessment of Monaco's AML measures is due to take place in 2009, when the Principality's authorities will present the MONEYVAL committee with an update on how they have implemented the recommendations of 2007. Given the relatively minor progress between 2002 and 2007, the Council of Europe assessors will no doubt hope to see more legal certainty in the way in which Monaco's casinos are regulated.

Foreign affairs – a lead on sanctions

The oak-panelled reserve of a dining room which offers tables set in booths to avoid the chance that conversations might be overheard - reputedly favoured by the secret service – and an excellent menu, made Simpson's-in-the-Strand a natural choice when MLB editor Timon Molloy met with ***Mark Daws****, UK Head of AML Services, and a director in the Forensic team at KPMG, to discuss the current challenges facing anti-money laundering professionals.*

While we waited for the first course, I took the opportunity to ask about the structure of the AML group at KPMG. The core team in the UK comprises 15 to 20 specialists, who "work on AML day in, day out," said Daws. This team also draws upon a deep pool of AML expertise across the global network of KPMG where clients have extensive cross-border operations. One problem is finding people with the necessary skills, "It's a recruitment headache, actually." There is a need to understand the operation of the newer industries that are now part of the regulated sector but also to know how the various sanctions regimes apply. It is an extremely complex area which invariably falls in the AML remit. "I believe that sanctions compliance is a separate job in its own right," said Daws, although it must fit into the anti-money laundering framework, he believes, when there are "so many touch-points", for example, at customer take-on the prospect already has to be screened against both sanctions and Politically Exposed Person (PEP) lists. The subtleties of the sanctions programmes, notably under the US Office of Foreign Assets Control (OFAC), call for specialist training. Screening for a target entity or individual appearing on a list brings its own pitfalls around name matching but still further thought and interpretation are needed when assessing the legality of transactions into a designated jurisdiction: a product or service that

it is permissible to sell to one country may be banned from delivery to another territory.

Although there is strictly a "binary obligation", said Daws, that no payments should be made to persons appearing on a sanctions list, it is possible, theoretically, to design systems that risk assess the strength of the match and the exposure of operations to sanction risks . "It's a question of looking at the individual operation: if it is highly unlikely that a domestic-focused business would make a payment to a targeted party, the decision might be taken that investment in technology is not warranted but that staff will be given extra training in identifying high risk transactions instead. To achieve the right balance between the criminal liability for a sanctions breach and the risk based approach calls for a certain "intelligent ingenuity", Daws acknowledged. In practice, the net result is a big batch of potential hits, which must be examined to determine if they are real matches on proscribed entities or not. Typically, firms will deploy several review teams. Staff in the first may not be the most skilled but will be responsible from dividing the alerts into true and false positives. Those marked as accurate hits will be referred on to more experienced individuals, but this leaves the question of how to deal with the "closed out" cases. "Should they be subject to a secondary check? Some organisations outsource the initial screening to offshore cheap locations and send the output to highly-trained teams in the UK or elsewhere in the EU." Quality assurance on a sample of closed cases will reveal if they have been classified correctly.

In automatic payment filtering, an algorithm will segregate clean from the doubtful. There will always be a residual risk that some payments that should not be allowed will be passed. All the firm can do is ensure that the software is properly implemented and tested as well as conduct a periodic deep-dive inspection of some of the higher risk transactions. "It may be that the review identifies a small number of payments to countries in the developing world where corruption is rife; these should be looked at more closely," said Daws. If it transpires that the software was configured incorrectly or malfunctioned, in the UK, HM Treasury, which is responsible for the sanctions regime, would have to be notified. Daws was confident that if the firm was able to show, in addition to effective installation and performance review, that the team working on the payments screening system was adequately skilled and resourced, that it analysed past transactions on a regular basis, notified the system vendor when any faults or detection capability gaps emerged in order to prevent repetition, and was able to indicate precisely which amounts had been paid, in breach, to which entities, then the UK authorities may recognise this as an involuntary breach

A lot of attention is being focused on the US sanction programme under OFAC. The major banks have teams whose sole job is to deal with technical queries around sanctions application, Daws noted. The institution might dictate an overarching policy that says under no circumstances should any business be conducted with a particular jurisdiction but there will always be the exceptional case that calls for a waiver. "The team will need to know exactly what the rules are for dealing with, say, Cuba, Iran, Sudan and Burma. But even after looking at the payment – the economic purpose and dynamic behind it – and talking to the relationship manager, there may still be an element of ambiguity, which will mean discussion with in-house or perhaps even external legal counsel."

People working on sanctions often have a background in compliance, he noted; they also need to have a sound knowledge of the business. "There is a parallel with those who work on transaction monitoring. They need to combine understanding of the institution's products with an appreciation of money laundering typologies and the ability to exercise judgement when presented with a report."

Over coffee the conversation turned to other AML priorities. PEPs are a concern for clients, said Daws, but they are "not all equal. It's a bit like the first-year philosophy question, 'If all corrupt individuals are PEPs, are all PEPs corrupt?' Of course the answer is no but there is a tendency amongst some consultants and practitioners to make this assumption." It was right, he thought, that back in 2003 FATF should concentrate on ways to prevent embezzlement from national treasuries, or "grand corruption" as the US term it, but the journey since then had turned into a "rather tedious" debate over definition. "At the end of the day, it's all about identifying individuals who are high risk for the organisation. Yes, it is important to look at the class of persons classified as PEPs because they represent a particular type of risk but if someone happens to fall just outside the neat definition it does not mean the firm should not put in procedures to mitigate that risk." Some banks do not make a distinction between foreign and domestic PEPs at account opening, Daws noted, but then vary the enhanced due diligence and ongoing monitoring according to the perceived risk.

