Money Laundering bulletin

The monthly briefing service for anti-laundering specialists

The AML, CTF and Sanctions jigsaw: do the pieces fit together?

Leaving the British Bankers' Association (BBA) after just over two years dealing with money laundering, terrorist financing and sanctions is a good time to take stock and risk a few suggestions for the future, writes ***David Coates****.*

Rather than work through the usual topics I want to tackle the subject by addressing the following themes: the statistical basis for action; resources; certainty; and responsibility. Underlying my analysis will be the assumption that in a situation of patchy information, limited expertise and scarce resources, significant progress will only be made if private sector actors, government, law enforcement and the regulators, work more closely together in defining the targets to be tackled and pool resources more effectively to achieve them. At present, despite some heroic efforts to the contrary, the overall situation for the banking sector could be characterised as the unremitting addition of extra requirements by the United Nations, Financial Action Task Force, the European Union and HM Government, together with fragmentation of effort where successful cooperation depends on a network of relationships rather than settled structures.

The Statistical Basis for Action potential reports

Apart from the area of card fraud, where APACS' (the UK payments association) figure of UK£535 million a year for total losses commands general respect, we are still in the era of crude estimates. Professor Michael Levi's report for the Association of Chief Police Officers (ACPO) on the "Nature and Economic Impact of Fraud in the UK", based on a critical survey of the existing literature, estimated that annual losses from fraud were at least UK£13.9 billion. But in his concluding comments Professor Levi added that the "patchiness of the data was self-evident" and mused whether the patterns of fraud identified by the report might reflect more the level of data-gathering effort and ease of compilation for individual sectors rather than a comprehensive picture. In a speech on 5 March, Jacqui Smith, the Home Secretary spoke of UK£20 billion lost to organised crime annually. Losses to HM Revenue & Customs from VAT repayment and Tax Credit fraud are often in suspiciously round figures. More reliable figures are critical to the targeting of prevention and asset recovery efforts. Similarly, accurate information on the proportion of criminal assets that leave UK jurisdiction very soon after they have been generated is relevant to asset recovery targets and the amount of resource

April 2008
Issue 152

IN THIS ISSUE

devoted to cooperation with overseas law enforcement agencies.

The reporting sector produced 220,484 suspicious activity reports (SARs) from October 2006 to October 2007. Banks and others are still waiting for comprehensive feedback on the relationship between the SARs they supply at considerable cost and the benefit to law enforcement. Anecdotal evidence linking SARs to individual investigation and arrests boosts the morale of counter staff and of those sifting the inflow of potential SARs in the MLRO centres. But something much more sophisticated and quicker-acting is required to refine financial institutions' targeting and nip new criminal trends in the bud before they are rolled out en masse.

Fortunately this is an area where there is room for guarded optimism. The new arrangements whereby banks take responsibility for reporting fraud against their customers to the National Fraud Reporting Centre, which comes into operation this year should, over time, give a much better snapshot of the extent of the problem and future trends, possibly at the cost of giving the impression of a massive upsurge in fraud in the first year. Sir Stephen Lander has always said that the Serious Organised Crime Agency's (SOCA) first priority is to "build knowledge and understanding of organised crime… and of the effectiveness of the various responses." That process may focus as much on the structure and geographical reach of large criminal enterprises as on the volume of the flow of criminal proceeds. Some signs of collars being felt and criminal assets recovered keep government ministers happy and banks on side, but SOCA needs to keep its collective nerve in mounting a deliberate and structured approach to its direct interdiction efforts. The enhanced asset recovery targets proposed by the Home Office in 2007 should not, in the interests of meeting short-term targets, be allowed to deflect the organisation from the painstaking work of identifying and then dismantling the large criminal networks SOCA suspect of being behind a large proportion of criminal activity.

In this context, SOCA's implementation of the SARs Transformation Project is critical to the organisation's success. Effective data mining and the related business changes should move SOCA's financial intelligence unit (FIU) further away from a focus largely on data channelling and quantitative feedback, towards maximising the connections between the packets of intelligence provided by SARs and other sources of information available to it. This would help both the investigative sections in SOCA plan their own work and also produce more usable intelligence products for the law enforcement agencies (LEAs), which will continue to be the main end-users of SAR material. But there is a much bigger prize dangling out there. The informal consultation process between the SOCA's project mappers and the reporting sector, and the parallel process with law enforcement agencies, offers an opportunity for a new look at how the various roles could be configured. Banks may not want to be drawn too deeply into the details of law enforcement, which, for its part in turn, may want to keep operational intelligence very much in- house. But the general shortage of expertise in financial investigation and the close working relationships which cluster around production and confiscation orders mean there are already strong links between law enforcement and the banks' investigation teams. Mutual testing of proposed approaches at an earlier stage before new strategic initiatives are rolled out could save much wasted effort and improve the ability of financial institutions, and government departments to take preventative measures. There is also a question as to whether the high volumes flowing from an 'all crimes' reporting system does not generate a fog of detail (including a degree of defensive reporting), which acts as a disincentive to some local police forces to take SARs seriously. It is worth bearing in mind that not all financial crime work by the police revolves around SARs. One of the case studies at a late 2007 financial crime conference described rolling up a financial crime syndicate at Luton. Not a single SAR had been involved in the initial investigations.

Resources

The 2007 National Financial Crime Strategy is pretty light on discussion of resource issues (and does not cover fraud). Some extra money has been found to implement the new National Fraud Strategy which is welcome. The SOCA budget for 06/07 was UK£416million with UK£41 million for capital spending. But the pressure on local police resources has meant that the number of police officers ring-fenced for work on financial crime has fallen dramatically in recent years as the Fraud Review noted.

Home Office officials smile wearily when resources are mentioned. Flat budget settlements do not help. Accordingly, part of the rationale for the SARs Transformation Project is the need to produce a shift in the attitude of officers investigating non-financial

crimes towards treating SARs as an essential tool to build up knowledge on suspects and their associates. Banks too are hitting a resource ceiling for anti-money laundering and counter-terrorist financing and having to devote an increasing proportion of their efforts to chasing the needles in haystacks that are part of their legal obligations in areas such as sanctions or financial services provided in connection with goods needing export licences

Certainty

There are plenty of relevant texts with a Russian doll-like progression from UN Resolutions to FATF Recommendations to EU Directives and regulations to Treasury regulation to industry guidance. The *Serious Organised Crime and Police Act 2005* represents text with teeth. Some are more helpful than others. The Money Laundering Regulations 2007 set out the requirements of the Third EU Money Laundering Directive as transposed into UK law by the Treasury, which consulted widely with the financial sector and made changes to the draft legislation in reaction to some of the responses.

The Joint Money Laundering Steering Group (JMLSG) Guidance is the best attempt yet to bridge the gap between law and operational practice, produced by the specialists in each of the financial sectors after intensive consultation with their memberships and painstakingly discussed, in reverse consultation, with government, the FSA and to a lesser extent, law enforcement. Yet even the Guidance does not claim to provide a clear cut solution to every problem. The legal profession still has some difficulty trouble with the status of industry guidance incorporating a risk-based approach, despite the Chancellor's formal approval of the JMLSG Guidance. Smaller firms feel uneasy at having to make so many judgements, perhaps without the opportunity of easy benchmarking with their peers. Large organisations relish the chance to apply resource in accordance with the detailed knowledge of their largest risks. Even for the larger firms, however, the risk-based approach brings with it the possibility that with post-event hindsight the Regulator may take a different view from their own on the quality of their risk mitigation.

The area of sanctions is particularly challenging. The scope of the obligations on governments under Paragraph 6 of UN Security Resolution 1737 on Iran to prevent any involvement, however remote, by their financial sector in the provision of financial services in connection with Iran's uranium enrichment programme, is almost infinite. Even the FATF, in drawing up "non-binding" guidance, has had to balance the obligation on banks to spot the needle in a haystack with encouragement to member governments to give their financial institutions a clue as to where the needle might be found.

"Politically Exposed Persons" (PEPs) is another term which gives rise to endless debate. The EU charmingly decrees that in-country PEPs, for example British Ministers or MPs, are less of a risk than those banking across national boundaries and therefore not automatically candidates for enhanced due diligence. In referring to reliance, the Third EU Money Laundering Directive makes frequent reference to "equivalent jurisdictions". Those variations known to exist between EU member states are ignored; there is no list of acceptable or unacceptable jurisdictions outside the EU. Fair enough in a way, since this allows the exercise of judgement by firms with the comparative advantage of experience of operating in difficult environments; and equally for judgement by those without such experience, but the vacuum leaves a lot of firms floundering.

Responsibility

In the system, risks are not equally distributed between the private and public sector. The Home Office sets no financial crime targets in deciding how to assess the performance of individual police forces, although national asset recovery targets may change the picture in the future. SOCA has responsibility for the overall operation of the SARs system but no line management authority over other LEAs or influence over their budgets.

