

Money Laundering bulletin

Cracked record

No shortage of holiday reading for AML professionals this summer but with little enough room left for the bucket and spade if all the research papers and guidance were printed out and packed; an iPad with sunlight filter would now seem to be an essential piece of compliance kit.

40+9 scorecard

First off, the International Monetary Fund (IMF) published a study of how well countries have conformed to global, ie, Financial Action Task Force (FATF) standards. [1] The mind-numbing econometrics reduce to one simple conclusion – ‘badly’. A revealing table, which features in an annex [2], sets out percentage compliance across all 40+9 Recommendations, taking into account every mutual evaluation conducted in the period 2004-2011. Of 7,889 observations (161 country assessments X 49 Recommendations), full compliance with any FATF Recommendation occurred in only 12.3%. Average compliance overall was 42.5% and non compliance 24.9%. The Working Paper noted marked weakness (22.1% of the theoretical full compliance score) in customer due diligence (CDD).

FATCA – a breathing space

Financial institutions, globally, will certainly be raising their CDD game to meet the US authorities’ demands for identification of US taxpayers under FATCA (the Foreign Account Tax Compliance Act) and avoid 30% withholding on their US source income. A six-month extension, announced in July means that foreign financial institutions will now have until 30 June 2013 to enter an agreement with the US Internal Revenue Service (IRS) in time to meet the FATCA effective date of 1 January 2014.

UK-Swiss tax compromise – elegant but how beneficial?

Swiss banks, additionally, will have to check for accounts held by those liable to UK tax. In a deal that partially preserves local bank secrecy, from 2013, on behalf of HM Revenue & Customs, the Swiss will levy withholding tax on future income of UK accounts at a rate of 48%. A one-off levy of between 19% and 34% will also apply to accounts extant at 31 December 2010 and still open on 31 May 2013; the exact percentage will depend on the size and age of the deposit. The Swiss reached a similar

September 2011
Issue 186

IN THIS ISSUE

- 1 Cracked record**
IMF on global 40+9 compliance; tax evasion; US and beneficial ownership disclosure; FATF reports – corruption, piracy and kidnap, human trafficking and smuggling; enforcement actions
- 4 What’s in a name? Would a SAR filed under any other name be as sweet?**
Shah v HSBC – court weighs anonymity for staff who report suspicion against open justice
- 7 Systematics**
AML technology – challenges both new and familiar
- 9 Perennial problems – banks and the PEP risk**
Latest FSA thematic review findings in detail
- 13 Derrick ponders... Ricky’s Risks**
Risk-based – approaches vary
- 15 I am not a number, I am a free man**
Human trafficking and smuggling – FATF report
- 17 Wide but not unbounded – the definition of criminal property**
POCA pitfalls for prosecutors
- 19 Usury – an Italian money-spinner**
Recycling criminal money at high interest
- 20 The third way – FATF promotes reliance**
Easier CDD for groups ere long
- 22 Unclear targets – PEPs**
FATF Recommendation 6 – more to do
- 24 Diary**

The new Money Laundering Bulletin website is now live.
Visit www.moneylaunderingbulletin.com today.

To request your new username and password, or for help
with online access, please email onlineaccess@informa.com
or call +44 (0) 20 7017 4161.

informa
law & finance

understanding earlier in August with the German government but UK tax evaders face a future tax rate of nearly double that paid by German account-holders. In addition to the remitted tax, which HM Government believes may contribute UK£5bn to the Exchequer, UK authorities will be able to request banking details of 500 UK persons, whom they suspect of tax evasion, each year. One has to question how many high net worth individuals will happily wait till 2013 to pay their dues, plus penalties, or have their affairs probed. A more likely scenario is surely wholesale flight of funds to more accommodating secrecy jurisdictions. Even if an individual was committed to Switzerland, he or she might choose to run down their account balance before the agreement takes effect, by buying real estate or other assets, leaving little to recoup.

US – staring at the corporate veil

The pressure on the Swiss to compromise, if not blast holes in their own banking secrecy provisions follows the US authorities' success in fingering US taxpayers who had hidden funds from the Internal Revenue Service offshore through UBS. [3] The high-level negotiations to secure those names were long and hard and it would have been surprising if the US's own less than perfect record on transparency was not held up to question in the process: how many US citizens are using corporate vehicles registered in onshore secrecy jurisdictions like Delaware – whose senator for 36 years was Vice President Joe Biden – to conceal the proceeds of evading US tax? Who knows is the answer as the obligations on company registration agents to identify ultimate beneficial owners are so limited. Senator Carl Levin, indefatigable campaigner for integrity in US financial services as chair of that Congressional conscience, the bipartisan Senate Permanent Subcommittee on Investigations [4], is seeking to expose the whole issue of ownership to scrutiny through the *Incorporation Transparency and Law Enforcement Assistance Act*. Proposals, which would address some of the shortcomings catalogued in the 2006 FATF mutual assessment of the US [5], include requiring the States, whether directly or through licensed company formation agents, to identify beneficial owners of corporations or limited liability companies (LLCs) formed under a State's laws, and keep the information up to date and accessible in case law enforcement, armed with a subpoena or summons, demand it.

Corruption – the same grand tour

If the legislation is passed, it should help investigators track the whereabouts of the funds of corrupt politically exposed persons (PEPs) – the subject of an FATF report published in July 2011. [6] The paper, based on study of a set of reported grand corruption cases – from the estimated US\$27m stolen by Chilean

dictator Augusto Pinochet (1973–2004) to the US\$5bn to US\$10bn amassed by Ferdinand Marcos during his time as president of the Philippines (1965–86) – notes that in every case corporate vehicles, trusts or non-profit entities of some type were used. It also observes that little has changed in the ten years (1996–2006) between two earlier FATF typologies reports, which highlighted the potential for abuse of corporate structures.

In 2010, Professor Sharman at Griffith University, Australia contacted 45 company services providers; 17 were prepared to set up a corporation on receipt only of a credit card details and a mailing address to which the documents could be sent. Some vehicles are even capable of evasive action in the event of official interest: “certain trusts, for example, require the trustee to transfer assets upon receiving notice of a law enforcement or regulatory inquiry.”

Gatekeepers, notably lawyers, skilled in setting up these structures, as well as opening bank accounts, making transfers, acting in the purchase of property and organising cash couriers, crop up frequently in the paper. Abuse of client-attorney privilege and client accounts was evident in the review of four cases of West African PEPs by the Permanent Subcommittee on Investigations in 2010. (US lawyers, it is to be remembered, are not required to file suspicious activity reports on their clients, although the American Bar Association issued voluntary guidelines on AML in August 2010.) Eventually the US banks cottoned on “and closed the attorney accounts, but not before hundreds of thousands of dollars had passed through.” It helps, certainly, if, the PEP's legal advisers are either highly incompetent or wilfully blind. In a civil recovery action [7] brought in the UK against Frederick Titus Chiluba, former president of Zambia, who embezzled an estimated US\$72m, his lawyer withdrew UK£30,000 – “an amount that vastly exceeded the president's annual salary” – and hand-delivered it to him.

The corrupt PEPs studied, “in nearly every case”, used foreign bank accounts; harder for the victim country to penetrate, viewed as “more stable and safer” and easier to access, they add to the complexity of asset tracing: the individual might “stack” jurisdictions with an account opened in one country owned by a corporation in a second and controlled through a trust in a third. Ownership may be further obscured through use of associates and family members as nominees, also found to be “common” in the inventory of cases. The paper cautions, however, that the presence of middlemen should not be viewed as a red flag per se since they frequently feature when the funds are legitimate. Domestic financial institutions are used to launder stolen funds as well: in 1998 a Spanish investigating magistrate issued a worldwide freezing order in

connection with an investigation into Pinochet's involvement in human rights abuses and other crimes. The ex-President was still able to obtain money from banks in Chile against cashier's cheques valued at US\$1.9m (in US\$50,000 increments) drawn on his account in the US.

Grand corruption, by definition, entails large sums: the unscrupulous PEP has to balance the advantage of withdrawing the money to break the audit trail against the risk of detection when re-placing it in other accounts. FATF found "in a significant number of cases" that PEPs opted to withdraw cash and were able to reinsert it into the financial system without arousing suspicion.

Pirates call the shots

Cash is also the form of payment dictated by pirates. FATF notes, in another report released in July 2011 [8], that, once paid, "the money trail generally goes cold." Failure to systematically record the serial numbers on notes handed over does not help and the paucity of intelligence is evident in continuing debate around whether Somali pirates use hawaladars or money service businesses to move the large sums received; these have grown exponentially in recent years, from an estimated total US\$5m in 2006 to US\$180m last year. [9] Although anecdotal evidence suggests that ransom proceeds may have been used to purchase property in Puntland (a self-appointed polity in Somalia), Eastleigh and Mombassa in Kenya, these reports have not been substantiated.

Efforts to combat piracy for ransom (PFR) are hampered by a perception amongst ship owners and operators that they have been abandoned by their governments: anxious to recover crew members, cargoes and vessels intact, they are not inclined to prioritise information-sharing with officials. Lack of local AML capacity in the horn of Africa is another major obstacle. "Somalia has no formal authorities or structure to implement an AML [regime] and Puntland is known for its complicity." Kenya has not established a Financial Intelligence Unit (FIU), or implemented its AML law. AML/CFT frameworks in Ethiopia, Seychelles, Yemen and Tanzania are still under construction while Uganda does not even have an AML statute.

One bright spot is an absence of proven links between the pirates and terror groups. Kidnapping for ransom (KFR), on the other hand, has been exploited by both terrorists and criminal organisations: the FATF project team was surprised to discover that the formal financial system, banks especially, play a prominent role. SARs filed in KFR cases, says the report, "can often have significant impact on a successful resolution" although law enforcement is often not informed of ransom payments. The job of the police is not rendered any easier when governments budget for making payments

to terrorists and by the confirmation that some groups which use KFR move the money through hawaladars to frustrate pursuit.

The people business

Cash, popular with pirates, is also king for the criminals who engage in human trafficking and people smuggling, according to questionnaire-based research by FATF. [10] Predominantly an East-West flow, the trade is estimated to generate US\$32bn annually [11], a significant slice of the yearly US\$130bn pie from illicit commerce, as calculated by the UN Office on Drugs and Crime (UNODC). However, the report remarks both inadequate data on the numbers of people moved for money and "even less information about the income generated by this activity and how it is laundered."