Identifying terrorist financiers is a very different problem but Daws was reasonably optimistic that the industry response need not be purely reactive, based on tracking the audit trail after an attack. "We'll make

progress as we understand more about the dynamics of terrorism, how different terrorist cells gain funding and the possible patterns of behaviour." Advances in knowledge will depend on analysis of both transactional and behavioural data on individuals. Insurance companies are already experimenting with similar modelling when looking at claims fraud: by examining socio-economic data they are able to assess the exposure by postcode and customer type. Despite the security imperative in countering terrorist finance, issues remain about intelligence sharing between the public and private sectors. "Should institutions pool all their transaction and behavioural data in a central utility for screening by some 'super agency' or continue to work in silos, all the while improving their own tools?" The civil liberties implications have yet to be addressed.

The next twelve months will also be characterised by increased focus on bribery and corruption as the US authorities make increasing use of powers under the *Foreign and Corrupt Practices Act*. Decisions about whether a putative transaction will fall foul of corruption legislation often falls on the MLRO's desk, "Should it be their call? In many respects no but it is, probably on the basis that if a bribe is detected a SAR may have to be filed." There is also a perceived high degree of commonality between the tasks involved in AML and combating corruption, both, for example, require customer due diligence and finding out who lies behind counterparties.

AML is rapidly coming of age, Daws observed. "In the old days it was just about ticking boxes but there is a new professionalism which means it can hold itself equal to other the risk disciplines – credit and market." The risk based approach has helped by providing a clear methodology that can command respect at the same time as coherent management structures are taking shape: fraud, money laundering and perhaps market abuse may well report into a director of financial crime, "It is recognisably a risk department in its own right. But it's very much a developing area. You won't find the need for a Financial Crime Officer (FCO) mentioned in the Money Laundering Regulations but the Joint Money Laundering Steering Group Guidance does refer to the benefits to be derived from a holistic approach to financial crime, and increasingly the FCO is being viewed as a board position." There is no clear-cut answer to whether firms should merge their fraud and AML teams but Daws reflected that the skillset needed to identify incidence of fraud and then perform follow up investigations is not the same as the qualifications for money laundering control. Some banks have pulled their operations together into one function but have not necessarily integrated the teams; the AML and fraud teams use their own software systems – often fraud detection tools have been in place long before the advent of AML packages - and report in to different senior managers, who, in turn, answer to the FCO. "The critical component," Daws added, "is the extent of senior management oversight, responsibility and drive."

The coffee finished, we emerged into the street to head back to our offices, "AML is a fascinating business," said Daws in parting, "mixing international law and regulation, foreign affairs, technology, not to mention criminal psychology, and it never stands still. Frustrating at times, it maybe but for a worthwhile, stimulating line of work, it's hard to beat."

Mark Daws *may be contacted on tel: +44 (0) 20 7694 5137; email: mark.daws@kpmg.co.uk*

Melted down into dollars

As regular readers will know, writes ***Sue Grossey****, I like to top and tail my articles with pertinent quotations, but it's proving rather (but perhaps not surprisingly) difficult to source light-hearted witticisms on the subject of terrorist financing. What I do find interesting is that, like most human endeavours, no matter how lofty and idealistic, terrorism still needs money to succeed. Or, as Charles Dickens wrote when his hero Martin Chuzzlewit arrived in New York and saw the hard-working Americans: "Dollars! All their cares, hopes, joys, affections, virtues and associations seemed to be melted down into dollars."*

When it first set up shop in 1990, the Financial Action Task Force (FATF) undertook to produce two major documents each year: an annual report, and a typologies report. Perhaps because no-one ever quite understood the word "typologies", this latter document was superseded in 2006 by specific subject-based reports. And the latest of these was published on 29 February 2008: a 37-page report entitled simply *Terrorist Financing*. [1]

Ever since the 9/11 attacks promoted terrorist financing to headline status, I have been concerned at the way governments around the world have forced it into close proximity with money laundering – as in the dreaded phrase "AML/CFT" (or occasionally, for variety, "AML/CTF"). I recognise that criminals who

are trying to hide their illegal proceeds and terrorists who are trying to get their money to where they need to spend it have certain features in common, in that neither group wants to draw attention to its members or its money. But to my mind, the differences between them are far greater than the similarities, and I am concerned on behalf of the regulated sector that these differences are frequently overlooked.

I see two major differences between them. Firstly, money laundering always involves the proceeds of crime, whereas terrorist financing frequently involves money that has been legitimately earned and willingly donated. And secondly, money laundering involves very large amounts of money, while terrorist financing is often so small as to be imperceptible (figures issued by the UK's National Terrorist Financial Intelligence Unit suggest that the London bombings in July 2007 cost a mere UK£7,420 to perform). And why am I concerned on behalf of the regulated sector? I am worried that if the public thinks that money laundering and terrorist financing are the same, they will expect the regulated sector to be able to detect and report them both – and current systems within the regulated sector will struggle to pick up small movements of non-criminal money. And when there is another terrorist attack (as there will be), and it turns out that financing was involved (as it will be), blame for the movement of that money will fall on the regulated sector. I long for the day when legislators realise that the two issues – although related – do not belong together, and produce two sets of requirements for the regulated sector, differentiating between what can reasonably be expected to counter the two threats. And so I was agog to see what this latest report from the FATF – titled as it was with just the one issue – would say on the subject.

How they use it

The first three sections of the FATF report deal with the ways terrorists use funds, raise funds and move funds. The section on the use of funds makes the very valid point that terrorists need money not just to launch attacks (the headline issue), but also to maintain their organisations: "Funds are required to promote a militant ideology, pay operatives and their families, arrange for travel, train new members, forge documents, pay bribes, acquire weapons, and stage attacks. Often, a variety of higher-cost services, including propaganda and ostensibly legitimate social or charitable activities are needed to provide a veil of legitimacy for organisations that promote their objectives through terrorism." A distinction is therefore made between the costs of "direct operational support" (ie, attacks) and those of "broad organisational requirements". The former will include vehicles, bombs, subsistence for terror cells, travel and training. The latter will include longer-term expenses, such as promotion of terrorist ideals through charities (particularly, as the report comments, "in high-risk areas and/or under-developed parts of the world where the welfare provision available from the state is limited or non-existent") or the mass media (eg, the production of videos promoting the cause).