The banks have a duty to obey the law and meet the requirements of the regulator. Their individual employees are liable to criminal prosecution for act of omission as well as commission under the *Proceeds of Crime Act* (POCA). On conviction they are liable to up to 15 years' imprisonment. The rebalancing of the risk of criminal prosecution implied in the Option 2 of the Home Office Consultation Document on the SARs Consent Regime [1] would help would reassure industry MLROs that they were being treated as partners with difficult decisions to make, rather than as potential felons. Banks have no control and little influence over the obligations that government imposes on them and are frequently involved in conversations after the event to explain why application of measures decided with the best of intentions in a political context would, if applied to the letter, cause havoc in the international financial system

without securing the intended benefit. The EU Regulation on Payer Information on wire transfers is a case in point. The Treasury and the FSA have proved helpful with post-event "fixes" but it would be preferable to avoid the problems at source.

UN sanctions lists names without unique identifiers require considerable manual intervention to weed out false positives, usually all of the names thrown up by the automated checking system. Officials sometimes fail to grasp the difficulty of applying handicraft methods to a high volume, straight-through processing system. The lists are often slow in gestation, allowing potential targets plenty of time to make alternative arrangements. In essence, the lists often appear to be nothing more than a political gesture.

Future

SOCA needs a little more time to bed down a raft of innovation brought in over the last two years and a few more successes to keep hope alive in the meantime. Outreach to industry needs consolidating. Harmonious interaction with local LEAs is work in progress. Funding for data mining should be maintained even if there have to be cuts elsewhere. SOCA might also look harder at new ways to incorporate into its own priority-setting process input from those in large financial institutions deciding priorities for their own firms. The treatment of fraud cases reported to the National Fraud Reporting Centre for SARs purposes also remains to be determined

Turning to government, the area of sanctions needs a root and branch examination firmly grounded in the resource implications of current requirements and what might be done to improve outputs on the basis of the level of resources available. Many of the initiatives in this area originate outside the UK but our government is an active player in the UN, FATF and the EU, which function largely on the inputs from member states. The initiatives do not come from Mars. The FATF outreach to the private sector should be encouraged and broadened beyond the charmed circle of the Wolfsberg Group.

As for the regulator, I hope the risk-based approach to AML survives undamaged in the post-Northern Rock FSA and that the very energetic Philip Robinson can limit himself to only two new thoughts before breakfast daily!

Notes

1. www.homeoffice.gov.uk/documents/cons-2007-consent-regime?view=Binary

David Coates *is immediate past Director, Financial Crime (AML & CTF), British Bankers' Association. He may be contacted on email: david.coates@live.co.uk*

Tipping off – the new regime

On 26 December 2007 significant changes were made to the tipping off offence in Part 7 of the Proceeds of Crime Act 2002 (POCA) by the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007.

Peter de Verneuil-Smith*, barrister, 2 Temple Gardens, looks at how the new offences differ from the old and what impact this is likely to have in practice.*

The old *section 333* offence

Section 333(1) of the *Proceeds of Crime Act 2002* (POCA) entitled "Tipping off", made it an offence for a person to a make a disclosure that was likely to prejudice any investigation which might be brought following a protected or authorised disclosure, when that person knew or suspected a protected or authorised disclosure had been made. Although that section made no reference to the *mens rea* required, it was clear from *section 333(2)(a)* that no offence could be committed unless the individual knew or suspected that the disclosure was likely to prejudice any investigation. Further, no offence could be committed if no suspicious activity report (SAR) had been made at all.

The tipping off offence was a huge worry for all those who might know or suspect that a protected or authorised disclosure had been made, mainly those in the regulated sector. Banks, solicitors and accountants have sunk thousands if not millions of man hours worrying about whether a disclosure made to a client, or even a colleague, could constitute the offence of tipping off and expose them to a prison sentence of up to five years.

The recent changes to the tipping offence were an opportunity for the government to ameliorate some of the confusion regarding tipping off. However, as discussed below, that opportunity has been largely missed and although some improvements have been made, a further dimension of worry has been bestowed upon the regulated sector.

The genesis of the new offence

The change to tipping off can be traced to the 2003 update to the 40 Recommendations made by the Financial Action Task Force (FATF). Recommendation 14 provides "*Financial institutions, their directors, officers and employees should be: a)…b) Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU [Financial Intelligence Unit].*" The note to Recommendation 14 states "*Where lawyers, notaries, other independent legal professional and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping off.*"

The EU has sought to update anti-money laundering standards in accordance with the 2003 FATF Recommendations through the Third Directive on Money Laundering (2005/60). Article 28 of the Third Directive is concerned with tipping off and its exceptions (which go well beyond the one exception recognised by FATF).

The new tipping off offences

Section 333 has been abolished and replaced by *section 333A*. *Section 333A* contains two new offences. *Section 333A(1)* makes it an offence if three conditions are met: (i) a person discloses that there has been a disclosure under Part 7 of POCA to a constable, an officer of Revenue and Customs, a nominated officer or a member of staff of SOCA of information which came to the person making the Part 7 disclosure in the course of business in the regulated sector; (ii) the disclosure is likely to prejudice any investigation which might be conducted following the Part 7 disclosure; and (iii) the disclosure is based upon information which came to the person in the course of a business in the regulated sector. The *actus reus* is very similar to the old *section 333* save that (i) the new offence focuses on tipping off that a SAR has been made and (ii) the new offence can only be committed by a person who acquired knowledge of the SAR whilst acting in the course of a business in the regulated sector. The *mens rea* is also, happily, the same as under the old *section 333*. *Section 333D(3)* provides that no offence is committed under *section 333A(1)* if the person did not know or suspect that the disclosure was likely to prejudice any investigation.

The second offence is contained in *section 333A(3)* and occurs when (i) a person discloses that an investigation into a money laundering offence under Part 7 is contemplated or underway, (ii) the disclosure is likely to prejudice that investigation, and (iii) the information on which the disclosure is based came to the person in the course of a business in the regulated sector. Again the *actus reus* is essentially the same as the old *section 333* save for (i) the focus on a money laundering investigation that is contemplated or underway and (ii) the new offence can only be committed by a person who acquired knowledge of the investigation whilst acting in the course of a business in the regulated sector. The *mens rea* is the same as for *section 333* and requires knowledge or suspicion that prejudice was likely (see *section 333D(4)*).

Whilst both of the new offences (disclosure of SAR and disclosure of investigation) apply to a smaller pool of individuals than *section 333* did (because the new offences can only be committed by those carrying on business in the regulated sector), *section 333A(3)* has a wider scope of criminality. Whereas no offence could be committed under *section 333* if (i) no SAR had been made or (ii) the individual did not know or suspect that a SAR had been made, those requirements are absent from *section 333A(3)*. Thus the bank clerk who learns from a MLRO briefing that SOCA is contemplating an investigation into customer X and that no SAR has been made in respect of X and then discloses this casually in a conversation with X will probably commit the *section 333A(3)* offence. But *section 333A(3)* was not necessary to criminalise that sort of tipping off. Such a disclosure would also be an offence under *section 423* of POCA, which provides that an offence is committed (i) where a person knows or suspects that a confiscation investigation, a civil recovery investigation or a money laundering investigation is being conducted or about to be conducted and (ii) that person makes a disclosure which he knows or suspects is likely to prejudice the investigation. However, as part of these changes *section 342* has been hived off to apply only to the unregulated sector. A new *section 342(3)(ba)* has been introduced which provides a further exclusion to the offence where the disclosure is based upon information which came to the person in the course of a business in the regulated sector. Because these changes are pursuant to *European Communities Act 1972* there is a ceiling upon the criminal sanctions of two years' imprisonment. In contrast, the unregulated sector (which logically should be less culpable for tipping off than the regulated sector) is exposed to a higher penalty under *section 423* of five years' imprisonment. It seems the only reason that *section 333A(3)* has been introduced is, as discussed below, to limit the disclosures made by professionals in the regulated sector to clients which are immune from tipping off.

The exceptions to tipping off

In line with the Third Directive the new offences are subject to four sorts of exception.

First, intra-institution disclosures. No offence is committed when a disclosure is made by an employee, officer or partner to another such individual within the same undertaking (*section 333B(1)*). No offence is committed when a disclosure is made between credit or financial institutions situated in the EU or in a country with equivalent money laundering requirements and both institutions belong to the same group (*section 333B(2)*). Group is defined by Directive 2002/87 (essentially parent and subsidiary companies). No offence is committed when a disclosure is made by a professional legal adviser or a relevant professional adviser (meaning an accountant, auditor or tax adviser) to another such adviser in a different undertaking that shares common ownership, management or control (*section 333B(4)*). These are helpful exclusions that should relieve some of the tension which has historically attended discussions between in-house professionals, such as MLROs, and other employees of an undertaking or an associated undertaking.

Second, inter-institution disclosures. No offence is committed when a disclosure is made (i) by a credit institution, financial institution, professional legal advisor or relevant professional advisor to an equivalent party (which is situated in the EU or a country with equivalent money laundering requirements), (ii) which relates to a client or former client or a transaction or service involving both parties, (iii) the disclosure is for the purpose of preventing a money laundering offence and (iv) both parties are subject to equivalent duties of professional confidentiality and personal data protection (*section 333B(2)*). This is an exclusion which encourages the exchange of information between different professionals and entities in order to combat money laundering.