Patterns are discernible in the nationalities of organised crime groups involved – Russians, Albanians and Italian mafia take the lead in Europe and the Chinese gangs and Japanese Yakuza dominate in Asia. Atypical examples of traffickers are also cited: diplomats who restrict the movements of foreign workers they take with them on overseas postings and children in Koranic schools in Senegal, some as young as four, who are forced by their teachers to beg on the streets.

The report sets out a long list of red flags: there are some common elements like use of the same mobile number, address and/or employment references to open accounts in different names and frequent transfers of small amounts from trafficked victims to members of organised crime groups elsewhere in the same country or abroad. Other clues include payment of rent and bills on addresses in areas known for prostitution; credit card disbursements to online escort services for advertising; and, less obviously, large cash deposits inconsistent with the notional business activity of the account-holder; heavy use of cash, including for the purchase of business assets; and bank accounts characterised by flow-through – funds enter over a short period and broadly the same amount is quickly sent on to parties in a third country.

Enforcement – also lucrative

In addition to the substantial research papers, AML professionals need to keep an ever-watchful eye on the enforcers' modus operandi: the UK Financial Services Authority has fined Willis Limited, one of the largest insurance and reinsurance brokers in the London Market, UK£6.895m for failing to operate effective anti-bribery and corruption (ABC) systems and controls over payments to overseas third parties. [12] Between January 2005 and December 2009, the firm distributed UK£27m, almost four times the penalty, to "introducers" or "producing brokers" to help them win or retain business worth UK£59.7m; the FSA made no determination on whether any of the contracts were

corrupt although the firm filed two suspicious activity reports on payments totalling US\$227,000 to agents in Russia and Egypt during the investigation.

FSA found that Willis had not identified and documented the rationale behind payments or performed adequate initial due diligence on third parties supplemented by regular review. Between January 2005 and May 2009, the firm also fell down on monitoring its own staff to ensure they could properly explain why an overseas intermediary should be engaged. Senior management, throughout the period, was not provided with enough information on how the ABC policies were working to assess if the corresponding risks were correctly addressed.

In the US, JP Morgan Chase (JPMC) has paid US\$88.3m to settle ‘apparent’ violations of multiple sanctions programmes around dealings with Cuba, Iran, Sudan and Liberia. [13] The bank processed 1,711 wires transfers involving Cuban persons, totalling around US\$178.5m, between 12 December 2005 and 31 March 2006. Despite notification by another US financial institution and an internal investigation, which confirmed the points to JPMC management and supervisory staff, the bank did not act to prevent a repeat or voluntarily disclose the apparent breach to the Office of Foreign Assets Control (OFAC).

On 22 December 2009, JPMC made a trade loan for approximately US\$2.9m to the bank issuer of a letter of credit when the underlying vessel was subject to embargo for its connection to the Islamic Republic of Iran Shipping Lines (IRISL). JPMC managers and supervisors decided that OFAC should be told but the disclosure was not sent in until March 2010, three days before receipt of repayment of the loan. JPMC also took its time to answer OFAC’s queries about the transaction. The bank’s compliance management were similarly unhelpful in responding to requests for documents relating to a wire transfer that mentioned ‘Khartoum’; they repeatedly denied possession of

the material until OFAC provided a list based on its communications with a third-party financial institution.

Not surprisingly, OFAC deemed these incidents “egregious because of reckless acts or omissions by JPMC”, reiterating in the same paragraph “that JPMC managers and supervisors acted with knowledge of the conduct constituting the apparent violations and recklessly failed to exercise a minimal degree of caution or care with respect to JPMC’s US sanctions obligations.” There is, however, no mention of any action against individuals. Puzzling also is the treatment as non-egregious of another transfer, on 24 May 2006, of 32,000 ounces of gold bullion, worth about US\$20,560,000, for the benefit of an Iranian bank. JPMC failed to disclose the matter to OFAC. Sanctions penalty management – it’s an esoteric art.

Notes

1. www.imf.org/external/pubs/ft/wp/2011/wp11177.pdf
2. Ibid, Table 6, p61.
3. www.ubs.com/1/e/about/news/archive/archive10?newsId=170330
4. <http://hsgac.senate.gov/public/index.cfm?FuseAction=Subcommittees.Investigations>
5. www.fatf-gafi.org/dataoecd/44/9/37101772.pdf
6. www.fatf-gafi.org/dataoecd/31/13/48472713.pdf
7. *Attorney General of Zambia v Meer Care & Desai (a firm) & Ors* [2007] EWHC 952 (Ch).
8. www.fatf-gafi.org/dataoecd/40/13/48426561.pdf
9. Remarks, Mark Harris, ASI Global, 21 January 2011.
10. www.fatf-gafi.org/dataoecd/28/34/48412278.pdf
11. International Labour Organisation (2005), ‘A Global Alliance Against Forced Labour’, www.ilo.org
12. www.fsa.gov.uk/pubs/final/willis_ltd.pdf
13. www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20110825.aspx

Timon Molloy, Editor

What’s in a name? Would a SAR filed under any other name be as sweet?

In Shah & Anor v HSBC Private Bank (UK) Limited [2011] EWHC 1713, the High Court held that identities of staff forming suspicions of money laundering leading to a suspicious activity report (SAR) are relevant and prima facie disclosable. However, the public interest immunity prima facie operates to withhold disclosure of such identities. Whether identities are disclosable in any particular case depends on

balancing the public interest in open justice and the public interest in retaining anonymity. On balance, the judge ordered partial removal of redactions but left open the possibility that AML compliance staff may in some circumstances be required to give evidence in open court. Charles Thomson and Ben Ko of Baker & McKenzie trace the court’s reasoning in the latest chapter of this test case.

Facts

Mr Shah, a businessman with Zimbabwean interests, brought a US\$300m action against HSBC for damages caused by delays in executing four instructions to transfer funds from his account. The bank delayed processing the transfers because it suspected the funds were proceeds of crime and filed a SAR. The Serious Organised Crime Agency (SOCA) did provide consent in each case and the transfers were executed shortly thereafter (save for one instruction, which was cancelled). Mr Shah claims that the losses occurred when an intended transferee, an ex-employee, tipped off Zimbabwean authorities that Mr Shah was being investigated for money laundering. According to the claimant, this caused the Zimbabwean authorities to become suspicious and seize his assets, resulting in alleged losses of over US\$300m.

Procedural history

At first instance, Hamblen J summarily dismissed the claim. He rejected the four ways in which the claimants pleaded their case and held that, in light of the bank's evidence of suspicion, the action would fail unless the claimants showed the bank acted in bad faith.

In the appeal by Mr Shah, HSBC argued that a court would not expect bank employees to give evidence of their suspicion and neither would a court require the bank to disclose evidence of the basis of its suspicions. This was rejected by the Court of Appeal, who considered such an argument as tantamount "to saying that the dispute is completely unjusticiable and that, therefore, the bank must win". Accordingly, the Court of Appeal held that the bank should prove its suspicions through disclosure and calling witness evidence in the ordinary way at full trial.

Protection of identity

In July 2011, the High Court considered whether redactions of names made by the bank to the internal reports and the SARs that were disclosed to the claimants were permissible. Coulson J had to decide three principal issues:

- whether or not the identities of bank staff are relevant to the issues between the parties;
- if the identities are relevant, whether the documents and employees will prima facie attract public interest immunity; and
- if immunity is *prima facie* available, whether the redactions should be permitted in this case.

Are the identities of individual bank staff relevant?

The judge considered that, given the decision of the Court of Appeal that the bank had a case to answer with regard to the basis of its suspicion, the key issue is whether or not the suspicion was genuine.

Like many other banks, HSBC's reporting system required that the suspicion of client-facing employees be first reported to the compliance department before it was internally reported to the Money Laundering Reporting Office (MLRO), which would consider whether the suspicion should be externally reported to the authorities. If the MLRO considered the matter merited further investigation, it would ask the employee to provide an internal memorandum identifying the customer; reasons for suspicion; the activity causing concern; and details of the payments. The nominated SOCA officer in the MLRO would consider the memorandum and make a decision based on it, and any other knowledge he or she had, whether to file a SAR.

The bank disclosed these memoranda, internal reports and other similar documents to the claimant but all of them redacted the names of authors, recipients and anyone else referenced in the document, save for the head of the MLRO, Mr Wigley.

Under the Civil Procedure Rules, standard disclosure requires a party to disclose documents on which he relies; adversely affects his own case; adversely affects another party's case; or supports another party's case. HSBC argued that the identities of staff members neither supported Mr Shah's case nor adversely affected the bank's case. This argument was rejected and the judge held that the redactor must demonstrate irrelevance. The test for relevance is found in the judgment of Sir Thomas Bingham MR in *Taylor v Anderton* [1995] 1 WLR 447. The party seeking disclosure must suffer no litigious disadvantage by not seeing the redacted parts and will gain no litigious advantage by seeing them. The bank failed to satisfy this test. Given that the Court of Appeal had held that Mr Shah is entitled to put the bank to proof as to whether it held a genuine suspicion, an understanding of how, when, and from whom those suspicions emanated is a potentially important factor in the case. Accordingly, Mr Shah would suffer a serious litigious disadvantage by not knowing more about the precise identity of those involved in the reporting process and the genuineness of the suspicion cannot be properly determined without that information. Redacting the identities of every staff member involved, save for one exception, effectively limits who may be cross-examined by the claimant as to the bank's suspicion.

The judge recognised that Mr Wigley is clearly not the only person who can provide helpful evidence – as an officer in the MLRO, he only became involved as a result of the suspicions of others. Mr Wigley may well have formed suspicions of his own after reviewing these reports, in which case his decision to make reports to SOCA may well be shown as genuine. However, the fact that he did not originate these suspicions and the fact that he simply acted on what he read meant that

another scenario, where bank employees further down the chain produced memoranda and reports in bad faith, could not be ruled out. Accordingly, the redacted identities were held to be *prima facie* relevant.