How they make it

Terrorists use a wide variety of means to raise funds: "In general, terrorist organisations may raise funds through: legitimate sources, including through abuse of charitable entities or legitimate businesses and self-financing, criminal activity, state sponsors and activities in failed states and other safe havens…. These sources of terrorist financing can be divided into two general types: financing *from above*, in which large-scale financial support is aggregated centrally by states, companies, charities or permissive financial institutions; and financing *from below*, in which terrorists fundraising is small-scale and dispersed, for example based on self-financing by the terrorists themselves using employment or welfare payments."

With regard to the raising of funds from legitimate sources, the report uses a term that I have not seen before: black-washing, "where legal funds, for example money stemming from collection by charities or governmental subsidies and social benefits, are diverted for purposes of radicalisation, recruitment or terrorism". This is in contrast, I suppose, to the "whitewashing" of money laundering.

The abuse of charities in particular is of ongoing concern to the FATF, which – in its paper *Combating the Abuse of Non-Profit Organisations: International Best Practices* [2] published in October 2002 – noted that "the misuse of non-profit organisations for the financing of terrorism is coming to be recognised as a crucial weak point in the global struggle to stop such funding at its source". As to why terrorists target charities to assist in their fundraising, the report suggests several reasons: "[Charities] enjoy the public trust, have access to considerable sources of funds, and their activities are often cash-intensive. Furthermore, some charities have a

global presence that provides a framework for national and international operations and financial transactions, often in or near areas most exposed to terrorist activity. Finally, charities are subject to significantly lighter regulatory requirements than financial institutions or publicly-held corporate entities."

Although terrorists try to use legitimate funds whenever they can (in order to minimise the likelihood of detection and disruption), they do sometimes turn to "alternative sources of financing, including criminal activities such as arms trafficking, kidnap-for-ransom, extortion, racketeering and drug trafficking". As terror organisations have lost "state sponsorship", they have turned to drug trafficking in particular as a good source of income, taking advantage (as do criminal groups) of "the internationalisation of communications and banking systems". In fact, as the report notes, "investigations and intelligence have revealed direct links between various terrorist and drug trafficking organisations that frequently work together out of necessity or convenience and mutual benefit." For example, an investigation in the Netherlands revealed that an organisation involved in importing cocaine from South America to Europe was sending money to Paraguay and Brazil to buy supplies of drugs, and then wiring profits from sales to accounts in Lebanon, where they are suspected to have gone to a terrorist organisation. And in Costa Rica, nine people were arrested for involvement in a conspiracy to exchange cocaine and cash for US$25 million of weapons – their weapons broker was arrested in the US.

Credit card and cheque fraud are popular crimes for terrorists, as they are lucrative, hard to detect and difficult to prosecute, and carry low penalties. As the report comments, terrorists sometimes go back to basics to raise money from old-fashioned frauds: "Bank accounts [are] opened using false identity documents and fraudulent deposits. Cheque books are then stockpiled; and when a large number have been accumulated, they are used to purchase goods from department stores costing under the amount that would trigger verification to ensure sufficient funds were available in the account. The goods are returned for a cash refund. This activity can be carried out by organised individuals, who draw on cheques from the same account simultaneously in several locations."

A rather distasteful way in which funds can be raised is through extortion: "Supporters of terrorist and paramilitary groups exploit their presence within expatriate or diaspora communities to raise funds through extortion. A terrorist organisation would make use of its contacts to tax the diaspora on their earnings and savings. The extortion is generally targeted against their own communities where there is a high level of fear of retribution should anyone report anything to the authorities. They may also threaten harm to the relatives – located in the country of origin – of the victim, further frustrating any law enforcement action."

Finally, the report expresses concern about "safe havens, failed states and state sponsors", which "create enabling environments or otherwise provide support to terrorist organisations", notably in Somalia, Iraq and on the Pakistan-Afghanistan border.

How they move it

The report concentrates on the three main ways in which terrorist organisations move their money: use of the financial system; through the international trade system; and the physical movement of cash. The first is probably of most direct relevance to readers of this article, particularly the use of wire transfers: "Money and value transfer mechanisms have proven to be particularly attractive to terrorists for funding their activities… [ranging] from the large-scale and regulated funds transfer mechanisms available in the formal financial sector, to small-scale alternative remittance systems…. It was the use of wire transfers that the FATF was addressing when it issued Special Recommendation VII in October 2001 which requires that full originator information accompany any such transfer."

The use of the international trade system was explored more fully in another FATF paper: *Trade Based Money Laundering* [3], published in June 2006 (and reviewed in *MLB* Oct 2006). And improved safeguards in the financial system have forced terrorist organisations to revert to "traditional" smuggling methods: "The physical movement of cash is one way terrorists can move funds without encountering the AML/CFT safeguards established in financial institutions…. Some groups [convert] cash into high-value and hard-to-trace commodities such as gold or precious stones in order to move assets outside of the financial system…. As legitimate financial institutions tighten their due diligence practices, [cash smuggling] has become an attractive method of transferring funds without leaving an audit trail."

What we are doing about it

The final section of the report deals with the international response to terrorist financing, noting that several of the FATF's own Special

Recommendations have been issued specifically to counter the threat of terrorist financing: SRIII (Freezing and confiscating terrorist assets); SRVII (Wire transfers); SRVIII (Non-profit organisations); and SRIX (Cash couriers).

The report comments that "Financial information – including that gathered from suspicious transaction reporting – has a central role in identifying terrorist financing and the movement of terrorist funds through the financial system". However, it is recognised that "financial information alone may not be sufficient to identify terrorist financing activity. However, when combined [usually by the Financial Intelligence Unit] with counter-terrorist intelligence drawn from surveillance of the range of terrorist activities and networks, financial information can be leveraged to provide financial institutions with a concrete indication of possible terrorist activity, whether these use legitimate or criminal sources of funds."