However, the exception is particular and requires the disclosure to be to the equivalent party. Thus a disclosure made by a lawyer in London firm to an accountant in a German firm about a mutual client would not be protected. The London lawyer must make the disclosure to a German lawyer who in turn, relying upon *section 333B(1)*, may disclosure the same information to the accountant at the same firm. This rigidity is unfortunate as it necessitates increased costs for those seeking to prevent money laundering. Thus French auditors would not be able to alert English solicitors of suspicions regarding a mutual client. Instead, the French firm would have to instruct a professional legal adviser who could then make a disclosure to the English solicitors.

Third, disclosures made to a supervisory authority or made as part of compliance with POCA (*section 333D*). This is not controversial and replaces what was *section 333(2)(b)*.

Fourth, client persuasion disclosures. No offence is committed if a professional legal adviser or a relevant professional adviser makes a disclosure to the adviser's client for the purpose of dissuading the client from engaging in an offence (*section 333D(2)*). This exception replaces what was previously the privilege exception set out in *section 333(2)(c)*. Of all the changes this is the most problematic. The privilege exception to *section 333* had a long standing statutory base (*section 93D Criminal Justice Act 1988*) and it was clear that bona fide legal advice given to a client could not amount to tipping off (see paragraph 104 of *Bowman v Fels* [2005] 1 WLR 3083). However, the scope for a bank's lawyers making a disclosure to a customer's lawyers was unclear (compare Longmore LJ's dictum in *Re K Limited* [2006] 2 Lloyd's Rep 569 paragraph 18 to comments in *C v S and Others* [1999] 1 WLR 1551, 1557B and *Bank of Scotland v A Limited* [2001] 1 WLR 751, 756). That uncertainty is how not to commit an offence. What about the case where a customer's bank account is frozen and he wishes to obtain legal advice? The answer is that, whilst there is no applicable exception under *section 333D(2),* no tipping offence can be committed because the solicitor's suspicion or knowledge of a SAR or an investigation will not have come to him in the course of a business in the regulated sector. Hence in cases of litigation advice there is no scope for a *section 333A* offence. But what about the conveyancing solicitor whose client asks for an explanation for the delay in a property transaction? The solicitor may suspect that a SAR has been made in respect of the other party to the transaction and wish to tell his client as much. But it is hardly the case that the solicitor is seeking to dissuade his client from committing an offence. This exception will cause real difficulties in practice because there are many cases where solicitors and other professionals operating in the regulated sector will want to disclose to clients suspicions of a SAR or an investigation in circumstances where the client does not need to be persuaded against committing an offence. In those situations solicitors would have enjoyed the comfort of the privilege exception to *section 333* but now are at risk of committing a tipping off offence. It is a pity that the Government slavishly followed the Article 28.6 of

the Third Directive and ignored the warnings given by commentators as to this exception. It seems that those in the regulated sector will, in cases where the relatively low threshold of suspicion (a more than fanciful possibility - *K Limited* [200] 4 All ER 907) is passed, have little choice but to refuse to advise and suggest advise is sought from the unregulated sector, or seek permission from SOCA before making a disclosure. As a last resort those in the regulated sector may seek a declaration against SOCA (pursuant to CPR 25.1(1)(b) and *Bank of Scotland v A Limited* [2001] 1 WLR 751) in order to obtain protection against tipping off whilst being able to make some sort of disclosure.

In conclusion, whilst it is to be welcomed that *section 333A* maintains the same *mens rea* as the old *section 333*, the removal of the privilege exception from the regulated sector introduces a stark and artificial difference in the risk of tipping off compared to the unregulated sector. The very limited client persuasion exception in *section 333D(2)* is likely to unnecessarily expose professionals in the regulated sector and drive up compliance costs as those in the regulated sector may well have to encourage clients to seek advise from other professionals in the unregulated sector. In terms of overall anti-money laundering strategy it is difficult to comprehend how these changes, and in particular the shift from advice being given by the regulated sector to advice being given by the unregulated sector, make any difference to the effectiveness of anti-money laundering in the UK.

Peter de Verneuil-Smith *may be contacted on tel: + +44 (0)20 7822 1200; email: PdeVerneuilSmith@2tg.co.uk*

Our friends in the east: part II

One of the most difficult aspects of the MLRO's job is keeping up with what the legislators are pleased to call "national and international findings" on money laundering issues. In last month's column, writes ***Sue Grossey****, I started looking at the recent batch of country evaluations published by the Asia/Pacific Group on Money Laundering (APGML). Like the Financial Action Task Force (FATF), the APGML uses the agreed Assessment Methodology and Mutual Evaluation Questionnaire and Report Templates, as administered by a team of experts, to assess the effectiveness of the anti-money laundering/counter financing of terroristm (AML/CFT) regimes of their member jurisdictions. In 2007, four reports were published as part of the APGML's second round of evaluations [1]: working alphabetically, I looked at Macao and Malaysia last month, and this month it is the turn of Mongolia and Taipei.*

Mongolia

In case you are as confused as I was, and somewhat misled by childhood threats of being sent to Outer Mongolia as a punishment for misdemeanours, I have done a little research on exactly what and where Mongolia is. It is a landlocked nation, bordered by Russia to the north and China to the south. It is massive – the nineteenth largest country in the world, covering 1.5 million square kilometres. But with a population of only 2.6 million (that's slightly larger than the population of Jamaica), it is the least densely populated country in the world. A third of that population lives in the capital, Ulan Bator, and another third is nomadic. The term "Outer Mongolia" is now ridiculously outdated; it became simply Mongolia in 1911, while the old "Inner Mongolia" is now part of China.

This first-ever evaluation of Mongolia's anti-money laundering/ counter financing of terrorism (AML/CFT) regime was undertaken by a team from the APGML in December 2006. [2] It seems that Mongolia, despite its small population, presents many vulnerabilities to money laundering. Its recent political history has made it particularly vulnerable to corruption (and therefore to the laundering of the proceeds of corruption), as noted in the APGML report: "In common with a number of economies transitioning from communism to a free market, over the past 14 years Mongolia and independent observers have identified considerable problems with corruption, in particular associated with activities involving the privatisation of large sections of state-owned enterprises and property… In 2006 Mongolia passed a comprehensive anti-corruption law which, amongst other things, laid the foundations for the creation of an independent corruption fighting body."

Other significant predicate crimes in Mongolia are tax evasion, drug trafficking (eg, of heroin overland to Russia), poaching of and trafficking in endangered species, smuggling of antiquities and fossils, and human trafficking. There is an additional risk from the activities of the delightfully-termed "ninja miners": "Mongolia has a very large informal mining sector, with estimates

that there are up to 100,000 'ninja miners' operating who illegally extract deposits of gold and other minerals without a mining licence."

As a predominately cash-based economy, Mongolia has a large "informal sector", which, with its lack of supervision, is vulnerable to money laundering. The country's large underground banking sector "reflects demand for low cost remittance [thanks to] the relatively high costs and slow speed of remittance using the formal financial sector and the large number of foreign workers remitting money to Mongolia." Currency smuggling is also rife – probably for the same reasons. And to top it all, "Mongolia has an expanding real estate sector with rapidly increasing prices and a trend of 'off the book' transactions which poses a significant vulnerability for money laundering through this sector."

Mongolia seems to be at the start of the process of creating an effective AML regime. Money laundering is implicitly criminalised under the Criminal Code, but the scope of this offence does not meet international standards. A law on Combating Money Laundering and Terrorist Financing (CMLTF) came into effect on 8 July 2006, but this law does not establish any criminal offences. Rather, the CMLTF law allows for the establishment of a financial intelligence unit (FIU) (which will in turn develop AML requirements for financial institutions, such as customer due diligence (CDD), reporting and internal controls) and provides for international cooperation. The FIU was created within the Bank of Mongolia (the central bank) in November 2006, but has yet to start receiving SARs, and there are fears that it may be hamstrung by the limited investigative powers granted to it by the CMLTF law – it is too early to tell.

As for the theory of what the FIU will be able to demand of financial institutions under the CMLTF law, there seem to be serious deficiencies. There is no requirement for the regime to be risk-based; there is no requirement to verify the identity of beneficial owners; there is no requirement for on-going monitoring; there is no mention of enhanced due diligence for PEPs or correspondent banking relationships; and SARs are not required for non-cash transactions of any kind, nor for domestic transactions under 20 million tugrik (about UK£8,500).

As for other businesses, the report makes sad reading: "Designated Non-Financial Businesses and Professions [DNFBPs], as set out in the FATF standards, have not yet been brought into the AML/CFT regime in Mongolia, with the exception of trust service providers… With the exception of trust service providers, there are no CDD requirements on DNFBPs operating in Mongolia, nor are there any obligations to maintain records of customer identification or transaction data… Self-regulatory organisations [eg, for accountants] have only a limited role at present and no role in relation to AML/CFT measures for DNFBPs."