Availability of public interest immunity

In considering the application of the immunity from disclosure by reason of public interest, the court approached the question by reference to two principal factors: whether the documents fell within a class to which the immunity applies and whether the redacted individuals were covered by the public interest immunity.

Both the documents and the bank employees were held to be covered by the immunity and both issues were decided on the same reasoning. The judge considered the position of bank employees reporting their suspicions to SOCA to be directly analogous to police informants and child neglect whistleblowers, to both of whom the public interest immunity has previously been applied. In particular, the judge relied on a passage in the judgment of Waller LJ in *R v H, P, S* [2004] EWCA Crim 3325, which specifically pointed out in relation to SARs: “The suspicious transaction reports would seem *prima facie* to be documents which would be covered by public interest immunity. These reports are in the same category, as it seems to us, as information coming from informants in other aspects of the detection of crime. One can see that it might rightly... be of concern to banks if reports which divulge the identity of employees got out into the public domain... there would appear to be a serious risk of damage being done to the machinery which at present leads to these reports being made.”

The judge considered the fact that bank employees are under a statutory duty, at the risk of prosecution, to report suspicions to the authorities meant that they should be afforded the same immunity as police informants who volunteer information to the police (often for financial gain). It was also noted that SARs are used not only by SOCA but by law enforcement agencies around the world, with the banking sector accounting for 78% of all SARs filed. Coulson J considered it a real possibility that this flow of information would be adversely affected if confidentiality was not the norm as bank employees would err on the side of cautious inaction out of self interest in borderline cases. Accordingly, the public interest immunity was held to apply *prima facie* to bank employees reporting suspicions under the *Proceeds of Crime Act 2002* (POCA).

The balancing exercise

Having established that the identity of bank staff who formed the suspicion is *prima facie* relevant for disclosure purposes, and also having established that the documents and the bank employees themselves are,

prima facie, within a class that are protected by public interest immunity, it fell to the court to decide whether the identity of the individuals ought to be disclosed in this particular case. The court had to balance the competing public interests of open justice against the public interest in ensuring that individuals subject to non-delegable statutory obligations under POCA are free to report their own clients without fear of their opinions being personally attributable to them.

On the one hand, there is a clear public interest in the administration of public justice. This would include the right of an accused to cross-examine his accusers in open court to test their evidence. The judge also noted that the claimant’s case is that his loss is attributable to a failure by the bank to follow his instructions; a failure which is justified by the bank by reference to a suspicion of money laundering. Open justice would therefore appear, “at the very least”, to entitle the claimants to know the basis for the suspicion, who formed it, when and how it was formed.

On the other hand, the court recognised that there would be a real risk of inhibition in the discharge of reporting duties under POCA if those subject to such duties would have their identities revealed, which may take the form of physical intimidation or retaliation. The court noted that a number of other agencies, from the British Bankers’ Association to SOCA themselves, emphasise the importance of confidentiality.

On balance, the judge decided that in this case, the claimants are entitled to a further level of disclosure. However, the judge did make clear that in “ordinary civil cases”, the balance would favour confidentiality, the principal reason being the real risk of inhibition should the identities be disclosed. In this case, the judge pointed to three fact specific factors that tipped the balance in favour of further disclosure, these being the fact that it has now been established that Mr Shah is not (and was not) a money launderer; that the bank employees are not at risk of reprisal; and the long relationship between the claimants and the defendants meaning that the claimant must already have a good idea of the identities of at least some of the individuals involved.

In a further indication that, in an ordinary case, the public interest in confidentiality and protection would outweigh the public interest in open justice, the judge did not order unqualified removal of all redactions. Instead, the judge ordered each bank individual mentioned in the memoranda and reports to be assigned a numbered alias indicating where in the bank they worked with that alias to be disclosed in place of their actual names. This way, their identities would still be protected but the spread of employees forming the suspicion would become clear. For instance, the claimant could then tell whether the suspicion that was fed up

to Mr Wigley was widespread amongst a number of employees (in which case, the risk that one employee reporting out of bad faith, causing the suspicion formed by Mr Wigley to be contaminated, is lower) or whether it was one or two individuals who were repeatedly responsible for escalating suspicions to the MLRO (in which case the risk of bad faith contamination of the suspicion is greater). In the latter case, the defendant's position that Mr Wigley alone can justify the bank's suspicion would be more difficult to sustain and the motives of that handful of employees would be more significant. If required, a further application could then be made to reveal the identities of those few employees.

Comment

This case once again highlights the dichotomy and inherent conflict between contractual duties that are owed to customers and statutory reporting duties owed under POCA. It does appear that Coulson J achieved the correct balance. Plainly, granting AML staff blanket immunity from cross-examination in all circumstances would deny justice to claimants as it would be almost impossible to make out a case against the reporter, which would be tantamount to holding that such cases against reporting institutions are unjusticiable, an outcome very firmly rejected by Longmore LJ in the Court of Appeal. However, it simply cannot be right to haul MLROs and other compliance staff before the courts to justify their suspicions as a matter of course, given that they are under non-delegable statutory duties to report. To do so would lead to a real possibility of widespread reluctance to report.

In practical terms, the court's approach to the public interest immunity should offer reporting institutions, and the reporting officers within those institutions, some degree of comfort. The judge very clearly pointed out that in ordinary civil cases, the public interest in protection of reporting officers would outweigh the considerations of open justice.

However, the case does highlight a side issue – the dangers of AML compliance systems and controls that place too heavy a burden on a small number of individuals. Where suspicion is formed by a small number of people, given the higher perceived risk of them forming that suspicion in bad faith, Coulson J left open the real risk of a court ordering that their identities be revealed and having their suspicion put to proof in the witness box. An institution may seek to protect their compliance staff by ensuring that the reporting system requires a spread of employees to reach an independent view on suspicion and that such suspicion is thoroughly and contemporaneously recorded before it is externally reported. Ensuring that suspicions leading to SARs are comprehensively evidenced and independently formed by a number of staff members will assist a reporting institution that finds itself being asked to justify its suspicions.

Charles Thomson (+44 (0) 207 919 1879, charles.thomson@bakermckenzie.com) is a senior associate and *Ben Ko* (+44 (0) 207 919 1733, ben.ko@bakermckenzie.com) a trainee solicitor with Baker & McKenzie in London

Systematics

“This was always going to be a big year for anti-money laundering, being a decade on from 9/11,” says **Dr Tony Wicks**, Director of AML Solutions at NICE Actimize, sitting across the tea table in Browns Hotel, Mayfair, “but we couldn't have anticipated the additional resurgence of interest in AML arising from other events – the Arab Spring with its sanctions repercussions; ABC [anti-bribery and corruption], a new acronym to conjure; the increased regulatory focus on customer due diligence; and FATCA [the US Foreign Account Taxation Compliance Act]. We've also seen some significant changes in the market, including vendor consolidation and removal of some of the smaller players.”

By way of background, he pauses to sample the house blend before explaining how NICE Systems, the firm's NASDAQ-quoted parent, bought Actimize in 2007

and how Actimize has been actively acquiring businesses as well. “We secured Fortent, which owned Searchspace, in September 2009, and SYFACT, leader in case management and link analysis, in August that year.”

NICE Actimize doesn't just deal in AML, it also provides enterprise solutions for financial crime, fraud and trading compliance. The firm's direct client list includes “10 of the top 10” and spans 250+ banks, “with more than half using the AML solutions”. The company has also been successful in providing its offering through partners like Pershing and FIS, which are able to offer multi-tenant hosted solutions for smaller customers.

“We are seeing stratification in the market; there are banks, mega-banks and smaller financial institutions,” says Wicks, “The market is working top-down, with

the mid-sized and smaller institutions benefiting from the same enterprise AML technologies as those being used by the largest institutions. At the lower end, we are seeing the advantages of hosted AML solutions”.

Currently, the NICE Actimize AML Solutions suite covers transaction behaviour through its SAM (Suspicious Activity Monitoring) product; customer due diligence (CDD), both at onboarding and as part of ongoing review of account behaviour; and fourth generation watchlist filtering (able to cope with non-Roman character sets, transliteration and cultural name matching). The solution also covers processing regulatory and legal requests, like production orders; and regulatory reporting, including of currency transaction reports (CTRs) – “a big operational cost and pain point in the US”.

“Convergence and consolidation are big drivers in the AML market as banks respond to cost pressures,” he says. Asked if there is a growing trend towards financial crime systems, Wicks notes, “We have some good customer examples where this is the case – Bank of Ireland is one, they bought both our AML and fraud products at the end of last year to get a holistic view of activity.” He goes on, “the trend toward ‘Head of Financial Crime’ as a job title is becoming noticeable in conference delegate lists, I think that suggests the two areas are beginning to integrate.”

Bringing systems together under a financial crime umbrella is one change but, at the same time, clients now expect the AML technology to be more tailored to their specific needs, which vary based on the size and type of institution: “Although there are general similarities, the requirements for retail banking and securities are different; one is focused account monitoring and with securities we need to also look at trading activity, where it’s really the combination of patterns that’s interesting.” One major advance that is apparent is the focus not only on activity but also its absence vis-à-vis expectations – for example, in securities, a lack of trading activity associated with the movement of money in and out of the account.

Distinct typologies also apply to insurers and correspondent banking. Traditionally, most AML systems monitor value flows in and out of accounts, looking for anomalies and patterns of risk in, for example, cash and cash equivalent movements. “The focus in correspondent banking is as much on understanding the parties involved, including the intermediary institutions in the chain,” says Wicks.

New bank product lines present additional challenges: prepaid cards, attractive to launderers and recently subject to FinCEN regulation in the US [1], should, ideally, be treated as a cash equivalent transaction type, he notes. Debit and credit cards have not, in the past, been assigned as high a risk rating as cash – issuers

have had an incentive to look closely at the customer since they ultimately underwrite the expenditure. Pre-pay fundamentally changes the relationship with their customer; it essentially removes the credit risk, on top of which, distribution is far more widespread.

“It is now possible, in the UK, to obtain, completely anonymously, a card loaded with up to UK£1,000 – and spend it abroad. They can be bought over the internet, in off licences, corner shops, anywhere”. Issuers, he says, will need “to monitor for clusters of card use – heavy reloading and outlier volumes of sales of cards by merchants.”