This is a useful and timely report, mainly because it draws together in digestible form information on all aspects of terrorist financing, covering both characteristics and responses. As always, the conclusion is that much depends on the effective sharing of information between concerned parties, ie, private sector, public sector and law enforcement. In particular, information submitted by the financial sector through SARs can be of great assistance: "Financial information is now used as part of the evidential case to hold criminals and terrorists to account. It also has a key intelligence role – for example by allowing law enforcement to: look backwards, by piecing together how a criminal or terrorist conspiracy was developed and the timelines involved; look sideways, by identifying or confirming associations between individuals and activities linked to conspiracies, even if overseas – often opening up new avenues for enquiry; and look forwards, by identifying the warning signs of criminal or terrorist activity in preparation." Terrorist financing – although not the same as money laundering – is a threat to the stability of our financial systems and societies, and steps must be taken to understand and disrupt it before it can be used for its intended purpose. As Mr Burns, lovable corporate tyrant in *The Simpsons*, once said: "What good is money if it can't inspire terror in your fellow man?"

Notes

1. Download report from http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf
2. Download from http://www.fatf-gafi.org/dataoecd/53/53/34260889.pdf
3. Download from http://www.fatf-gafi.org/dataoecd/60/25/37038272.pdf

Sue Grossey *may be contacted on tel: +44 (0)1223 563636; email susan@thinkingaboutcrime.com*

Beside the dragon: Taiwan

In the April 2008 issue, Sue Grossey examined the Asia/Pacific Group on Money Laundering's (APGML) January/February 2007 assessment of the Taipei AML regime. Here, ***Dominique Patton****, who is based in Beijing, discovers more about the challenges which the jurisdiction faces by talking to local practitioners.*

Although Taiwan's tense relations with China do not improve cooperation with the mainland that would help bring some of the island's biggest economic criminals to book, it is nonetheless eager to work with international authorities to fight money laundering.

The country is a founding member of the Asia-Pacific Group on Money Laundering (APGML) and also part of the Egmont group of financial intelligence units (FIUs). Talking to *MLB*, Arthur Shay, partner at Shay & Partners, a law firm in the capital Taipei, underlined the fact that the Taiwanese Ministry of Justice has been "very active" in international forums.

William Bryson, head of banking and finance at global law firm Jones Day in Taipei, agrees: "Taiwan is not a member of international organisations like the United Nations but the government has always attempted to comply with international guidelines to show that they're a good citizen. It's part of their appeal to the world."

In June 2007 Taiwan amended its *Money Laundering Control Act 1997* (MLCA) – to bring its laws into line with recent recommendations from the Financial Action Task Force (FATF). The most significant amendment, according to Mike C J Lan, senior special agent at Taiwan's FIU, its Money Laundering Prevention Centre (MLPC), is a new clause criminalising the financing of terrorism.

Taiwan had drafted a counter-terrorism bill but had difficulties passing the legislation, said Lan. Instead it

has included a paragraph in the MLCA (paragraph 3, article 11), stating that anyone found financing terrorist activity that is acknowledged or kept track of by an international anti-money laundering organization will be imprisoned for between one to seven years and can be fined up to NT$10 million (US$330,000). A principle of reciprocity was also written into the Act, allowing Taipei's AML forces to inform foreign authorities of the results of their money laundering investigations even if there are no agreements between Taiwan and those authorities.

Such amendments were a condition of Taiwan's membership in the APGML, according to Nigel Morris-Cotterill, head of the Anti-Money Laundering Network based in Malaysia. And furthermore, it is another sign of the island's good intentions when it comes to AML terms: Taiwan does not have a real problem with terrorist financing and is not a 'hotspot' for money laundering, he says. "It doesn't come across the radar as being of particular concern. It's much more open than Korea or Japan, and more plugged into the international world." Others agree. "The currency is not completely convertible so not the most convenient for laundering anyway," said Bryson. A bigger issue is the domestic laundering of money. "Most of the money laundering is likely taking place domestically with the proceeds of corruption," said Morris-Cotterill.

In 2006 the bulk of Taiwanese money laundering prosecutions came from economic crime investigations relating to amounts of less than US$30,000, according to an APGML mutual evaluation published in July last year. It said Taiwan has "generally comprehensive" measures ensuring its financial institutions report and act upon suspicious transactions but that many are only in the form of guidelines.

"The regime is relatively simple," explained Bryson. "It's a system where financial institutions are expected to make their own determinations about suspicious transactions." Financial institutions are generally complying with the transaction and customer record-keeping measures, according to the APGML. But Bryson said that Taiwan-based US banks are likely to be over-reporting (because they also have to comply with American regulations) while others probably use more discretion. "I would imagine that there's not as much uniformity in reporting as there should be."

Under the MLCA, Taiwan's threshold for large cash transactions that must be covered by customer due diligence is higher than in most countries at NT$1 million (US$33,000). The APGML report also noted that Taiwanese "record-keeping requirements for non-cash transactions [are] inadequate and there are no requirements for those outside banking to monitor large or suspicious transactions." In fact, jewellery retailers are required to monitor suspicious transactions too but while government authorities have asked real estate brokers, land registries and others in the property sector to take steps to prevent money laundering, the measures are not mandatory.

Taiwan's anti-money laundering forces suffer from lack of manpower and training, the APGML found. James Wu, a former counter-intelligence supervisor, agreed that "we still need more well-trained law enforcement elites to fight such crime. The MLPC only has 27 agents and really needs more." That said, Mike Lan stressed justice minister Shih Mao-lin had recently made public announcements about the need to focus on the proceeds of crime, money laundering and asset forfeiture and has organised two training seminars next month for frontline prosecutors in Taiwan.