In the final analysis, the Mongolian AML/CFT regime was found to be fully compliant with only three of the FATF's Forty Recommendations – and largely compliant with six, partially compliant with nineteen, and non-compliant with ten, with one not applicable. With regard to the nine Special Recommendations, Mongolia was partially compliant with three and non-compliant with six. There is clearly much work still to be done.

Taipei

Goodness, I'm certainly picking them today. The Republic of China was established in 1912 and at that time encompassed much of mainland China. At the end of the World War II, it acquired the island groups of Taiwan (Formosa), Penghu (the Pescadores), Kinmen and Matsu. Then in 1949, the Republic of China shrank to just the islands when the Kuomintang lost the Chinese Civil War to the Chinese Communist Party and the People's Republic of China (PRC) was founded in mainland China. So now we have "China" referring to the mainland People's Republic of China, and "Republic of China" referring to the islands. In fact, because of diplomatic pressure from the People's Republic of China, the Republic of China is commonly referred to as "Chinese Taipei" by international organisations (such as the APGML). The population of just under 23 million is spread across the islands, with the majority living on Taiwan, where the capital city Taipei is located. The population density is the twelfth highest in the world, and the economy is the sixteenth largest in the world (with the finance and insurance sectors contributing 10.72% of gross domestic product).

This second evaluation of Chinese Taipei (henceforward simply Taipei) was undertaken by a team from the APGML in January/February 2007. [3] Although the evaluation was of the country's AML/CFT regime, it was noted from the outset that the two problems are treated differently – mainly because terrorist financing is not yet criminalised in Taipei (a law has been drafted but not yet tabled). Unlike Mongolia, Taipei has a well-developed anti-

money laundering regime, as described in the APGML report: "The money laundering threats from serious crimes are as follows (in order from serious to less serious): economic crimes, corruption, drug-related crimes, racketeering and others. Taking the statistics of 2005 as an example, there are 1,173 prosecuted money laundering cases, which includes 1,081 cases from economic crimes, 7 cases from corruption, 2 cases from drug related crimes, 2 cases from organised crimes and 78 from others. There were 1,678 suspects in total, about NT$7.7 billion [about UK£126 million] being laundered and NT$213 million [about UK£3.5 million] being seized."

The statistics are equally helpful when it comes to evaluating which sectors are most at risk from money laundering: "In 2005, there were 871 money laundering cases in which the illegal proceeds were laundered through banks, 287 cases through postal offices, 6 cases through credit unions, 2 cases through farmers' and fishermen's credit associates, 2 cases through securities companies and 5 cases through non-financial industries (underground banking, real estate or precious stone stores)…. Many non-profit organisations might be abused to engage in illegal activities, including money laundering, breach of trust, embezzlement, tax evasion, etc…. Authorities have identified money laundering cases that involved alternative remittance systems operated by jewellery stores and which usually use couriers to move currency cross-border."

As for measures taken to guard against money laundering, Taipei passed its *Money Laundering Control Act* (MLCA) in 1996 and amended it in 2003 and 2006, and further revisions are currently under discussion (including extending the scope of "serious crimes", improving international cooperation and requiring the detailed reporting of cross-border currency movements). However, despite recommendations of the FATF and other international agencies to the contrary, Taipei has not enshrined all of its AML requirements in law, but rather presents many of them in the form of guidelines issued to the financial sector and others.

There are significant weaknesses in these guidelines. As regards cash transactions, CDD and record-keeping are required only when the amount involved is about NT$1,000,000 (about UK£16,300) – a much higher threshold than is usually suggested. Little clear guidance is given on the need to establish beneficial ownership. Record-keeping requirements are inadequate: there is no mention of the need to keep records for five years or in a form that could be used in court, international transaction records are not captured, and there is no requirement to keep account files or business correspondence. With the exception of the banking sector, there are no specific obligations on financial institutions to monitor and keep records of complex, unusual or large transactions, or unusual patterns of transactions.

Taipei has a single financial regulator: the Financial Supervisory Commission (FSC). It is responsible for overseeing the AML/CFT regimes of financial institutions. However, the sanctions at its disposal "are assessed as inadequate in view of levels of findings of compliance breaches for the banking sector". Money changers and bureaux de change have only recently been required to put in place an AML regime, while insurance agents and brokers are still exempted.

As for DNFBPs, dealers in precious metal and stones are the only category covered by the MLCA – which means that there are no specific AML/CFT requirements imposed on lawyers, notaries, real estate agents, accountants, or trust and company services providers. (Casinos are outlawed in Taipei.)

Taipei's FIU is the Money Laundering Prevention Centre (MLPC). It is affiliated with the Ministry of Justice Investigation Bureau, which investigates (among other things) major economic crime and money laundering.

In the final analysis, Taipei's AML/CFT regime was found to be fully compliant with six of the FATF's Forty Recommendations – and largely compliant with nineteen, partially compliant with twelve, and non-compliant with six. With regard to the nine Special Recommendations, Taipei was largely compliant with three, partially compliant with one and non-compliant with five.

Personally, I find the reports issued by agencies such as the APGML to be invaluable. It is almost impossible to keep up with the developments in the AML/CFT regimes of every jurisdiction around the world, but at the same time, the risk-based environment places an obligation on the MLRO and his senior management team to keep up with these changes. Much of the information is interesting but generally irrelevant. However, if scanning a report can uncover such pertinent gems as the lack of oversight of DNFBFs in Taipei, or the financial misdoings of ninja miners in Mongolia, it is time well-spent. I will end with another thought from Winston Churchill, to match his pronouncement in last month's column: "True genius

resides in the capacity for evaluation of uncertain, hazardous and conflicting information." Bon courage!

Notes

1. Reports on two other APGML member jurisdictions were published by other bodies and adopted by the APGML in 2007, but are outside the scope of this article. A report on Cambodia was published by the World Bank, and one on Thailand by the IMF – both can be downloaded from the APGML website.
2. The full 147-page report can be downloaded from the APGML website at http://www.apgml.org/documents/docs/17/Mongolia%20Mutual%20Evaluation%202007%20-%20Final%20.pdf
3. The full 226-page report can be downloaded from the APGML website at http://www.apgml.org/documents/docs/17/Chinese%20Taipei%20MER2_FINAL.pdf

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

Risk adjustment

Are UK financial services firms making compliant sense of the risk-based approach to anti-money laundering (AML)? The Financial Services Authority (FSA) arguably took a big risk itself in August 2006 when it switched off the Money Laundering Sourcebook and substituted high level rules in SYSC (the Senior Management Arrangements Systems and Controls Sourcebook), which left firms to devise the AML model that best fits their business, although at the same time it strengthened the MLRO's hand by insisting that a senior manager assume responsibility for overall AML strategy. In June 2007 the FSA's Financial Crime Operations Team took a deep breath and went into the field to see if the concept was working; its findings, based on visits to 43 firms of various sizes and types, wholesale and retail and a survey of a further 90 small businesses, were published last month. The good news, as we intimated in the last issue, is that, (very) broadly speaking, the industry is adapting to the move away from tick-box to 'creative' compliance. As expected, performance varies considerably, largely on the basis of firm size and therefore with resourcing and level of scrutiny by the regulator.

Large firms, the survey found, had generally carried out a formal money laundering risk assessment and a couple had asked external consultants to review their processes. Independent audit is not a requirement under the rules but there is a distinct risk to doing more than is needed since it is very hard to retreat from a self-imposed super-equivalent standard; today's best practice all too easily becomes tomorrow's regulatory expectation so it may be just as well for the MLROs at the two firms in question that the FSA names no names in its report.

Variation is beginning to emerge in AML practice even amongst large firms: there was no consensus about how often the risk assessment should be conducted, some said it was continually under review, which is the ideal, but others suggested that it would happen as new products were introduced, annually, or that it was a one-off exercise, which must have met with stony looks from the FSA reviewers, though not as grim-faced as when some firms admitted that they had not performed any risk assessment at all. If this was the range for large firms one can only guess at the diversity in medium-sized institutions; the FSA said assessments in this group "varied greatly with most focused more on fraud risk". Small firms, while they had undertaken "some kind" of risk assessment, viewed the money laundering risk as low since their customer funds had already entered the system and would have been subject to prior checks; business often came through lawyers and accountants, trusted professionals subject to their own AML obligations.

More positively, the FSA found that communication between MLROs and line managers was working well. The senior manager charged with AML in large firms was usually at the level of Chief Risk Director, Chief Security Officer, Chief Operating Officer or Director of Compliance. The individual might also be the MLRO but it was usually their deputy who acted as the nominated officer, who has to report SARs to the FIU. It was common practice for the MLRO to provide a monthly report to the Compliance Director, including any serious instances of fraud or money laundering and progress with AML work programmes, which would cover any actions in response to recommendations contained in the previous year's MLRO annual report to the Board. The Audit Committee or Group Risk Committee was frequently the conduit for management information (MI) on AML issues to the Board. In medium-sized firms, even when the MLRO wore several hats – he might be company secretary, compliance officer, possibly the

CEO – the FSA found that, barring a few cases, he or she had enough time to spend on AML, which suggests that it need not be as onerous a task as the vast amount of literature produced on the subject might lead one to believe, although the task of sanctions compliance and Politically Exposed Person (PEP) screening alone would seem to be a full-time job on its own for all but the smallest operation. The regulator must also be at least slightly concerned that while all MLROs in small firms had a background in financial services, not all had specific AML experience and training. It makes one wonder quite what they include in their annual MLRO report, although perhaps it is comforting to know that the subject is not so technical that someone equipped with the Joint Money Laundering Steering Group Guidance, the FSA rules and sound sense should be able to create an AML framework to satisfy the regulator.