False positives are recognised, increasingly, as one of the hidden costs of an AML system purchase. “We’ve done a lot of work with clients on refining the default settings and responding to their requests for tuning.” Optimisation is far from easy. “Contrast it with fraud, which is a measurable problem with cases classified – you have it or you don’t and if you do then sooner or later a customer will tell you. So you can go back, reassess the system and quantify the risk.”

Money laundering is subjective: first, there is the individual decision about whether a behaviour is suspicious enough to raise an alert; and second, if so, should it be disclosed to law enforcement? Both elements are used in gauging system performance but need to be read in context. “Depending on their business needs and risks clients have different strategies, some might be considered to be aggressive, others conservative in the way that they investigate and decide to file. System tuning needs to fit the business need and the risk appetite.”

Progress on reducing false positives is evident, says Wicks. “A couple of months ago, a US client told me that they were getting one in three good alerts and wanted, with a risk-based approach [RBA], to improve results further.” Therein lies the dilemma for financial institutions, he adds – how to design an RBA to monitoring that doesn’t create more alerts than they are able to handle. The question of appropriate resourcing of AML operations and the RBA has not been tested – “even examiners we talk to find it difficult to determine what the right level would be” – so far but it is entirely possible that, faced with the passage of criminal funds through an account, an MLRO might face cross-examination about the number of automated alerts generated and how, and the process of validation or rejection; the interrogation would aim to show that monitoring was inadequate, designed first and foremost with an eye to costs rather than effective detection – managing the alert flow rather than the true laundering risk. “The law of diminishing returns applies here,” says Wicks.

“The RBA means focusing on areas of highest risk. When calibrating the system we look at alerts under

the waterline to see how many more we would have to investigate to find something interesting.” If the alert detection rate remains the same it is necessary to drop the threshold still lower until the ratio accords with the declared risk appetite. “This is evidence which can be presented as part of a regulatory examination,” he says. In practice, larger institutions may have “teams of upward of 20 people investigating suspicious activity alerts,” but that number excludes those working on AML IT, in the regulatory risk functions and data mining/analysis roles. Wicks is slightly worried, he says, when he hears that some AML systems generate so many alerts that they need to be triaged prior to any real investigation. “In my view, the system settings should be accurate enough in the first place to enable a decision on whether a transaction is genuinely suspicious or not.”

Looking more widely, if there is a common theme running through financial crime management currently it is “due diligence”, says Wicks, “It’s in nearly every report one reads, and was central to the Financial Services Authority’s review of banks’ treatment of high

risk scenarios.” [2] In ABC, “half the problem is about due diligence – understanding employees and suppliers” and again, it is central to FATCA compliance. “It’s almost as if financial institutions should be going back to the good old-fashioned basics of knowing and understanding their customers and suppliers.

“Ten years on from 9/11, technology has improved considerably, we can now do more with analytics, work more quickly and on higher data volumes, use computational linguistics and risk-based algorithms, but some of the basics are the same – understanding your customers and how they do business. This is the key to business success.”

Notes

1. www.fincen.gov/news_room/nr/html/20110726b.html
2. www.fsa.gov.uk/pubs/other/aml_final_report.pdf

Tony Wicks (tony.wicks@actimize.com, +44 (0) 20 7255 1065) is Director of AML Solutions at NICE Actimize. Report by Timon Molloy.

Perennial problems – banks and the PEP risk

*The last issue of MLB took in the broad sweep of UK Financial Services Authority criticism of banks’ management of high money laundering risk areas in its latest thematic review [1]. In this article, **Mark Dunn** examines the failings around PEP controls in all their painful detail.*

At June’s annual Financial Services Authority (FSA) Financial Crime Conference in London, the FSA’s Acting Director, Enforcement and Financial Crime Division, Tracey McDermott, announced several new initiatives and reports, one of which was the publication of a thematic review titled ‘Banks’ management of high money-laundering risk situations – How banks deal with high-risk customers (including politically exposed persons), correspondent banking relationships and wire transfers’. McDermott expressed the FSA’s dissatisfaction with the findings of the report and how too many firms are failing to meet the requirements expected by the FSA to mitigate the risks of money laundering and financial crime across the UK financial services sector. The FSA’s damning verdict goes on to say that little has improved in the way banks manage high risk accounts since March 2001 when its investigation into the handling by banks

of UK accounts linked to General Sani Abacha, the former President of Nigeria, uncovered significant failings in financial institutions’ systems and controls. As a consequence, two cases have been referred to the FSA’s Enforcement Division.

Groundwork

The document is the latest in a number of FSA thematic reviews that aim to keep track of how well banks have been tackling their obligations under the Money Laundering Regulations 2007 (MLR). In compiling the review, the FSA selected and met with 27 banking groups in the UK, which, given their business profile, were perceived to be at a higher risk of money laundering. The FSA also visited several large banks’ overseas centres to assess outsourced functions including resources involved in payment processing and processing the alerts generated by transaction monitoring systems. Meetings were conducted with both front and back office staff involved in managing relationships with PEPs and other high risk customers. Prior to visiting banks, the FSA also held meetings with law enforcement agencies, lawyers and other consultants for their views on how well banks were dealing with high risk clients.

The FSA’s main objective for this latest thematic review was to: “Assess whether banks had robust and

proportionate systems and controls in place to identify, detect and prevent the misuse of correspondent banking facilities, meet the requirements to identify the originators of international wire transfers, and reduce the risk of corrupt PEPs and other high-risk customers misusing the UK banking system.”

This article will focus on the section of the review regarding high risk customers and politically exposed persons. The driver in the FSA report for focusing on PEPs is the combating of international corruption and this mirrors work underway elsewhere on tackling bribery. The recent FATF typology *Laundering the Proceeds of Corruption* [2] covers similar ground. However, the FATF document goes into much more detail, drawing together extensive case studies and other material to highlight areas of vulnerability within the global financial services sector. There is also the delayed British Bankers' Association guidance expected on the Bribery Act 2010 adequate procedures, which is currently being reworked.

Evidence

The FSA's findings are highly critical of banks' handling of high risk clients and PEPs, stating that around three quarters of the banks visited, including major financial institutions, are not managing these relationships effectively. The FSA cites their investigation into the management of UK bank accounts held by the former President of Nigeria, General Sani Abacha, which, after three months of digging, concluded in March 2001. At that time the investigation uncovered serious failings in the handling of Abacha's cash: 98% of the US\$1.3bn turned over by accounts in the UK passed through 15 banks where significant control weaknesses were identified. According to the latest FSA report, banks have made few improvements in the management of PEPs and high risk clients since the 2001 review.

Everyone had a policy

The relevant section of the report opens with the findings concerning banks' AML policies and procedures. FSA notes that all the financial institutions visited had in place an AML policy but that some firms' policies had not been updated and still referred to the Money Laundering Regulations 2003. Other firms had invested in consultants to review their policy on hearing that the FSA were to visit, only for the firm to have failed to implement the changes outlined in their new policy document.

PEP recognition

The FSA also comments on the definition of who is deemed a PEP, which varies considerably between some banks. A third of banks visited referred to the PEP definition contained in the Money Laundering Regulations 2007. However, as expected, some banks also include domestic PEPs in their definition

together with more granular segmentation depending on the levels of perceived risk that need to be managed. The FSA is concerned about the lack of understanding in some banks' back office teams of their own firm's definition of a PEP. There is also a rebuke for those firms that considered the reputational risk of working with a potentially corrupt PEP to be more important than whether or not the PEP was actually committing financial crime. The FSA is critical of staff training and they expect firms to consider more bespoke training for those personnel dealing with high risk customers. The absence of such training led to insufficient staff understanding of potential money laundering risks and, in consequence, to poor judgments when working with high risk accounts.

Risk without review

The FSA go on to cover their findings regarding the risk assessment process. The report lists some of the common criteria used to calculate AML risk scores and categorise clients as high, medium or low risk. Such criteria have been in use for years and reflect much of the Joint Money Laundering Steering Group (JMLSG) guidance, including factors such as connections to high risk countries and political figures, the source of customers' funds, their reputation and industry sector, etc. Where a perceived high risk is uncovered, the process of escalating this to Compliance is also referred to.

FSA criticism of banks' risk assessment policies and processes concerns their failure to regularly review and keep their risk criteria up to date. The report states that a third of the banks visited failed to consider the impact of emerging risk factors, including changing country risk (for example, a failure to reflect FATF high-risk and non-cooperative jurisdictions) or a shift in focus by criminals to targeting different products and services offered by banks. The review provides an example at one bank where a customer from a low risk country was rated as such, only for that same client to be subject to allegations of corruption elsewhere.

We assess risk?

The FSA also refers to faults in sectoral risk assessment where banks had rated those industries at greater risk of bribery & corruption, such as pharmaceuticals and extractive industries, as low risk on the basis that these sectors were regulated. The FSA points out that these industries are not regulated for AML purposes. Similarly to the feedback on AML policies and procedures, many staff were found to not understand how their firm's risk assessment process worked or were unaware that such a process existed. A number of banks had also either conducted their first risk assessment or changed an account's status from low to high risk just before the FSA came into the bank to review their systems and controls. Customer due diligence (CDD)

files also lacked the supporting evidence used to determine why accounts had received particular risk ratings.

Deficient customer files

The FSA looked at banks' customer due diligence (CDD) processes in more detail as part of the review, breaking the report down to reflect different parts of the customer take-on process. Identifying and verifying the identity of customers opening accounts was the first area of CDD to be considered. Most banks had robust PEP screening processes in place; however the FSA points out that some banks did not consider the ongoing risks posed by customers who had once been PEPs but were no longer politically exposed. The fact that a political figure had left office didn't necessarily mean their previous high risk status as a PEP had changed. Customer due diligence files were also found to contain missing information which had not been addressed at the account review stage.

Undue influence

The FSA also comments on risky business practices that were still in use, for example, where the CDD process was influenced by personal introductions or business acquaintances. At one bank, the CEO appears to be introducing a number of new clients to the firm without the AML team questioning his judgment or the clients' integrity. Similarly, where banks have opened accounts for clients from other overseas business units or branches within the group, they were unable to demonstrate that UK-equivalent CDD standards had been applied to the customer take-on process.