Another area of "significant weakness" is cross-border currency movements, according to the APGML. "There is a need to review sanctions for non-declaration and the smuggling of cash," it concluded. Lan said the government in Taipei is trying to shake up surveillance of cross-border cash smuggling but that customs manpower is "limited". More than 3,900 people work for customs but only 130 are charged with checking cross-border currency movements. Cash smuggling and transfers of funds through other underground channels are "quite rampant" because of restrictions on currency exchange across the Taiwan Strait and the absence of any cross-strait currency clearing mechanism, said Gary Hung, a junior partner with law firm Chien Yeh. Underground funds transfer between Taiwan and China was more than NT$77 billion (US$2.55 billion) from 2002-2006, according to official figures, said Hung. "Since it is difficult to track down the source of funds that are transferred through underground channels, criminals from Taiwan tend to use these channels to move their illicit wealth to China," he added. Wu said underground channels between Taiwan and the People's Republic of China are like "an expressway" for money launderers and mafia-type criminal organisations. This could increase as more people pass through offshore islands like Kinmen and Matsu: the Executive Yuan, or cabinet, decided recently to relax rules for Taiwan business people travelling to China by sea via the two islands.

Meanwhile, the MLPC plans to increase

information exchange with China, but is hampered by difficult relations with Beijing. "The MLPC has not had any formal information sharing with China. [It] is trying to set up cooperation channels with its counterpart [China] but is facing some impediments caused by political issues," said Lan. Wu agrees, saying "it is still hard to gain cooperation from the PRC (People's Republic of China] police." Taiwan's relations with China also make extradition of economic criminals virtually impossible. In one famous case, Beijing refused to repatriate Chen You-hao, the fugitive alleged to have embezzled about NT$800 million (US$26.6 million) from the Tuntex Group in 1995 and invested it in China. "It's a real problem," said one senior foreign lawyer in Taiwan, "The violent criminals get repatriated but white collar criminals don't."

Cooperation could improve if the incoming newly-elected Kuomintang (KMT) president Ma Ying-jeou carries out his pledge to improve relations with China. But if he proceeds with much debated financial reform, allowing more Taiwanese banks to open in China, money laundering may actually increase, claimed Shay and Wu. Already, the "hot money from Hong Kong is falling into Taiwan," said Shay, explaining that Taipei authorities have difficulty in tracing the sources. "It's becoming significant. There's a rumour in the market that officers in China that are corrupt transfer their illegal gains to Hong Kong and then to Taiwan."

Seeking new ways to destroy

Launderers are motivated to cover their tracks but with far more at stake the terrorist financier is continually looking for innovative means to disguise and move funds. ***Simon Dilloway****, formerly of the UK's National Terrorism Financial Investigation Unit, Metropolitan Police, distinguishes the methods adopted by groups who attack domestic and foreign targets before examining some of the emerging channels that are making life difficult for law enforcement.*

Terrorist finance, like money laundering, is an evolving phenomenon. As has been stated many times, there many similarities between the two activities, as well as some fundamental differences. The primary difference, of course, is the fact that all standard laundered money is dirty from the outset; it is the proceeds of crime of some description. However, while a proportion of terrorist money is undoubtedly proceeds of crime, a significant proportion of it is not actually dirty from the start, at least not on casual inspection.

I am referring to the very large sums of money that are donated by sympathisers, whether they be individuals, businesses, or even rogue states. The money is clean until such time that an intention is formed that it should be used for terrorist purposes. At that point, it becomes terrorist money as defined by the various acts of Parliament, but it does not immediately take on any other suspicious characteristics as it is moved through the system. The need to employ money laundering techniques only arises when it has to be moved to its destination, and used for whatever nefarious purpose is intended.

The other significant difference is in the amounts. While large amounts can be involved, so indeed can small amounts, which rarely happens in criminal laundering. This will be expanded upon below. As legal systems and the commercial world take a greater and greater interest in financial crime, so the means used by launderers and terrorists come under closer scrutiny. Ever resourceful, they naturally turn to more innovative methods of raising and moving their money to achieve their ends and to avoid detection. It is therefore of the utmost importance that everyone who has an interest in the prevention and detection of this activity, from governments, through law enforcement to companies and consumers, remains vigilant and open-minded, to spot the emerging methods and perhaps to second-guess the abuse of brand new methods.

Before we discuss the potential new methods of terrorist financing, it is first necessary to identify fully the extant typologies. Secondly, we should look at those methods that are emerging at the present time, those areas where there is evidence and intelligence to indicate that new methodologies are making use of innovative means to raise and move terrorist funds. Awareness of these changes will assist those charged with fighting terrorist funders, making it easier to actively seek out instances of potential terrorist activity. We should then highlight and discuss financial activities that might be exploited by terrorists.

By making new technologies and financing methods more difficult to abuse – so-called 'target-hardening – it may be possible to force the financiers to resort to already known methods that are much more likely to be detected, they might even be obliged to resort to

using cash couriers, an efficient but very high risk strategy. The message must therefore be that while identifying new means of terrorist financing should always be at the forefront of a successful counter terrorist financing (CTF) strategy, it is also important to ensure that tried and tested means of identifying illicit traffic are not neglected, either by the enforcers or the regulated sector, because in desperate times, terrorist financiers as well as money launderers will always seek the line of least resistance, and exploit the weaker or less regulated areas.

It is necessary first of all to break out the main features of the overall funding picture. Firstly, there is the 'travelling terrorist', those who go to foreign countries to perpetrate their acts of violence or sabotage; then the needs of the 'home grown' indigenous terrorist, who is planning to launch an attack against his or her fellow-citizens; and finally the funders of insurrection, those donating and sending money to areas of armed conflict where the main reason for the unrest relates to the cause they support.

The first category refers to the needs of such terrorists involved in attacks on the USA in September 2001, where hijacked aircraft were crashed into various sites including the World Trade Centre and the Pentagon. Those involved were not US residents, and had no ordinary means of support whilst engaged in the preparation for the attacks. They needed to enter the country, they required food and accommodation, and they needed to learn how to fly the aircraft.