One of the much-vaunted benefits of the risk-based approach (RBA) is the opportunity to identify of retail customers by means of a single official document. One retail bank, which had elected to go down this route, estimated the savings to be UK£10m per annum, although it had balanced the move with increased risk-based sampling to combat fraud risk and still required submission of two pieces of original ID from prospective clients from higher risk jurisdictions. Sample selection would also be based on jurisdiction status, as well as post codes and branches that had proved vulnerable to fraud or for which account opening rates were lower than expected. Another bank had decided to still insist on two pieces of ID based on its view of the fraud potential and to enable cross-selling of other products and services, which would raise the customer's risk profile, without having to go back to them for further documentary assurance of their identity. The most popular official documents were passports, EU identity cards and the photo driving licence. Medium and smaller firms tended to err on the side of caution and require two pieces of ID evidence, the second was usually a recent utility bill or bank statement.

Enhanced due diligence (EDD) could be triggered by many factors in large firms, including the jurisdiction in which the client was located; whether he or she was a PEP; and the nature of the business, for example, if it was a money service business or casino. Offshore trusts, special purpose vehicles, international business companies (IBCs) in territories where AML controls are weak or which operate bank secrecy rules were also likely to prompt closer monitoring. Other EDD drivers were the existence of bearer shares and customers who operated several accounts across different jurisdictions. EDD was characterised by more intense checks on identity, notably of beneficial ownership and more rigorous examination of source of funds and wealth. Senior management sign-off was also needed before clients subject to EDD were adopted.

In some cases large firms were going to great lengths to check on PEPs and sanctions list status; they looked not only at the immediate customer but also at whether it was owned or controlled by individuals or entities in one of these categories. One international bank even looked for PEP connections with corporate clients when there was no element of control, which made life especially challenging in the Far East, since every company of note in the region will have a PEP on the Board.

The large banks were equally careful in their review of potential respondents, risk-rating prospects, which would determine the level of manager approval needed to establish the relationship, how often it would need to be reviewed – generally, at least annually for the higher risk class – and the treatment of any alerts raised through the firm's automated transaction monitoring programmes.

Commercial database providers have been busy signing up larger institutions to their PEP and sanctions list screening products but, according to the FSA findings, they have not had much success in the medium-tier market, which cannot afford their charges and so fall back on manual checks. In small firms the main criterion for EDD proved to be geographic location and screening for PEPs or sanctions list proscription was not always carried out regularly on the basis that it was unlikely that they would encounter this type of client. Financial planning for families was cited as a case where firms believe that they already gather sufficient information to obviate the need for EDD.

Although the majority of large firms have invested in automated transaction monitoring systems, based on rules or profiling or some combination of the two, the results have been mixed and the software was widely viewed as only useful in the high-volume retail environment. A few institutions were still concentrating on exception reports based on transaction threshold breaches with limits set between UK£3,000 and UK£9,000. Medium-sized firms relied mainly on manual review, monthly, of reports based on application of database interrogation rules that reflected possible suspicious activity like early redemptions and cancellations, investment transfers to different

beneficiaries and changes to customer details. The FSA found that only two mid-sized firms were looking to implement a fully automated transaction monitoring system. No small firms were contemplating automation but instead their MLROs would review weekly or monthly records of client transactions. In other cases the MLRO would check a proportion of new business – normally 10% – taken on by each consultant.

Training was commonly delivered by computer in larger firms and offered scope to tailor the questions and test understanding; it was an annual requirement. Some institutions sought to assign staff risk ratings according to their level of customer contact and whether they handled client data. Higher risk roles would be given additional tailored training, either face to face or on video/DVD. Medium-sized firms also used computer-based training (CBT) but normally in conjunction with other instruction, including workbooks produced in-house, ad-hoc sessions around required reading and testing, scenario consideration, team exercises and training videos. Half of these firms carried out annual refresher training; the rest either expected staff to undertake it every other year or had no documented requirement in place, they claimed their training policies were either under review or provision was already made on an ad-hoc basis. Small firms favoured in-house face-to-face training but testing was not common, which makes it difficult, the FSA notes, to determine whether the message has gone home. Although refresher training occurred on a one to two year cycle in small firms, wholesale entities were marked out for their lack of adequate AML training provision of any sort.

The full FSA report may be read at www.fsa.gov.uk/Pages/About/What/financial_crime/money_laundering/library/reports/index.shtml. Report by ***Timon Molloy****.*

The China syndrome

A year after China began enforcing its Law of the People's Republic of China on Anti-Money Laundering - effective from January 2007 - observers are wary about the ability of the country's under-staffed enforcement agencies to keep pace with huge inflows of questionable funds into China's booming economy. writes ***Mark Godfrey*** *in Beijing.*

China fared relatively well in a June 2007 assessment of anti-money laundering (AML) and counter financing of terrorism (CFT) standards by the Financial Action Task Force (FATF): in a "very short time" it has made "significant progress" building and enforcing systems to counter money laundering and terrorist financing, the FATF reported.

Some local experts point to challenges facing the law's enforcement. "There is no effective personal asset declaration system in China," said Hao Wang, a partner at Rayyin, a local law firm in Beijing. In its June 2007 assessment the FATF noted that "information on beneficial ownership is not available which presents a major shortcoming."

Tweaking the system will be hard in China, say locally-based experts, who point to a combination of economic expansion – GDP growth exceeded 11% in 2007, a 14-year record – and endemic corporate-political corruption encumbering AML legislation and policing. "There is no clean money in China," said a prominent French lawyer who practises in Beijing and Shanghai, "Fortunes here are not made through hard work and innovation, but rather through renting or paying for government positions and special access to resources."

He instanced the case of a soldier-turned-businessman approved to supply coal to Chinese army installations. A portion of the coal, taken from state mines at favourable terms available to the military, is shipped to North Korea for dollars which are then moved back to China on returning coal trucks. "He's bought 15 apartments in SOHO New Town [a fashionable downtown Beijing apartment complex] with the proceeds."

Real estate is a "very convenient" way to launder money, says the lawyer, who claims that 60% of recent Beijing real estate developments have been built on "dirty" money. China's booming real estate and manufacturing sectors are both hungry for funds given recent government credit tightening measures designed to cool off the economy. Fittingly perhaps, the FATF recommended that China's AML and CFT measures and laws should also apply to a "wider range" of non-financial businesses and professions. China's new AML law targets officials at financial institutions - the law lists banks, credit unions, stock brokerages, insurance companies and investment trusts as those responsible for alerting the authorities to suspicious transactions.

However, China's borders have been porous to

"sacks" of money coming into the country undeclared, said Nigel Morris-Cotterill, director of the Malaysia-headquartered Anti Money Laundering Network group. He suggested better technology is needed to monitor cash movements. Cross-border transportation in excess of RMB 20,000 or US$5,000-worth of foreign currency must be declared. Yet the FATF noted that information sharing between China's police and customs is "not optimal", noted Morris-Cotterill.

The local money laundering combat regime is young however. China first began seriously focusing on AML and CFT issues in 2003, with three sets of regulations improving due diligence at financial institutions. The People's Bank of China (PBOC) began on-site AML compliance inspections in 2004, and filed for FATF membership the same year. Established to comply with the FATF Recommendations, the Financial Intelligence Unit (FIU) at the PBOC operates two arms: the investigative and policy-setting Anti-Money Laundering Bureau (AMLB) set up in 2003, and the China Anti-Money Laundering Monitoring & Analysis Centre (CAMLMAC), established in April 2004.

This is progress, but even though it has an AML law and related institutions in place, China may lack the expertise to enforce it. Under-staffing at government agencies was listed by the FATF as one of its key worries. Although 35,000 police officers are available to investigate AML and terrorist financing, there are only 10 police in the AML division of the Economic Crime Investigation Department (ECID), a 200-man division of the Chinese police force.

The international standard-setter also recommended clearer communication channels between enforcement and supervision agencies. Staff at Chinese AML bodies are unable to "cooperate spontaneously" with foreign counterparts, according to the FATF report. A shortage of funds may be the issue. "It has been said that there is no separate allocation of expenditure for anti-money laundering from the state-council," said Hao Wang. "They have to share budget with the anti-fake money programme."

Staff and funding are both badly needed: a staff of 60 at the CAMLMAC, according to the FATF, receives 130,000 reports on suspicious RMB transactions and 350,000 reports on suspicious foreign currency transactions each month.