Record (up)keeping

More than half of the banks visited by the FSA had also failed to keep their CDD records up to date. There were some accounts where no formal evidence had been obtained to verify the customer's identity. Customer files had also not been updated to reflect changing risk factors associated with the account. The report goes on to mention that three banks only updated their CDD files shortly before the FSA were due to visit.

Ultimate owner unknown

The perennial issue of identification of ultimate beneficial owners is also picked up by the FSA review. A third of the banks visited did not have in place sufficient procedures to establish their customers' ownership and control structure. Where the ownership structure was considered overly complex, banks had not questioned their customers to establish why this was the case. The FSA's findings also highlight the problem of trying to identify indirect beneficial owners, often out of sight behind the customer's business. A fifth of the banks visited failed to identify these individuals and the FSA points out that as a result the banks did

not know who their client's ultimate beneficial owner was. Essentially, the report states, not knowing who the ultimate beneficial owner is breaches banks' legal obligations and impacts their ability to determine any underlying risk of money laundering or financial crime.

Commercial databases do not suffice

The process for screening customers to identify if they are PEPs or not is the next part of the CDD workflow to come under scrutiny in the FSA report. The FSA stresses that firms should not rely on screening their clients' names against commercial PEP lists alone but should complement this type of data with other publicly available information to help establish money laundering risk.

Wealth, funds and reasons

The review continues through the CDD process and considers the steps banks are taking to establish the nature and intended purposes of the business relationship and the customer's source of wealth and funds. The FSA is critical of banks failings in this area and indicates that over 40% of the institutions visited did not adequately obtain information from the customer. Clients were not being questioned on why they had chosen to bank with the financial institution and the reasons for requesting certain products or services that did not seem to make sense. The FSA goes on to stress the legal obligation banks have to establish a customer's source of wealth and funds. In the event, customers were either not asked to provide these details or were not questioned further when insufficient information was given. The FSA's findings also highlight instances where banks appeared to accept investments that were derived from the proceeds of crime. Ultimately, the report states, too much reliance was placed on what the customer said or the Relationship Manager thought, even when there were "serious allegations of criminal conduct".

Holes in the due diligence

The FSA reviewed banks' enhanced due diligence (EDD) processes and although EDD was a key process at client take-on, there were still flaws in this process uncovered by the report. Despite conducting EDD checks, the FSA notes that a third of the banks visited failed to analyse and act on the information retrieved. One bank branch whose parent office charged them for running their EDD checks stopped requesting these reports due to the cost. Over a quarter of the banks visited failed to act on allegations of corruption linked to some of their clients, as lack of criminal convictions was seen as a sufficient reason to proceed with an account. Alternatively, if the client held an investment visa, this was considered safe enough ground to take on the customer. The FSA also references examples of client Relationship Managers deliberately

withholding potentially damaging information on their clients from the Compliance team in the bank.

On CDD record keeping procedures, before their visit, the FSA informed the banks reviewed that they wanted to see the CDD files for certain high risk customers. The outcome was that a third of the banks met were unable to provide the CDD records requested. Information was either incomplete, scattered across multiple databases, held by other branches outside the UK or simply lost.

Conflict escalation

The FSA goes on to report on the aspects of banks' AML systems and controls that cover approval and business relationships. This section of the report focuses on the role and responsibility of senior management and the Money Laundering Reporting Officer (MLRO), escalation procedures and the quality of the information used to reach business decisions concerning a high risk client. The FSA is critical of the lack of clear audit information detailing why a certain business decision was taken on an account. There are also concerns raised about the lack of a clear escalation process in some banks. In some cases, Relationship Managers had allocated a low risk rating to avoid the escalation procedure. Accounts that had been given a high risk rating and required sign-off for business to proceed were also being dealt with by junior members of Compliance staff. A few banks had neglected to implement an escalation process at all. At a quarter of the banks visited, the quality of the information presented by the Relationship Manager to Compliance was considered poor. The FSA comments on the conflict of interest a Relationship Manager has between providing their Compliance team with full and accurate information on the account, and their desire to secure the customer's business. In some cases, MLROs were not given sufficient authority to challenge the Relationship Managers on the information they had been given, effectively undermining the bank's AML systems and controls.

Remote management

The FSA signs off this section of the thematic review with a look at the risk appetite, culture and resources focused on tackling AML compliance. Regarding adequate risk management, the FSA states that the risks focused on by more than a quarter of the banks visited "were of limited relevance to AML". The report goes on to say that at nearly half the banks visited the FSA observed a "poor AML compliance culture" and an "apparent lack of leadership on AML issues from senior management." Even the larger banks do not escape unscathed as at a fifth of the banks visited "Group MLROs were too remote from their business units and sometimes had a poor awareness of the group's

highest risk relationships". At one bank, the MLRO didn't see the point in gathering CDD information as the culture was such that "customers would be taken on even if they were subject to serious allegations of criminal activity".

Concern for reputation over crime

The FSA also comments on the higher priority banks appear to give to mitigating reputational risk and the concern that a client may have been involved in a public scandal. There is a sense that managing reputational risk is considered more important by banks than, what the FSA terms, "criminality risk" - whether the customer is actually corrupt, engaged in financial crime and trying to launder the proceeds of that crime through their bank account. An example is given where a third of the banks visited often discounted serious allegations against their clients as it was unlikely that criminal charges were to follow. This led to very high risk customers being taken on because the reputational damage to the bank was perceived as low. Other banks led on credit risk and were willing to conduct business with clients as long as their risk rating was sound, regardless of other risk factors.

Beyond take-on

The FSA's findings on high risk customers and PEPs is completed with a review of the approach taken by banks to enhanced monitoring of high-risk relationships. Smaller banks were found to have inconsistent processes in place. One small bank had yet to apply the Money Laundering Regulations 2007 and adopt a risk-based approach to AML. Another small bank had failed to respond to a series of transactions in an account that was expected to handle deposits on an income of UK£20,000 to UK£30,000 and in the event had received over UK£3m in the three years since the account was opened. The FSA stress the importance of the Relationship Manager in the transaction monitoring process given their regular engagement with clients. However, almost half of the banks visited neglected regular reviews of their high risk or PEP relationships.

More guidance

In common with other thematic reviews, the report also highlights examples of good and poor practice observed during the FSA's onsite visits. The FSA goes on to explain that this information, alongside other examples from previous thematic reviews, will form proposed guidance as part of the new 'Financial Crime: a guide for firms' document, which is currently out for consultation until 21 September. [3] This guidance joins a plethora of existing material from the Joint Money Laundering Steering Group, Financial Action Task Force, Wolfsberg and the Ministry of Justice. Although the FSA states that their proposed guidance is

non-binding and is not intended to compete with other guidance material, they make it very clear that, once the consultation phase has passed and the new guide is completed, firms are expected to be aware of the content and consider, as appropriate, how to apply some of the material in implementing effective policies and controls. So there is plenty of work ahead for the AML teams as they digest this latest thematic review. There is also no sign of relief in the long term as Tracey McDermott stated in her speech at the FSA's annual Financial Crime Conference, when introducing the document's publication whilst heralding the incoming Financial Conduct Authority (FCA): "This report and, indeed, our mortgage fraud report are the product of a style of intensive, intrusive supervision that will be carried into the FCA."

And the report itself stresses that: "Given the nature of our findings, the management of high-risk customers,

including PEPs, will remain a significant focus of our anti-financial crime work for some time to come."

Notes

1. See 'Incredible indifference to 'credible deterrence'', *MLB*, July/August 2011; 'Banks' management of high money-laundering risk situations: How banks deal with high-risk customers (including politically exposed persons), correspondent banking relationships and wire transfers', www.fsa.gov.uk/pubs/other/aml_final_report.pdf
2. www.fatf-gafi.org/dataoecd/31/13/48472713.pdf
3. www.fsa.gov.uk/pages/Library/Policy/CP/2011/11_12.shtml

Mark Dunn (+44 (0) 20 7400 2984, risk@lexisnexis.co.uk) is Market Planning Manager, Risk & Compliance, LexisNexis.

Derrick ponders... Ricky's Risks

The UK has long been a proponent of the risk based approach (RBA) to anti-money laundering. Derrick Paterson discusses the minimum requirement for a process to be risk-based.

The risk based (or risk sensitive) approach was an important step forward for the anti-money laundering and counter terrorist finance (AML/CTF) regime. What is its role? The reason normally given is that it allows firms to concentrate resources where they will do the most good ("getting the most bang for the buck") but it is important to understand its limitations. It cannot be error-free and it can only be as effective as, one, the analysis that underlies it and, two, the effectiveness of those who implement it.

Ricky, the MLRO of Cabbage LLP, is called to a meeting with Graeme, a senior partner. Graeme has earned a reputation for being commercial and often lobbies Ricky to reduce the burden of the AML procedures on the firm. Graeme tells Ricky that a client has shown him an article entitled "Jacques' Jackets" [1] that says that the firm could have a simple, single client due diligence (CDD) procedure. He asks Ricky to explain why Cabbage needs its existing tripartite (low, normal and high) system.

Ricky does some research on which to base his response. The FATF's Recommendation 5 introduced the risk sensitive approach. It talks about performing CDD on a risk sensitive basis, with high risk categories

requiring enhanced due diligence (EDD) and lower risks only simplified due diligence (SDD). Recommendation 15 indicates that internal policies, training and audit should be appropriate to the risks.

The EU Third Directive goes on to talk about risk-based measures to understand the client's ownership and control structure and to verify the identity of a beneficial owner. It talks about risk-based procedures to spot Politically Exposed Persons (PEPs) and performing due diligence on existing clients.

The Money Laundering Regulations 2007 (Regulation 20) list the policies that should be established on a risk sensitive basis: "(a) customer due diligence measures and ongoing monitoring; (b) reporting; (c) record-keeping; (d) internal control; (e) risk assessment and management; (f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures."

Section 4 of the guidance issued by the Consultative Committee of Accountancy Bodies (CCAB) talks of targeting resources and effort to where the risk is greatest. So that senior management manage and mitigate the money laundering and terrorist finance risks, it needs to establish a risk profile for the firm. There is agreement on how this should be done. The Joint Money Laundering Steering Group's (JMLSG) guidance (4.2), the Office of Fair Trading's (OFT) guidance (5.3) and Her Majesty's Revenue and Customs's (HMRC) guidance (6.1) are almost identical.