Much is made of the relatively small sums necessary to commit these atrocities; however the best guess of around US$500,000, whilst small in comparison to the damage and loss of life caused, is still a substantial amount of money. This money had to be supplied by those organising the attacks, and it had to be transferred to the operatives who carried them out. The same is true of any group operating away from their country of residence.

The funding operation in 'domestic' attacks by residents is very different. For the purposes of illustration, consider the cost and funding of the attacks on London on the 7 July 2005. The perpetrators were all resident in the UK, one was a Jamaican-born UK citizen who had converted to Islam, and the other three were British born Muslims of Pakistani origin (first generation immigrants). They all had homes in the UK and all were either on social security benefits or had menial jobs. They were therefore able to function without external financial assistance.

The cost of the attacks was minimal in UK economic terms. The investigation concluded that the raw material for the attacks, including the bomb making equipment, cost no more than UK£2,500. Ancillary costs involved in the construction and deployment (car hire, rail tickets, rent and fuel), brought the sum up to around UK£4,600. The cost of international travel for two of the group for training and further radicalisation was around UK£1,800, and training and selection weekends in the UK no more than UK£825. The total required was therefore at most UK£7,235.

Funding such a sum in an affluent country was simple, even for those of a low socio-economic group and credit rating. The leader of the group obtained an unsecured loan of UK£10,000 from a high street bank in March 2004, and withdrew a total of around UK£4,000 in cash on credit cards during the next six months. In October 2004 he stopped all repayments. Efforts by the banks to reclaim the money took several months, and were not concluded by the time of the attacks. Whilst it is not known how much of that money was used to fund the attack, it can be seen that by this simple method almost twice as much as was required was raised with little effort.

The funding of armed conflict provides a different perspective on terrorist finance as far as investigators are concerned. In the first two examples, money was moved to, or raised in the country under attack. In this case, the money is raised in many ways and in many places, but predominantly flows from wealthy countries, largely in the West, to sites of conflict, often through countries with very poor records in AML/CFT regimes, such as some African states.

It is the case that all around the globe there exist populations of people originating from areas currently the subject of armed conflict. Afghanistan, Iraq and Palestine are the destination of funds from extremist Muslims worldwide. The sums largely comprise donations from people who are hostile to the country in which they live. Other examples, such as those fighting for a Sikh homeland in Khalistan, the Liberation Tigers of Tamil Eelam (Sri Lanka), and the PKK (Turkish Kurds) are somewhat different, in that they tend to be funded by people who have no quarrel with their host country but who are bound by racial, cultural and linguistic ties to the 'homeland'.

Methods of finance in these cases are often different, and can include extortion, blackmail, kidnap and ransom, as well as fraud, and of course donations from sympathisers. Businesses and charities are often used to disguise and facilitate the flow of funds, which are

transmitted through legitimate channels until they arrive at a jurisdiction of low security, where they then disappear into more traditional avenues of distribution.

General acquisitive crime, however, cannot be removed from the equation. It is known that low level fraud operations by various groups in the UK have produced significant amounts of funds for particular terrorist organisations. It is my opinion that, in general, affluent western countries are, for the most part, net exporters of terrorist finance to zones of conflict.

The enduring means of transporting money, and one which will, I am sure, continue, is the tried and tested carriage of cash by human 'mules', hidden in a myriad different ways. Whilst it is very effective, especially with the advent of the €500 note, it is very high risk, and detection means immediate loss of both funds and the courier, with concomitant risk of exposure of the wider network. Fundraising can be achieved by collections and donations, both of which are again traditional means of actually accumulating the funds, and underground banking of various descriptions is an ideal method of moving it to its final destination, despite the fact that it is illegal in most of its places of origin, such as India.

Crimes of violence are not a means used to any great degree by terrorists in the Western world to raise cash, probably because of the high profile and high risk of capture. Nevertheless it was always a mainstay of the Provisional IRA and other groups in Northern Ireland, and has been used by groups in Greece, as well as ETA in the Basque region.

As mentioned above, fraud is a favoured means of raising money by some groups, particularly those based in North Africa. Their method is to open many accounts by means of stolen identities, and run them normally for a period of time. They then use a variety of means to defraud the banks of relatively small sums per account, which are then funnelled out of the country as the 'account-holders' disappear, resulting in a large fund of money in aggregate. Defaults on loans, such as that described in the London attack, are an ideal means of fund-raising for the financier whose is going to disappear, such as a suicide bomber, while running up lines of credit for consumer goods by a fictitious company is another tried and tested means of obtaining illicit funds.

The following methods are evolving, in the sense that involvement in them by terrorists is either emerging or otherwise on the increase. Charities have proved to be especially vulnerable to abuse. Methods employed range from totally bogus charities, which take money from unsuspecting donors to divert to terrorism, to charities that are gradually subverted by trustees being brought in until the whole charity is controlled by terrorist groups, who can then use its reputation and financial channels to move funds unnoticed.

Innovative low-level fraud is illustrated in instances where two parties known to each other stage a 'car accident', following which several passengers claim for small injuries such as 'whiplash' neck injuries, and each receive several hundred pounds from the respective motor insurance companies. One such incident could easily raise sufficient cash to fund the London bombing of July 2005.

Internet auctions are another area where money can be moved around the world anonymously. For example, terrorist 'A' advertises an item for sale on say, eBay, which is then purchased by terrorist 'B' in another country. The money is passed from one to the other by conventional means, although no product changes hands or even exists. The money has therefore been successfully moved to its destination without suspicion, and is ostensibly clean. The relatively low amounts of money needed for terrorism make this a more worthwhile means for terrorists than perhaps for professional money launderers who need to handle much larger sums.

'eGold' is another internet phenomenon that is a great concern both in terms of AML and CFT. It is possible to buy, unregulated, shares of a stock of precious metal, which can be exchanged around the world, providing an effective and anonymous means of transferring funds.