China's increasing integration into the international financial system will continue to propel AML regulatory reform in the local financial services sector. Chinese financial institutions were readying themselves since the late 1990s "to avoid difficulties with international correspondents," said Neil Katkov, managing director of Asia Research practice at the Tokyo office of international strategy consultancy Celent. He sees China being prompted by a "ripple effect" of recent AML and CFT legislation in the EU and USA.

Reform of the local banking sector has been driven by the emergence of foreign competition in a recently liberalised market. An earlier system of organising state banks on a regional basis with a high degree of autonomy at branch level has changed, said Morris-Cotterill. He pointed to a "huge improvement" in governance at the banks in the past five years, with a more centralised structure and system of internal reporting.

Better personnel may be key to better due diligence. Hitherto complicit in many instances of money laundering, politically-appointed branch managers of state-owned banks are being replaced by trained bankers. "In return for the job, managers were expected to do the local [Communist] Party's bidding," said Morris-Cotterill.

Knowledge of AML procedures remains rudimentary among cashier-level staff however. "There's an enormous number of people who don't know anything," explained Morris-Cotterill. The road to reform will be long, he predicts, "The number of national financial institutions is small but their staff headcount is huge."

Criminal gangs have been quick to take advantage of the banks' weaknesses. Prosecutors in 2006 sentenced cigarette smuggler Huang Xi Tian and 15 cohorts to life in jail for smuggling US$20 million worth of cigarettes from Vietnam to China over five years. Vendors lodged cash in several accounts set up in Shenzhen and Guangzhou by local bank official Huang Guang-rui. Guangzhou and Shenzhen are both prosperous manufacturing hubs and port towns: laundering through banks is harder to detect here given that large (legitimate) international transactions are not unusual.

Judges sentencing Huang Xi Tian heard that bank staff had neglected to do due diligence on the bank account holders, who turned out to be fictitious persons created by Huang Guang-rui by using family members photos and altered ID numbers. While customer due diligence requirements on banks improved greatly with the AML law's passage, financial institutions, notes the FATF, are not required to conduct an ongoing review of the customer data.

Apprehending corrupt officials who embezzle state

funds in foreign jurisdictions has been a driving factor behind Beijing's new AML approach. "China wanted to cooperate with other [FATF] members concerning pursuing corrupted officials aboard. Without the new [AML] law, it would be very hard to pursue lots of related criminal activities," explained Hao Wang.

While it remains the source of the corruption that the AML legislation seeks to tackle, China's authoritarian but opaque political system could prove a barrier to the law's effectiveness. A clause in the law allows for penalties against financial institution staff for "having disclosed [a] state secret, business secret, or [breached] individual privacy." Authorities regularly use the pretext of protecting state secrets as an excuse to clamp down on journalists and activists working to expose political corruption.

The nature of the political system may not necessarily determine the effectiveness of an AML regime however. "A variety of political systems in Asia have cracked down on money laundering," said Katkov. "The region's leading economy, and a democracy, Japan is not ahead of China [on AML]," he claimed.

Worries about officials getting in the way of enforcement to protect privileges are overstated, said Katkov. Despite the absence of a sound asset declaration system, financial institutions, he says, can easily assess politically exposed persons (PEPs) in China. "There are plenty of vendors with these [PEP] lists who can provide them to financial institutions."

China however does not place AML requirements on foreign PEPs. It was also recommended to enact countermeasures against countries that are not compliant with FATF Recommendations. This is "unlikely to happen" given China's growing relationships with nations outside the FATF mechanism, said Katkov.

Despite these problems, China's AML regime bears reasonable comparison against neighbouring countries, according to most specialists contacted by *MLB*. Hong Kong, Australia and Singapore are regarded as regional leaders but Japan and South Korea, like China have been weak and late to enforce AML laws. "Most jurisdictions have a long way to go," said Katkov. In other Asian territories implementing existing laws remains the challenge. "There have been a lot of AML laws on the books [in Asia] but only lately legislators [and law enforcement agencies] have become serious about implementing them."

A large population and the global Chinese diaspora are assets in international money laundering activity. By contrast, money laundering in Japan and Korea remains largely limited to domestic criminal activity, said Morris-Cotterill. "There are not as many people worldwide who can speak Japanese and Korean." Chinese criminal clans by comparison have operated worldwide for "centuries."

Despite a recent spate of high level fraud convictions, cases based on specific money laundering charges are rare in China. "There seems to be a reluctance to pursue money laundering as a stand-alone offence, except as an offshoot of a known predicate criminal activity," notes the FATF's June 2006 assessment. Yet criticism of China's unwillingness to build cases on money laundering grounds only is undeserved, said Morris-Cotterill, "China is getting convictions on fraud on an hourly basis."

Three for one

The fight against money laundering took on a new character in early 2004 when the World Bank and the International Monetary Fund (IMF) formally adopted new methodology drawn up and agreed the previous year by the Financial Action Task Force (FATF). Since that time the three institutions have worked much more closely together and there have been substantial, if largely unquantifiable, savings from the elimination of duplication, writes ***Alan Osborn****. Given that the World Bank and IMF remits go much further than money laundering per se, it might be stretching credulity a little to call this a monolithic institutional front against money laundering but it is probably as close to that as is possible in today's complex financial world. In any event, a great deal of time, effort and money has gone into re-focusing the AML activities of the three institutions, inviting the question of how worthwhile it has been. This article considers what the three organisations have actually done "on the ground" in the past four or five years. We shall turn in a later issue to an assessment of the results.*

Of the three bodies – the FATF, World Bank and International Monetary fund – the FATF is clearly the standard-bearer, laying down the precise terms, definitions, methods, yardsticks and working practices in common use by anti-money laundering (AML) forces throughout the world today. In a sense, the FATF

"makes the weather" in this sector. As most AML experts know, FATF - formed in 1989 - is an inter-governmental body whose stated purpose is "the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing". It is a policy-making body which monitors its 34 members' progress in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and works to bring about national legislative and regulatory reforms in these areas.

In 1990 the FATF published a set of Forty Recommendations, revised in 1996 and in 2003, setting out the basic framework for anti-money laundering efforts and intended to be of universal application. A further nine Recommendations relating mainly to terrorist financing were added in 2001 and 2004.

The "40+9" have assumed iconic status in anti-money laundering/counter terrorist financing (AML/CTF) circles and lie behind the FATF's basic ongoing work, the mutual evaluation process. The purpose is to assess implementation in a member country of the necessary laws, regulations or other measures required under the 40+9 and to gauge their effectiveness. The evaluations are conducted by financial, legal and law enforcement experts drawn from FATF national delegations and the FATF Secretariat. The process includes an on-site visit to the jurisdiction and comprehensive meetings with government officials and the private sector over a two-week period and entails comprehensive and detailed procedures laid down in the FATF's indispensable Handbook for Countries and Assessors.

Countries have the right to keep all or part of the reports confidential but the FATF encourages wide dissemination and the sharing of evaluation and assessment reports by all bodies and organisations engaged in AML activities, notably the IMF and World Bank and the FATF-style regional bodies. Since 2004 all these have used the FATF Recommendations and methodologies. Vincent Schmoll, principal administrator of the FATF, explained the links between the FATF, IMF and World Bank: "When FATF first started, it did not work with the IMF or the World Bank as they had no interest or mandate for the work, although they were observers. It was around September 11, 2001 when the FATF was revising its standards that the IMF and the World Bank became interested in working with the FATF and contributing to the revision of the standards. At that time they were looking at countries that were trying to put FATF standards into place but were having difficulties," he told *MLB*.

"We published the revisions in 2003, meeting with the World Bank, IMF and regional bodies in the process. For about a year after that we worked closely with them and others to develop the methodology for conducting evaluations. We took all of the standards and broke them down into the component parts so they could be evaluated. We agreed to use the same methodology to eliminate duplication of effort. In the meantime the IMF and the World Bank had taken on AML as part of their function. When they did their regular assessments of countries, looking at everything to do with supervision, they would also develop an AML component, following the newly agreed methodology. This provided for a country that was going to be imminently evaluated by the IMF or the World Bank to allow an FATF evaluation to serve as the AML component – and vice versa. Under certain circumstances, the IMF/World Bank evaluation can serve as a mutual evaluation under the terms of FATF or the regional bodies," Mr Schmoll explained.

The FATF and its associated regional bodies decided that the majority of their mutual evaluations would be conducted by themselves, but recognised that for some countries an FATF or regional body evaluation was not imminent. In such cases the country could choose to have an evaluation by the IMF or World Bank of its entire financial system, of which AML would be a separate component, Mr Schmoll said. Such reports would in practice be identical to FATF evaluations "because the design of this collaboration is that you can take a report from one body and put it into the other and it would be the same," he said. But the treatment of such a report would be different. "Our evaluations and those of the regional bodies must be discussed in our plenary sessions. The IMF/World Bank reports are done specifically for their own purposes - they don't do mutual evaluations, and don't discuss them with the country concerned - they're handled internally though the reports should look the same in the end," he said.