The steps are to:

- Identify the money laundering and terrorist finance risks facing the firm;
- Assess the risks posed by: customers, products and services, delivery channels (such as in person/online/through third parties), and geographical areas of operation;
- Design and implement appropriate controls to mitigate the risks identified;
- Monitor the effectiveness of the mitigation process;
- Document what has been done and the reasons for doing it.

Since the risks associated with products and services, client types and jurisdictions will change, the JMLSG recommends formal and regular reviews. As it says (4.29), “Risk Management is dynamic.”

CCAB 4.6 says that risk-based procedures can never be error-free. JMLSG 4.5 quotes from a letter to the chairman of JMLSG from the UK Financial Services Authority (FSA), which makes clear that the FSA “... recognise[s] that any regime that is risk based cannot be a zero failure regime”.

There are two ways to construct a risk-based system. The first approach looks at generic risk: the geographic risk for, say, Nigeria is the same for all firms and the industry risk associated with oil extraction businesses is the same for all firms. This approach makes sense. Nigeria probably has a higher risk than France. Oil extraction probably has a higher risk than manufacturing greetings cards.

The second approach looks at risks specific to the firm. Consider Turnip plc, which deals exclusively with Nigerian oil extractors. To a regulator, Turnip may have a high risk profile. But should Turnip treat all its customers as high risk? It probably has a very good understanding of the players in the Nigerian oil industry, their reputations and the people associated with them. It can decide on other, specific criteria to identify its high risk customers – for example, it might treat as high risk those entities with which its other clients appear unwilling to have dealings. Should Turnip be approached by a French greetings card manufacturer, it might treat it as high risk because of Turnip’s lack of knowledge and experience of the jurisdiction and industry. Turnip might ask the question, “Why come to us when we have no experience?”

Thus Turnip’s MLRO might construct a CDD process that has 3 levels (Low, Normal and High). The Normal process would need to take account of the high risk profile of Turnip’s client base and might be similar to the High risk process for a firm with a more staid client base. Turnip’s Low risk process would be lighter touch and its High risk process would be more exacting.

But what about a firm that is not interested in making the commercial savings available from a lighter touch regime for lower risk customers? Could the firm have a single CDD process? I believe so. But there are two key provisos.

First, the process (be it CDD or any other process) must act as if all customers and situations are the very riskiest that they could be. Thus the little old lady, whose only income is her state pension, is treated as if she were a potentate from a dodgy country. To most firms this will be unappealing – because of costs and because of the PR impact of complaints from little old ladies. But some will have a client base that makes this an acceptable process.

Second, the firm must have a way to identify and document the risks associated with the customer. This is an unavoidable part of knowing your customer. It is not acceptable to place on file a pre-printed list of general risks associated with all clients – the risks must be validated against the client and inappropriate risks removed and additional risks added.

So what does Ricky say to Graeme? Cabbage provides to its clients a wide range of services, which may be delivered standalone or bundled together to give a tailored service. Cabbage has a large number of individuals and entities as clients. Both types of clients are a mixture of UK and overseas-based. Thus, Cabbage has a complex risk profile. I would expect there to be a significant difference in the verification evidence collected for a low risk client and a high risk client. It will still be necessary to conduct a risk analysis on each client and document that analysis. It would also make sense to assign each client a risk category – as a reminder to partners and staff that different clients are associated with different levels of AML risk. Opting to collect the same evidence for all clients (both at initiation of a relationship and ongoing) may result in substantial additional work.

This case study typifies many issues facing the MLRO. There are legal requirements but these are not laid out as hard and fast procedures – there is flexibility to meet commercial needs. The MLRO carries legal and regulatory responsibility for the decisions but senior management (who lack AML expertise) may need detailed briefings before they understand the full effects of making “simplifying” decisions.

Notes

1. See *MLB* July/August 2011.

The purpose of this article is to pose questions and instigate discussion. It does not represent advice.

Derrick Paterson Dip (AML) FCA MICA is Director of *Ophelimity Limited*, an independent AML consultancy. He may be reached on +44 (0) 7732 744 56, derrick.paterson@hotmail.co.uk

I am not a number, I am a free man

Devotees of the 1960s psychedelic drama series “The Prisoner” will recognise the title of this article as the refrain of the British agent known only as Number Six, writes Sue Grossey. The dehumanisation of individuals, and their reduction to homogeneous units, has long concerned us and it is the focus of a recent report by the Financial Action Task Force.

“Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants” [1] was published in July 2011 as an outcome of the Financial Action Task Force’s (FATF) plenary meeting in Mexico City in June 2011. [2] Its main sources of information were a questionnaire circulated to FATF members in 2010 (to which 52 responses were received), a study of the relevant literature, and a workshop for FATF and Egmont [3] experts in South Africa in November 2010.

The concept of trafficking in human beings is not a new one, although I should imagine that most of us hoped that the American Revolution and the Slavery Abolition Act of 1833 had put paid to the trade. We were wrong. According to the campaigning organisation Anti-Slavery [4], there are currently millions of men, women and children around the world living in slave-like conditions, where they are:

- forced to work, through mental or physical threat;
- owned or controlled by an “employer”, through mental or physical abuse or threatened abuse;
- dehumanised, treated as a commodity, or bought and sold as “property”;
- physically constrained, or have restrictions placed on their freedom of movement.

The third bullet point – the sale of human beings as a commodity, and the subsequent laundering of the proceeds from that trade – is the subject of this FATF report.

Trafficking versus smuggling

The report deals with both trafficking and smuggling, so terminology is important. According to Anti-Slavery: “People smuggling is the illegal movement of people across a border for a fee. It can be dangerous and expensive, but on arrival in the country of destination the smuggled person is free. People trafficking is fundamentally different as the trafficker is facilitating the movement of that person for the purpose of labour or sexual exploitation. This begins when they arrive at the destination and always involves violence, deception or coercion.” Of course the two trades can become blurred: often people will think that they are going to be smuggled, and in fact they are deceived into being trafficked.

The distinction between the two is further obscured by their shared profit motive, as explained in the FATF report: “The main difference is in the exploitation aspect of trafficking that is absent from the smuggling operation. However, making a profit is the main goal of both traffickers and smugglers.”

And it is quite some profit: statistics from the International Labour Organisation (ILO) suggest that 2.5 million people are currently being trafficked in the world, providing a total illicit profit of about US\$32bn annually. According to research done by the American Congressional Research Service in 2010, “the globalisation of the world economy has increased the movement of people across borders, legally and illegally, especially from poorer to wealthier countries. International organised crime has taken advantage of the increased flow of people, money, goods and services to extend its own international reach.” The FATF report reveals the inadequacy of our response to this escalating crime: “The US Department of State gathers statistics on the number of prosecutions and convictions around the world for human trafficking. In 2009, there were 5,606 prosecutions and 4,166 convictions for trafficking in persons.”

Quantifying the scale of people smuggling (and our success in combating it) is even more troublesome, as a successfully smuggled individual will of course not report the crime. In its 2010 Transnational Organised Crime Threat Assessment, the United Nations Office on Drugs and Crime (UNODC) estimated that each year about 55,000 migrants are smuggled from Africa to Europe and that about 3 million people enter the USA illegally through its border with Mexico. The FATF report reveals that “in 2009, in the US, 2,268 investigations were initiated on migrant smuggling (566 on human trafficking) and 1,338 convictions were pronounced in 2009 (165 for human trafficking).”

Calculating the profits from people smuggling is very difficult. According to the UNODC, “the income of smugglers operating from Africa to Europe amounts to US\$150m annually and smugglers operating from Latin America to North America are believed to earn about \$6.6bn each year.” It is perhaps more meaningful to look at the fees charged for smuggling:

- Mexico to US: up to US\$3,500 per individual;
- Brazil to US: up to US\$18,000 per individual;
- China to US: up to US\$70,000 per individual;
- Albania to western Europe: up to €6,000 per individual;
- Central Asia to western Europe: up to US\$10,000 per individual.

Where there's muck, there's brass, and where there's brass, there's laundering

According to research done by the UNODC – and not surprisingly, given the figures above – people trafficking is the third largest source of income for the organised crime groups after drug and arms trafficking. A movement into people trafficking is a good business decision for many reasons, as explained by the FATF report: “According to Europol, as human trafficking is one of the most lucrative of organised crime activities, it attracts all levels of criminal interests from the low level trafficker, the smaller groups operating on a more permanent basis through to the international networks dealing with large numbers of trafficked victims with connections in the source, transit and destination countries. Certain aspects of trafficking in Europe, for example, are largely supported by Russian and Albanian gangs and by the Italian mafia, whereas trafficking in Asia is largely controlled by Chinese criminal groups and the Japanese Yakuza. These international groups increasingly interact with local networks to provide transportation, safe houses, local contacts, and documentation. The traffickers are often also involved in other crimes such as drug smuggling/dealing. They use trafficked human beings as drug couriers or they force them to perpetrate other crimes like theft.”

The shady world of human trafficking and people smuggling was brought to our attention in the UK in 2004 by the Morecambe Bay cockling disaster. A group of Chinese people was harvesting cockles off the Lancashire coast when they were cut off by the incoming tide. Eventually 23 bodies were recovered from the water. Investigations showed that the workers were illegal immigrants from China, not trained for the dangerous work they were doing, and in 2006 their gangmaster was sentenced to 14 years in prison for immigration offences. The disaster led to the passing of the *Gangmaster Licensing Act 2004*, which required the formation of the Gangmasters Licensing Authority.

As demonstrated by the cockle pickers, target industries for illegal workers can be otherwise entirely legitimate, such as farming and construction, and the manufacturing and service sectors. Other industries attractive to those placing illegal workers are those that rely on cheap or seasonal labour, or that involve difficult and dangerous jobs. Added to these are what Interpol terms the “invisible” sectors of domestic work and entertainment. As the FATF report points out, “there can be a blurring of the distinction between [smuggling] and trafficking where those involved can start as individuals voluntarily engaging in the process of illegal entry into the destination jurisdictions but who then get exploited by criminal gangs taking advantage of their vulnerability arising from their

illegal entry into the country concerned.” This is perhaps most often the case for women who are promised jobs in the catering and hospitality sectors, and are then forced to work in the sex industry instead.