The production and sale of counterfeit goods is a controversial area in respect of terrorist funding. It is certainly true that the Northern Irish Terrorist Groups used the sale of counterfeit DVD to fund their activities, but opinion is divided about the use of other counterfeits to finance terrorism. Given that in the UK, the counterfeit fashion industry, which accumulates millions of pounds annually, is predominantly in the hands of criminal operators from the subcontinent, it would not be unreasonable to assume that there may be a nexus with terrorists.

Lastly, there are new areas where I believe there are significant vulnerabilities that will almost certainly be exploited by traditional and terrorist criminals. In brief, mobile phone banking, a boon to poor countries with limited banking facilities, such as those in sub-Saharan Africa, provides yet another anonymous means of transferring cash. Value can be inserted onto a phone at a point of sale, and transferred to any other phone, whence it can be further moved, or cashed in.

Whatever the customer due diligence (CDD) efforts, who knows who has the phone at the other end?

Electronic purses, or stored-value cards, offer almost identical problems. Added to this, if low value is placed on the cards, limited CDD is required, but there is nothing to stop one purchasing many of them. It is also the case that in some jurisdictions they are not considered to be 'cash', despite holding value, and cannot therefore be subject of a seizure. Online gambling, a new but huge phenomenon, offers identical problems to the internet auction scenarios, with players deliberately losing to each other anonymously.

Finally, 'Second Life'; this is an on-line virtual reality world where one can do pretty much anything, including buying and selling property with the corporate money that can be purchased. Activity in this 'world' is constant and unmonitored, except for preventing inappropriate behaviour. Transactions involving movement of money between willing partners will never come to light, and the potential is easy to see. There is already evidence of the presence of known terrorist sympathisers on the site.

The new trends described above are just some of the potential means that innovative and open-minded criminals can exploit for their own ends. It is essential that legislators, regulators, entrepreneurs and security/law enforcement agencies apply a diligent and vigilant approach to AML/CFT security. There is now an excellent opportunity, whilst keeping firm control of the traditional systems, to examine each new technology and facility, and to think of the possibilities for abuse before they become fact.

Simon Dilloway *may be contacted on tel: +44 (0) 1379 687593 or tel: +44 (0)7815 300169; email: sdilloway@lophamconsultancy.co.uk; website: www.lophamconsultancy.co.uk*

Secrets in Singapore

Singapore may rank high in global anti-corruption tables but it has come under considerable fire recently for its strict bank secrecy laws. Last October, in the wake of the brutal crackdown on protests in Burma (Myanmar), the island state was also accused of serving as a money laundering hub for top junta officials. ***Dinah Gardner*** *examines whether the doubts are justified.*

Singapore rates as one of the least corrupt nations in the world – it comes fourth out of 180 countries in Transparency International's 2007 Corruption Perceptions Index. It has a strong legal framework, a low domestic crime rate and an efficient judiciary. Furthermore, the Monetary Authority of Singapore (MAS) has broad powers to check that financial institutions are complying with money laundering regulations. Singapore also has an established financial intelligence unit with strong guidelines on how to prevent money laundering.

In recent years, the country has vigorously marketed itself as a banking centre with considerable success. At the same time the European Union (EU) has been pressing for greater transparency in the local banking regime
in order to facilitate its tax evasion investigations. In February this year, the MAS said it had no plans to change its banking secrecy regulations. "They allow for the necessary transparency in combating criminal activity, while safeguarding investors' interest for safety and security," an MAS statement said. However, late last year Singapore more than doubled the financial penalties for money laundering crimes to S$500,000 (US$369,494) from S$200,000 (US$147,819) for individuals and up to a maximum of S$1 million (US$739,098) for institutions and corporations.

Washington has also criticised Singapore for loopholes in its anti-money laundering (AML) framework and for lack of transparency in its offshore banking sector. "Stringent bank secrecy laws and the lack of routine currency reporting requirements make Singapore a potentially attractive destination for drug traffickers, transnational criminals, terrorist organizations and their supporters seeking to launder money, as well as for flight capital," said the US State Department International Narcotics Control Strategy Report 2008 [1], "… Singapore should lift its rigid bank secrecy restrictions to enhance its law enforcement cooperation in areas such as information sharing and to conform to international standards and best practices." Singapore should include tax and fiscal offences in its schedule of serious offences that are predicates for money laundering, said the report.

The Financial Action Task Force (FATF), which published its latest assessment of the country in February 2008 [2] also expressed worries in this area: "The size and growth of Singapore's private banking and assets management sector poses a significant money laundering risk based on known typologies."

The FATF was dissatisfied with several aspects of the financial system. "Singapore has, generally, been less

aggressive in pursuing money laundering as a separate crime in the past, particularly in relation to third-party laundering, through Singapore's financial system, of proceeds generated by foreign predicate offences." The numbers of arrests, prosecutions and confiscations of funds look abnormally low in view of the size of the banking sector and the "level of money laundering risk," it said.

Daniel Thelesklaf, senior anti-corruption specialist at the Basel Institute on Governance, agrees that Singapore has work to do: "I believe that the very recent FATF evaluation of Singapore gives a fair overview on the country's anti-money laundering/ combating the financing of terrorism system," he told *MLB*.

Peter Gallo, of Hong Kong-based consultancy Pacific Risk Ltd, observed that while Singapore's legislation is fine, the island state lacks the political will to enforce it, adding that Singapore's banking secrecy laws are ideal for shielding fraud and money laundering activities: "If the Singaporeans were serious about doing something about transnational organised crime within their own jurisdiction they would enforce their own legislation within their own jurisdiction. That is what they fail to do – they have a very low number of convictions. You think Hong Kong is bad, Singapore is extremely bad."

Singapore has long been accused of harbouring the ill-gotten gains of corrupt Indonesian businessmen. Last year the two nations signed an extradition treaty, making it easier for Indonesia to extradite crooked bankers it claims are hiding out in Singapore. More than 18,000 Indonesian millionaires, with collective wealth of approximately US$87billion, live in Singapore, according to the Merrill Lynch/Capgemini Asia Pacific Wealth Report 2006.