Mr Schmoll cited the Netherlands as a country which was not scheduled to have an FATF evaluation until near the end of the third round process – around 2009/2010 – but which chose to ask the IMF to conduct an evaluation to give them an idea of where they were on AML. "That was not discussed in the FATF and not treated as a mutual evaluation but the Netherlands chose to go through the mutual evaluation process twice and that was their choice," he said.

About the same number of experts are involved in any evaluation, Mr Schmoll stressed. For FATF and regional body evaluations "there will always be one or

two members of the secretariat in question and then a minimum of four evaluators, one from the legal area, two from financial and one from law enforcement." IMF and World Bank evaluations are similar except that most evaluators are from their own staffs though they may bring in experts, especially in law enforcement, where they do not have staff expertise.

An overview of World Bank AML activity was given by Ms Latifah Merican, programme director of the World Bank Financial Market Integrity Unit (FPDFI) financial and private sector development. "Like the IMF, we conduct AML as part of our Financial Sector Assessment Program (FSAP)," she said. FSAP was set up in 1999 by the bank and the IMF to help countries identify vulnerabilities in their financial systems and determine needed reforms. "This is mandated work and we have dedicated units within the Bank for it. We only deal with the financial aspects of money laundering," Ms Merican said.

The Bank's work in this area is divided into four core pillars:

- Assessment of countries' compliance with the 40+9 FATF Recommendations;
- Technical assistance (the largest single activity), which includes helping countries to build effective AML defences and provides legal advice and assistance for banks and related financial services like lawyers and accountants;
- Policy development, covering action against corruption; and
- Knowledge management covering dissemination of the bank's AML texts, tutorials, guides and handbooks.

Ms Merican noted that while the World Bank worked ever more closely with the FATF, it was fundamentally a development institution and was mandated to link all its work with economic development. FATF standards were designed for advanced financial structures, she noted, and the Bank worked mainly with "low capacity" countries with little ability to implement FATF measures. Nevertheless it was often vitally important for such countries to avoid being tagged as vulnerable to money laundering since this served to deter foreign investors among other things. Thus the bank did a lot of work in helping countries understand exactly where they were vulnerable to money laundering and which sectors they should best focus on – lessons which may not always be needed in more developed countries.

Similarly, the IMF brings its own particular expertise to the fight against money laundering, significantly stepping up its role in March 2004 when the IMF board formally agreed to make AML assessments and technical assistance a regular part of IMF work and to expand this work to cover the full scope of the FATF Recommendations. Today the work is carried out under basically the same main headings as the World Bank and much of it is done jointly with its sister Bretton Woods institution in Washington DC.

An important consequence of an IMF/World Bank FSAP assessment is a Report on the Observance of Standards and Codes (ROSC), which shows how countries observe certain internationally recognised standards and codes, focusing primarily on the areas of direct operational concern to the IMF. There are 12 such areas, including AML, which was added in 2002. ROSCs are used "to help sharpen the institutions' policy discussions with national authorities, and in the private sector (including by rating agencies) for risk assessment," said an IMF official.

Essentially the IMF's AML activities are handled "within the framework of the surveillance we do at the country level," added a spokeswoman at the IMF's Media Briefing Centre. "What the Fund basically looks at is the statistical data. The function sometimes goes a little bit further on request but not really into auditing, which is not our mandate," a spokeswoman said.

From the above one can infer that while they observe the same standards, share evaluations and cooperate increasingly closely, the FATF, World Bank and IMF often have different client bases that require different, specialised, inputs in the AML field.

Form over substance – Hong Kong

Hong Kong's proximity and constitutional links to mainland China have ensured boom times for the local financial services industry, while also creating problems for local money laundering watchdogs. ***Mark Godfrey*** *reports from Hong Kong and Beijing.*

The special administrative region's central banking regulator, the Hong Kong Monetary Authority (HKMA), in February announced that it would ensure a "major supervisory focus" on money laundering and terrorist financing during 2008.

This comes as an upcoming mutual evaluation of Hong Kong by the Financial Action Task Force (FATF) approaches; the final report is expected in June 2008. Hong Kong has been a member of the organisation since 1991, but some legal experts believe that the territory has not done enough to restrict money laundering activities, particularly those relating to mainland China. The evaluation is "a bit of a worry" for Hong Kong agrees Jim Jamison, a partner at the Hong Kong office of law firm Clifford Chance. Hong Kong's legislature is nervous about legislation which may scare away business from mainland China, he explains. "We're sitting on the edge of a huge but very immature market… The Hong Kong government feels it has to balance between stifling the financial industry and protection of international standards."

His voice is not the only cautious one. Hong Kong will have difficulty in meeting the FATF standards, particularly in relation to cross-border transactions, according to David Fernyhough, executive vice president of Hill & Associates, the Hong Kong-based risk management company. Increasing financial ties and a loosening of travel restrictions on mainlanders means the border with China-proper is becoming "more porous," he warned.

This would only serve to increase Hong Kong's greatest vulnerability - an increasing interdependence with mainland China. A "fairly primitive" mainland banking system means Hong Kong banks struggle to assess the credentials of mainland customers, said Jamison. "In dealing with mainland customers there are few of the procedures and financial history that would apply to establishing the bona fide of a European or US customer."

While the mainland's new *Anti Money Laundering Law*, implemented in 2007, has been welcomed in Hong Kong, the absence of a formal cooperation agreement between the two legislatures has been a glaring drawback in tracking and prosecuting money laundered from the mainland. "Hong Kong has mutual legal assistance agreements with other legislatures but not with mainland China," stressed Professor Simon NM Young, Director of the Centre for Comparative and Public Law at Hong Kong University.

Meanwhile, Hong Kong's real estate sector, frequently the destination of mainland cash, is widely seen as the least compliant with Hong Kong's own anti-money laundering legislation - the *Drug Trafficking (Recovery of Proceeds) Ordinance* (DTRoP) and the *Organised and Serious Crimes Ordinance* (OSCO). Realtors are unwilling to lose sales and fees and rather walk away from a suspicion transaction rather than report it to the region's Joint Financial Intelligence Unit (JFIU), which enforces local AML laws. "The FIU could count on one hand the number of reports from the real estate industry," a retired member of the Hong Kong police force, who now advises business on fraud and theft avoidance, told *MLB*.

The local insurance industry has been similarly criticised for non-compliance. "There are many instances of people coming to Hong Kong with a suitcase of cash and buying an insurance policy, wondering only how soon can it can be surrendered and on what rules," explained David Fernyhough.

Also, money wiring agencies have recently come under government scrutiny. While larger international wiring companies have put staff and systems in place, a multitude of smaller operations in Hong Kong change the as-yet unconvertible Yuan for mainland clients, said Fernyhough.

The HKMA has responded, authoring revisions to Hong Kong anti-money laundering laws in force since January 2007 that meet FATF requirements to compel local money wiring agents to retain the records of customers wiring sums of HK$8,000 (US$1,026). "Most of the smaller money wiring agencies don't comply with the law," however, noted Young.

While local financial institutions are praised for their compliance – "AML is an industry in its own right… All of major banks have their own team dealing with nothing but AML," added Jamison – second-tier banks and mainland banks by comparison are "totally non-compliant," said Fernyhough.

Professions such as accountants and lawyers are also reluctant to report suspicious transactions by clients. "It's not that they don't want to, it's because trust is a very important part of the client relationship," explained Young.

Hong Kong's laws are comprehensive, "probably stronger" than most other Asian jurisdictions, he continued: "There's an overarching duty in the law requiring everyone to report suspicious transactions." He compared Hong Kong to Canada, where the duty to report suspicious transactions applies only to specific industries.

Local law suffers from poor implementation however. "It [the law] is rather to catch the obvious offences, and make it more difficult for large money laundering to happen at institutions," said Jamison. The city's legal system "hasn't moved with the times," he suggested. Local legislative efforts have been driven by law-making in the EU and US, rather than by domestic

needs: the 2004 legislation was a "catch-up" measure, synchronising the territory with USA, he said.

Indeed, figures within the JFIU feel that the city is "paying lip service at best," said the retired police officer. "Most enforcement is reactive. Enforcement often happens when money laundering is related to another predicate offence."

And while the city's position as a regional financial services hub means sound legal and banking records are kept and kept well, enforcement bodies are understaffed: "There is just so much money coming through HK, it's so hard to keep track," says Fernyhough. "One large bank [by reporting everything] suspicious would overwhelm the FIU." Satisfactory enforcement of the Hong Kong law would require an FIU (currently 50 strong) force of 50,000 officers, estimated Fernyhough. "That is unlikely considering Hong Kong's entire police force is 30,000 strong."

Enforcement bodies tackle the most obvious cases. "They work on the basis of 'which drop of water in this downpour should I catch?'" he said. Cases involving a non-FATF compliant country are particularly hard for the local FIU to deal with. "There's a feeling that we'll never get to the bottom of it so they just put it on file."