The FATF report goes into further detail about the profile of the smuggler and of the trafficker, and the favoured routes for both trades, but the interest for *MLB* readers lies in the financial aspect of the crimes. Given the nature of both businesses, it is not surprising that they are cash-intensive activities: people looking for a new life, or coercing others into one, prefer the anonymity of a cash payment. Therefore “the use of cash-intensive businesses to launder the money is a major trend. Canada [one of the respondents to the FATF’s questionnaire] gave the example of car dealerships and convenience stores as well as import/export companies. The use of casinos has also been reported... The use of Money Service Businesses is also common [and] the hawala or other informal banking systems and cash couriers are also used.”

Organised crime groups have always been quick to spot linked opportunities, and the UK response to the FATF questionnaire noted a new development: “[There is] the trend of criminals who facilitate the trafficking of individuals from Eastern Europe, confiscate identity documents from those individuals when they arrive in the country and open bank accounts to gain access to credit through overdrafts, loans and credit/debit cards. In addition the accounts are used to [fraudulently] obtain tax credits and crisis loans. Debt accumulates on the accounts and is not paid back to the lender. When the lender tries to contact the account holder to demand payment, the organised criminals send the trafficked individual back to their home country and the lender loses their money.”

SARs and people trafficking/smuggling

According to the FATF report, the number of SARs that identify people trafficking or smuggling as the suspected predicate crime is low. For instance, out of 2,764 SARs submitted in Spain in 2009, 84 (3%) mentioned people trafficking/smuggling. And out of 579 cases passed to law enforcement by the Canadian financial intelligence unit (FIU) in 2009/2010, eight (1.4%) were connected with people trafficking/smuggling. Yet it is the third most profitable business for organised crime groups.

This low level of awareness of the dangers and ubiquity of people trafficking and smuggling is perhaps a result of what the FATF report terms “judicial focus”: “Trafficking in human beings is... frequently hidden within other criminality such as prostitution, illegal immigration, etc. This often results in instances of trafficking not being investigated or recorded as trafficking cases. Very often the focus of criminal justice practitioners is on the migrants rather than

their smugglers. [This means that human trafficking/smuggling] has established a reputation for being 'low risk – high reward' [not least because of] the difficulty in securing prosecutions due to the practical challenge of investigating crimes across international borders, or the difficulty in obtaining evidence from trafficking victims.”

Red flags

The FATF report helpfully provides several detailed case studies – which are ideal for staff training – and comprehensive lists of “red flag” indicators for various target sectors. Many of these are familiar, as they serve as indicators of money laundering for any cash-intensive criminality, but the more specific ones are worth highlighting here:

Red flags for banks

- the same mobile number, address and/or employment references used to open multiple accounts in different names;
- frequent money transfer to trafficking/smuggling “risk” countries;
- concentration of “risk” nationalities among the opening of accounts;
- numerous incoming money transfers or personal cheques deposited into business accounts for no apparent legitimate purpose.

Red flags for money service businesses

- small amounts sent with high frequency to unconnected persons;
- frequent transfers to “risk” countries;

- multiple customers conducting international funds transfers to the same overseas beneficiary.

Red flags for high value dealers

- transactions funded with cash;
- goods purchased for personal export to “risk” jurisdictions.

People trafficking may seem like a distant and theoretical crime, but the degree to which organised crime groups have become involved – deriving upwards of US\$32 billion from it – suggests otherwise. On the contrary, individuals who have been at best smuggled and at worst trafficked are likely to form part of our everyday communities: they live and work among us. We cannot ignore them, and the misery caused to them and their families, just so that criminals can earn and launder another dirty dollar. As George Bernard Shaw wrote: “The worst sin toward our fellow creatures is not to hate them, but to be indifferent to them: that’s the essence of inhumanity.”

Notes

1. www.fatf-gafi.org/dataoecd/28/34/48412278.pdf
2. The first joint plenary meeting of the FATF and GAFISUD – the FATF-style regional body of South America (www.gafisud.info).
3. The Egmont Group is the “trade body” for Financial Intelligence Units (www.egmontgroup.com).
4. www.antislavery.org/english/

Susan Grossey may be contacted on +44 (0)1223 563636, susan@thinkingaboutcrime.com

Wide but not unbounded – the definition of criminal property

The principal money laundering offences under the Proceeds of Crime Act require the property at issue to be criminal, which can prove an unexpected stumbling block for the prosecution. Shula de Jersey of Russell Jones & Walker explains.

The three principal money laundering offences under the Proceeds of Crime Act 2002 (POCA) are focused on dealings with criminal property:

- under s327 POCA it is an offence to conceal, disguise, convert, transfer or remove from the jurisdiction *criminal property*;
- under s328 POCA it is an offence to facilitate the acquisition, retention, use or control of *criminal property*;

- under s329 POCA it is an offence to acquire, use or possess *criminal property*.

Criminal property is defined in s340 POCA as property that constitutes a person’s benefit from criminal conduct or it represents such a benefit (in whole or in part and whether directly or indirectly), and the alleged offender knows or suspects that it constitutes or represents such a benefit. Criminal conduct is defined as conduct which constitutes an offence in any part of the United Kingdom or would constitute an offence in any part of the UK if it occurred there.

The meaning of criminal property has been the subject of a number of Court of Appeal decisions, most

recently *R v Amir and Akhtar* [2011] EWCA Crim 146. The detail of that case, and two other recent decisions, was the subject of an article in the May 2011 issue. [1] The interpretation of the meaning of criminal property by the Court of Appeal is clear: it has the same meaning in respect of all three principal money laundering offences as set out in s340: “It does not embrace property which the accused intends to acquire by criminal conduct... Property is not criminal property because the wrongdoer intends that it should be” [Lord Justice Elias in *Amir and Akhtar*]. The property must be criminal property at the time of the offence: “the natural and ordinary meaning of s328(1) is that the arrangement to which it refers must be one which relates to property which is criminal property at the time when the arrangement begins to operate on it. To say that it extends to property which was originally legitimate but became criminal only as a result of carrying out the arrangements is to stretch the language of the Section beyond its proper limits” [*R v Geary* [2010] EWCA Crim 1925].

In *Loizou* ([2004] EWCA Crim 1579) the court ruled that no offence under s327 was made out as the property was not criminal at the point of transfer. In giving Judgment, Lord Justice Clarke gave the following example to illustrate the point: “Suppose I receive pay as a judge in cash, that cash is not criminal property. Suppose I use that money to pay Hughes J for a car which I know to be stolen. In that event, I of course commit the offence of receiving goods knowing them to be stolen. I do not, however, commit the offence of transferring criminal property because the property I am transferring, namely the money which I earned as judge, is not criminal property. Of course in the hands of Hughes J as the seller of the stolen car, the cash is criminal property because it constitutes a person’s benefit from criminal conduct within s340(3) (a) which he knows or suspects constitutes such a benefit within s340(a)(b). Does Hughes J commit an offence under s327(1)? The answer is plainly no, because he has not concealed, disguised, converted or transferred criminal property. He has simply received what is now criminal property and retained it. s327(1) does not create an offence of receiving criminal property.”

In the example given by the court it is likely that the receiver of the monies paid for the stolen vehicle would be committing an offence under s329 POCA of possession of criminal property. The example does however illustrate the point that in money laundering cases the property in question has to be criminal property at the time of the offence.

A further illustration as to whether property was criminal property was argued in a case in which I was involved. Mr X was charged with conspiracy to use

criminal property with Mr Y. The case concerned the sale by Mr X of promotional CDs to Mr Y, who subsequently uploaded the CDs to a music file-sharing site. Promotional CDs are distributed by record companies in order to enable the broadcasting of material either before or contemporaneously with publication so as to promote particular music and artists. Such CDs often have ‘not for resale’ conditions impliedly attached. In order to succeed on the charge, the prosecution had to prove that the CDs were already criminal property at the time that Mr X used them, ie, at the point of sale to Mr Y. The difficulty the prosecution faced was proving that the CDs were criminal property in the hands of Mr X. By virtue of his role as a DJ and music producer, Mr X received the promotional CDs unsolicited from record companies. These were therefore lawfully obtained by Mr X and at the time the CDs were sold to Mr Y they were not criminal property. Whilst the CDs may have become criminal property as a result of the sale at this stage, Mr X’s use had ended as his discernible use was the sale. The prosecution recognised this difficulty and did not proceed with the charge of conspiracy to use criminal property.

As identified in the May 2011 article, there has been a trend towards the prosecution of the principal money laundering offences. Such offences can be attractive to prosecutors as frequently it can be relatively easy for the prosecution to prove the elements of the offence, particularly as there is no requirement to prove that the property in question is the benefit of a particular or specific act of criminal conduct. The prosecution is required to prove the property constitutes benefit from criminal conduct and can rely on circumstantial evidence from which inferences can be drawn that the property in question has a criminal origin. The further attraction is that the maximum sentence for a money laundering offence is 14 years. In fraud-related cases this is a higher maximum sentence than the underlying fraud offence; the maximum sentence for offences under the Fraud Act 2006 is 10 years. As in the *Amir and Akhtar* case it was readily acknowledged that on the facts it was probable a conviction for an offence under the Fraud Act would have been achieved yet the prosecution chose to charge the money laundering offence. As the recent decisions demonstrate, the law is clear as to the definition of criminal property and it must be criminal property at the time of the act.

Notes

1. ‘North and South – English and Scots case law’ by Jonathan Fisher QC, *MLB* May 2011

Shula de Jersey (+44 (0) 20 7657 1766, s.d.jersey@rju.co.uk) is a solicitor in the Business Crime & Regulation Department at Russell Jones & Walker.

Usury – an Italian money-spinner

If money is tight and the bank refuses to extend credit, there is always an alternative. Rates are bound to be high, writes Lee Andendorff from Lucca, but in Italy there is also a high probability that both funds and lender are criminal.