"Billions of dollars from super-rich Indonesians, many who fled the country when Suharto was toppled, are laundered in Singapore," asserted Chee Soon Juan, secretary general of Singapore's main opposition, the Singapore Democratic Party. But because there is money to be made in Singapore, "everyone is happy to kick poorer governments, they steer clear of Singapore."

Gallo agrees that Indonesia is a problem for Singapore. "Singapore is the offshore financial centre of choice for Indonesia and Indonesia is one of the most endemically corrupt countries in the world," he said, adding that Singapore is also making itself vulnerable by maintaining close ties with Myanmar.

Despite the criticism, there is some support for the Singaporean system amongst AML specialists. Nigel Morris-Cotterill of the Kuala Lumpur-based Anti-Money Laundering Network said that unless money from Myanmar was explicitly linked with crime, such as drugs, Singapore would be doing nothing wrong by transacting business with Naypyidaw. The vast majority of Indonesian investments in Singapore are not shady at all, he added: "There's an awful lot of people who put their money into Singapore for absolutely 100% legitimate reasons – there are also, just like any other jurisdiction, people who put their money in Singapore for illegitimate reasons. But that's no different to any other country."

On the subject of legislative weaknesses, Morris-Cotterill was equally positive: "Singapore hasn't got a problem with its bank secrecy laws. The US, in particular, has a problem with Singapore's bank secrecy laws because the US has a problem with everybody's bank secrecy laws." The pressure to change is grounded in suspicions that have arisen out of the rapid expansion of the banking sector in the last three to five years, he thought. "There's a lot of political manoeuvring going on here. The bottom line is that Singapore has a very good law, and it constantly tweaks it to make it better… over the years it has improved it dramatically."

Notes

1. International Narcotics Control Strategy Report, March 2008 – www.state.gov/p/inl/rls/nrcrpt/2008/vol2/html/100809.htm
2. FATF Singapore mutual evaluation, February 2008 – www.fatf-gafi.org/dataoecd/36/42/40453164.pdf

Continued from page 20

"Last year the Treasury said firms should be able to cut costs through simplified due diligence and reliance but I think the regulator expects us not to cut costs but to make more efficient use of our resources," Ogden commented. There are overheads to the flexibility in the risk based approach, it takes more thought and justificatory documentation to keep alive and current in response to changing threats: "So, if someone down the line comes in, you can say, 'we thought this through, that was our risk based approach at the time and it was reasonable.'"

For more information about the Anti Money Laundering Professionals Forum, visit www.amlpforum.com

Grey areas

The new UK Money Laundering Regulations 2007 (MLR 2007) may be popular at HBOS plc, as Jane Ogden, Head of Corporate Financial Crime Prevention at the bank assured delegates to the recent Anti Money Laundering Professionals Forum conference, but plenty of grey areas remain.

Enhanced due diligence (EDD) provisions contain traps for the unwary, she noted: non-European Economic Area banks feature in the simplified due diligence (SDD) section if they are subject to requirements equivalent to the Third EU Money Laundering Directive but once there is any correspondent relationship they slip into EDD. In non face-to-face business EDD is unavoidable but its meaning when the customer is a corporate has prompted "a lot of head-scratching".

Equivalence is another difficult area; even when markets are regulated they do not necessarily have the same disclosure obligations and there are some countries outside the EU with markets that are subject to very high standards – can they be viewed as equivalent? Public authorities benefit from SDD but their definition outside the UK is "cloudy", said Ogden. Politically exposed persons (PEPs) are an ongoing challenge, not least the question of who is covered - the MLR 2007 do not mention siblings but the definition in Schedule 2 is careful not to be exhaustive by making repeated use of the word "include" when listing examples of officials, family members and associates who should be subject to EDD. Domestic PEPs are not covered though HBOS plc, in common with many major institutions, fails to draw this distinction. A decision must also be made about whether to continue with heightened due diligence once the subject has been out of office for a year. "While we like the ethos of the risk-based approach… you have to do a lot of thinking," said Ogden, citing the example of a PEP who comes in to buy a low risk product, which would normally be subject to SDD.

Reliance remains fraught. Although in theory it is permitted to rely on customer due diligence (CDD) carried out by a firm that is regulated by an approved professional legal body, the risk-based approach may dictate a different approach according to whether the practice is a two-man operation or a large City firm. There is also a concern on the part of the party relied on as provider of the CDD. The Regulations stipulate a five-year record-keeping requirement but if after this point, the documentation is destroyed and the firm relied on is served with a Production Order, law enforcement are not likely to be impressed – they like to see even fake paperwork – although no one will have broken the law.

Determination of the beneficial owners of private companies and maintenance of records on changes in ownership and control may need "material system changes" with a long lead time, said Ogden. In the interim, many firms will be using manual workarounds, a point the regulators should appreciate, she added. Piercing the corporate veil to reach back to flesh and blood individuals behind the business – in command of 25% - may be further complicated by the capital instruments, including ordinary, preference and bearer shares with variable voting rights.

Continues on page 15

Editor: Timon Molloy • Tel: 020 7017 4214 • Fax: 020 7436 8387 • Email: timon.molloy@informa.com
Production editor: Frida Fischer
Publisher: Nicola Whyke
Sales and renewals: Scott Davis • Tel: +44 (0) 20 7017 4151 • Email: scott.davis@informa.com
Subscription orders and back issues: Please contact us on 020 7017 5532 or fax 020 7017 4781.
For further information on other finance titles produced by Informa Law, please phone 020 7017 4108.
Printed by Premier Print Group
ISSN 1462-141X

Published 10 times a year by Informa Law, Informa House, 30-32 Mortimer Street, London W1W 7RE. Tel 020 7017 4600. Fax 020 7017 4601. http://www.informa.com