A more effective and hypothecated forfeiture law could provide resources for enforcement agencies, some lawyers suggest, however. The HK$124 billion (U$15.4 billion) confiscated since 1990 has all gone into state coffers rather than into funding for an enlarged force, said Young. "The enforcement agencies don't see the rewards."

Delays caused by the fact that Hong Kong's forfeiture law is conviction-based (requiring a conviction before police can seize assets) is delaying action against money launderers, said Young. A civil forfeiture system, allowing police to seize assets without there being a conviction, would be more efficient, he concluded.

The long arms of Uncle Sam

The impact of US law is felt far beyond the shores of America through extraterritorial provisions of statutes like the USA Patriot Act and sanctions programmes operated by the Office of Foreign Assets Control (OFAC). The US money laundering legislation may well be familiar to MLROs internationally but ***Duncan Aldred*** *of CMS Cameron McKenna warns practitioners not to neglect other live legal risks around extradition and the Foreign Corrupt Practices Act.*

They call it the 'perpetrator walk'. Finger-printed and strip-searched, the accused shuffles from police car to court house, clad in green jumpsuit and shackled hand and foot. The Department of Justice (DOJ) loves to twist the knife by putting on this humiliating show. But, from this (UK) side of the Atlantic, we don't relish this chance of the limelight. We don't want to be bundled through a foreign rite of passage thousands of miles from home, the single concession to our non American status being the colour of our prison clothes.

Behind this nightmare vision, there are several other reasons why, given the choice, we'd be tried here at home rather than by Uncle Sam. Being uprooted from our home and family has an emotional impact, but some practical features follow, too. Legal defence costs in the United States are high, and there is no equivalent of legal aid. A strong plea bargaining culture can be confusing to a UK defendant, who also has to keep in mind that US conviction rates are higher than they are here, US sentencing guidelines are more severe and the US prison system does not offer the 'not really like prison' option that sometimes seems to make a custodial sentence a breeze for businessmen convicted of crimes here.

Unplanned travel

Caught up in a fight against our own personal extradition, there is another point that might strike us as very unfair. It might even cross our minds that the Americans had pulled one over on our Government, and that the people we elected have not done much to protect us. The fact is that, if the Americans want to haul us across the Atlantic, they only have to come up with 'information that would justify the issue of a warrant for the arrest of the person'. This test, provided by the *Extraditions Act 2003* (which came into force at the beginning of 2004) was a downgrade on the earlier requirement of '*prima facie* evidence' of the relevant offence, but it is also less than our authorities need if they want to bring anybody from the US to face justice here. The Americans insist that our authorities show 'probable cause'.

But surely, the nightmare of extradition to the US is for crooks; law-abiding types who read (or write) articles like this can sleep undisturbed in the knowledge that the US authorities can never come knocking on our door?

In answer to this question, there is some good news and then rather more bad…

First, the good news. That comes from Ian Norris, the retired company director who finally received a boost from a commonsense House of Lords judgment in March 2008. Mr Norris's case tested that part of the extradition arrangements that says that, for us to take the enforced trip across the Atlantic, the conduct of which we are accused would be an offence in both the UK and the US and would be punishable in either jurisdiction by a custodial sentence of at least one year. 'Price fixing' (which has been against the criminal law in the US for many years) only became a crime in the UK when our *Enterprise Act* came into force in 2003. The US Department of Justice, though, demanded Mr Norris's extradition to face charges connected with what had to him seemed like business as usual in 1989. Mr Norris had to go through years of judicial heartbreak before our highest court overturned earlier decisions and reached a conclusion that we might have been forgiven for thinking was obvious from the start.

So we have confirmation that our conduct must really amount to a fairly serious crime here as well as in the US before we can be extradited. That much good news, but now for the stuff that should keep us awake anyway…

US Patriotism

If we do business that touches the United States we need to be aware of what the US authorities are trying to achieve and just when they might want to stretch out that long arm in our direction.

The *USA Patriot Act* was rushed into force on 26 October 2001, in the wake of the 9/11 terrorist attacks. From a British point of view, there's something a little unnerving about a statute that really does have the full title 'the **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism (USA PATRIOT ACT) Act of 2001' (I have emphasised the initial letters to make the point even more obvious). Terrorism is the clearly stated target for this statute but even assuming we're not terrorists, we may still be in the firing line.

This Act implemented a vast number of varied provisions. Amongst them, there is a section that gives US District Courts jurisdiction over foreign financial institutions involved in money laundering offences that occur in whole or in part in the United States. Another provision empowers the Secretary of State for the Treasury or the Attorney General to issue a summons to any foreign bank that maintains a correspondent account in the US and request records related to that account.

Back in the seventies

But the picture is very much more complicated than this, and American efforts to exert a long-arm jurisdiction go back much further than 9 September 2001. The *Foreign Corrupt Practices Act* (FCPA) came into force in 1977. It applies to 'US issuers', which includes any US company and its foreign affiliates, and any foreign company issuing securities registered with the US Securities & Exchange Commission (SEC). The Act aims to stop people paying bribes to foreign government officials to obtain government contracts. 'Wilful' violation of this statute can bring 20 years in a US prison or a hefty fine. More relevant from our point of view, there are also very serious penalties for 'non-wilful' breach of the Act. Individuals can incur fines of up to US$100,000 and five years' imprisonment for passing 'anything of value' to a foreign government official to influence an official act or secure an improper advantage. It is confusing rather than reassuring that small 'facilitating payments' will not be caught by the Act.

To take the Americans' side for just a moment, it is clear that something needs to be done on this front. In October 2005, the Volcker Committee inquiry into the United Nations Oil for Food programme found that more than 2,000 companies had paid the Saddam Hussain regime over US$1.5 billion in bribes to obtain contracts to sell humanitarian goods to Iraq.

Apart from not paying bribes to foreign government officials, we also have to operate appropriate accounting procedures. The US Securities & Exchange Commission (SEC) polices provisions of the FCPA that require relevant businesses to maintain books and records and internal controls such that the payments of bribes could not go unrecorded and that payments of any kind can only be made with proper authority.

The Department of Justice lists a number of 'Red Flag' features that it warns potentially provide sufficient notice of corrupt conduct. We can't afford to ignore these handy hints, particularly when US issuers can be held vicariously liable for the conduct of their agents and affiliates. The DOJ's helpful pointers will be stacked up and used against us if we fail to take notice. It is vital for any relevant business to keep track of the DOJ's Red Flags: the US authorities will offer no concessions for those whose knowledge is out of date. It will be no surprise, though, for example, that we should expect alarm bells to ring if we deal with

officials in a country which has a pattern of corruption, if we deal with an agent who has a reputation for unethical business practices or where any transaction is recorded as cash.

Not forgetting sanctions

Along with the SEC and the DOJ, the other US bogeyman that has the power to give us sleepness nights is the Office of Foreign Assets Control (OFAC - www.ustreas.gov/offices/enforcement/ofac). OFAC administers and enforces economics trade sanctions based on US foreign policy and national security goals. OFAC does not just affect US citizens, it extends its influence over all persons and entities within the US and US-incorporated entities and their foreign branches. The slightest connection with the United States can be enough here, and it is important to bear in mind that any transaction involving a payment in US dollars will touch the United States and so come under OFAC's gaze.

OFAC operates by prohibiting affected persons from entering into certain transactions, publishing and policing a list of Specially Designated Nationals (SDNs) whose assets it regards as blocked, and maintaining sanctions programmes. The SDN list currently comprises more than 6,000 names of companies and individuals connected with sanctions targets and located throughout the world. US persons are generally prohibited from dealing with them.

It is vital for affected businesses to inform themselves about what OFAC has in its sights and then to keep up to date. Currently, OFAC's sanctions programmes are described, not altogether helpfully, as falling under the headings of Anti-terrorism, Drugs, Cuba, and 'Other'. That sanctions list changes over time, and the SDN list changes on a daily basis.

Just as the Department of Justice offers its list of Red Flags as a helping hand that we ignore at our peril, OFAC has a hotline that it says we must call if we have reason to believe that going ahead with a transaction might violate its regulations. OFAC can impose very substantial penalties. ABN AMRO had to pay US$40 million to OFAC following a December 2005 finding. In light of that experience, it seems wise to take OFAC seriously.

So, how do we avoid the perpetrator walk, the green jumpsuit and the big fines? Only King Canute would invest his time railing against the unfairness of the system. We can be grateful to Ian Norris for doing his bit, but our time now is better invested as follows:

- Understand the law wherever we operate;
- Don't leave it to our compliance officers alone;
- Be extra vigilant in dealing with 'command' economies (where particularly strong governments influence the granting of contracts);
- Produce a clear policy on 'bribes' and disseminate it clearly;
- Don't just tell staff, insist on hearing back from them with confirmation that they understand and accept this message;
- Test the system;
- Know and look out for the DOJ's Red Flags;
- Monitor the US websites; keep up with the programmes; keep the hotline number handy.

Duncan Aldred *is a partner at CMS Cameron McKenna. He may be reached on tel: +44 (0)20 7367 2709; email: duncan.aldred@cms-cmck.com*

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