Earlier this year the search of the house of a notorious octogenarian loan shark in Naples made headlines in Italy. It was newsworthy not due to his reputation as one of the city's most prominent usurers, but because of the amount of money investigators found hidden in his home: over €5m in cash stashed behind tiles and false walls together with hundreds of thousands of euros in debtor cheques. The case illustrates what Italian authorities have been aware of for some time: usury is not only alive and well in the Bel Paese, but thriving and producing enormous profits that are not easily deposited in a bank.

Usury has a history as old as that of banking, and, historically, it has benefited from economic recession. Access to credit tightens and both businesses and individuals find themselves stretched to pay the bills, easy prey for loan sharks or credit schemes operating at the limits of legality.

The most recent downturn is no exception. While Italy has seen the most severe drop in GDP of all industrialised nations, usury has boomed, rising a staggering 126% in the first four months of 2011 compared with the same period in 2010, according to the Italian Taxpayers' Association. The Legality Network of anti-racket and anti-usury organisations, launched in late 2010, estimates that of the 165,000 commercial activities and 50,000 hotels and restaurants to close their doors between 2006–2009 in Italy, 40% had fallen victim to over-indebtedness and usury.

This financial service has meanwhile evolved into a complex business, offering an ideal mechanism for money laundering according to Professor Ranieri Razzante, head of the Italian association of anti-money laundering professionals AIRA, and consultant to the parliament's anti-mafia commission. "The simple neighbourhood usurer has been largely absorbed by organised crime. Money laundering through usury is a double gain for these organisations. They lend money at disproportionate rates of interest and this of course makes them money; lending 100, for example, earns you 300. The second bonus comes from the fact that the 100 loaned by the usurer, who is part of a criminal organisation, comes from, say, a drug deal or a prostitution racket. That money needs to be inserted into the economy somehow, and usury provides a means for that," he said.

And there are, of course, a lot of illicit earnings in Italy to launder. The annual report of SOS Impresa, a

branch of the country's national business association 'Confesercenti', devoted to extortion and usury protection for businesses, estimates that the country's combined mafias are turning over €135bn a year. This total derives principally from the drugs trade, but significant sums are made by subverting environmental sectors (such as waste collection) and from usury and extortion. The report, with data based on police investigations and asset seizures, estimates that usury is worth some €15bn a year to the criminal organisations, and that around 200,000 businesses are affected by it. An average loan starts out as €60,000 and debtors are mainly small businesses, paying around 10% a month interest.

"Obviously, any estimate we have [of mafia earnings or usury] is approximate and is open to discussion, but the thing we are sure of is that we are talking about vast sums of money," said SOS Impresa national president Lino Busà. He said that laundering illegal earnings remained one of the biggest 'management' problems for the mafia and that usury represented a relatively low-risk way of channelling these funds into legitimate businesses. "Usury as a crime is de-penalised. While extortion and drugs can get you a long time in jail, it's not the same for usury and the risks are relatively low. At the same time it permits the circulation of great sums of money," he said. Mr Busà added that while usurers linked to organised crime were growing at the fastest rate, modern-day usury included a subclass of professionals and banking operators at the legal limits of the system, interested in acquiring property or shares in a company as the outcome of their loan activity.

Examples abound. In one operation, dubbed 'Usurama', Italy's finance police arrested six people in May this year, uncovering a scheme that was based on loans to indebted businesses and professionals across Rome and the surrounding regions. The group specialised in gaining credit for their 'clients' through fraudulent declarations to banks backed by counterfeit documents; corrupt bank managers 'facilitated' the account-opening and financial transactions. The scam had accumulated a network of 56 properties, 66 bank accounts, numerous cars and shares in 10 different enterprises with loans worth €12m and interest rates that could reach over an incredible 4,500% a year. More than €5m was apparently laundered through the scheme. One of the arrested gang members is also being investigated for driving an entrepreneur to suicide.

Despite intense activity by Italian law enforcement over recent years, usury remains a difficult crime to uncover, particularly as victims are generally reluctant to report the problem. Just a few hundred cases come

to light every year although a network of anti-usury associations and a special state-administered fund for the prevention of usury attests to the diffusion of the problem across the country.

A loan with a 'higher than reasonable' interest rate is considered usury if it goes beyond a threshold established by Italy's treasury department (adding 50% to the medium tax rate for various kinds of legal credit), and usury is punishable in Italy under a 1996 law that has, however, proved largely ineffectual, claim critics. "The objective of the law was to help victims and punish perpetrators," said Mr Busà, "but in this it failed and it's clear the law needs to be reviewed."

"People are scared to speak up and report it," said Prof. Razzante, who agreed that the bureaucracy associated with the law could act as a disincentive to using it. To obtain a loan from the anti-usury fund can take months, which may be time that indebted businesses do not have. "And in the meantime people turn to another usurer to get credit, and debt is added to debt. It's very difficult to get out of the terrible spiral of usury," said Prof. Razzante.

The Rome-based Eurispes research institute, in its annual report on Italy's social, economic and cultural situation, publishes a Usury Risk Index that compiles data such as GDP and unemployment, banking system and context, entrepreneurial landscape and crime rates to award each province with a risk value. The southern provinces of Campania and Calabria – historical home bases of two of Italy's most powerful mafias, the Camorra and the 'Ndrangheta – are rated as the two most 'at-risk' regions for usury, with generally high values throughout the south of Italy and Sardinia, while northern provinces tend to fare better.

This doesn't mean usury is less diffuse in the north, however, as recent busts show. Operation 'Borgo Pulito' saw the arrest of 14 affiliates of the Calabrian 'Ndrangheta in the Novara region near Milan in May. Their scheme was based on usury and extortion against local businesses; one entrepreneur became a usurer himself in order to re-pay his exorbitant debts. A bank

employee reportedly signalled businesses in trouble to the network, enabling them to target victims with precision. The scheme managed to create a turnover of more than €7m in just 18 months according to reports in local newspaper *Il Giorno*.

Another high-profile case, made public late last year, showed without a shadow of a doubt the significant presence of the southern mafias in Italy's financial capital. Operation 'Infinito' saw 170 arrests in the Milanese province of Lombardy, unearthing a network of 'Ndrangheta affiliates who had allegedly attempted to gain control of local building enterprises in financial difficulty, with the objective of using them as a cover to compete for the millions of euros in construction contracts for the World Expo in Milan in 2015. Indeed, Mr Busà stressed that Italian organised crime has moved far afield from its traditional home bases in the under-developed south. "The mafia are where there is lots of money going around," he said. And where there is mafia, there is also apparently a lot of money being laundered.

Speaking at Rome's higher school of economics and finance in May this year, the Deputy Director General of the Bank of Italy Anna Maria Tarantola said: "The IMF has estimated that money laundering accounts for 5% of GDP. Our own domestic estimates are rather more pessimistic (but given the incidence in Italy of criminal 'multinationals' it is perhaps no great surprise) and they indicate average dimensions that are superior to 10% of GDP and rising, thanks to the opening of international markets and to economic crises."

Results of anti-laundering operations in Italy are nonetheless encouraging. According to statistics presented by Ms Tarantola, suspicious transactions reported to Italian AML authorities have tripled from 12,500 in 2007 to 37,000 in 2010. Of these, 4,700 resulted in criminal proceedings in 2010 thanks to the Bank of Italy's Financial Intelligence Unit. Yet, Ms Tarantola said, the bulk of reports of suspect transactions originated with banking and financial intermediaries. Just 223 reports out of the 37,000 in 2010 came from professionals like lawyers and accountants.

The third way – FATF promotes reliance

Reliance on others to conduct due diligence, saving on widespread duplication of effort, has strong theoretical appeal, but adoption has so far been severely constrained by the inability of the relying party to similarly outsource responsibility for its completeness. The Financial Action Task Force is currently looking at how to foster greater

reliance as part of its review of the 40+9. Progress is perceptible, if limited, writes Alan Osborn.

Reliance on third parties to conduct proper customer due diligence (CDD) is fraught with legal and other difficulties. It is, not surprisingly, one of the areas where banks and others have urged the Financial

Action Task Force (FATF) to consider changes to the Recommendations during its current comprehensive review. The main stumbling block for many is the FATF requirement that “where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.” A further stipulation (among many) in the US, as laid down by s19 of the USA Patriot Act, requires a financial institution to respond to a request by an American federal agency for information related to anti-money laundering (AML) compliance “within 120 hours after receiving the request”, which means that a bank relying on another institution for AML has to ensure that the documents can be retrieved within 120 hours.

An official of FinCEN, the leading US AML agency, said it was “generally believed that the narrow conditions under which introduced business is permitted, combined with the existence of the 120-hour rule, provide very little incentive to institutions to adopt this approach [ie, reliance on third parties] and this is supported by comments from the banking industry.”

For similar reasons, the third party provision has been relatively little used in other countries even though FATF Recommendation 9, which introduced the right, has been carried into national legislation by member countries.

In the UK, for instance, “the provisions haven’t been as widely used as was hoped and envisaged when they were brought in through regulations following the FATF Recommendation,” said Susannah Cogman, a partner in the financial crime investigation department at Herbert Smith, the international law firm based in London.

The regulations specifying which institutions may be relied on and the nature of that assurance differ from country to country but everywhere the overriding stipulation is that responsibility remains with the firm that does the relying. “You can outsource the compliance but not the responsibility, and firms are understandably quite nervous, given that it’s a criminal offence if they don’t comply with regulations,” said Ms Cogman, “In the end it’s almost as much hassle as just looking at the underlying evidence and deciding for yourself.”

The reform proposals drawn up by FATF are now essentially agreed by the membership though they will not be formally approved until early next year. Essentially it is proposed that countries may allow any type of financial institution to rely on a third party, as at present, but the present de facto limits on the kind of entity that could be relied on will be widened so as to go “beyond the banking, securities and insurance sectors to include other types of institutions, businesses or professions, as long as they are subject to AML/CFT

[anti-money laundering/combating the financing of terrorism] requirements and to effective supervision or monitoring.”

Members of the FATF’s ‘Recommendation 9 Expert Group’, which has been discussing the issue, found that the concepts of reliance, outsourcing and agency differed from one country to another, and even sometimes from one financial activity to another, and recommended “a functional definition constituted by a set of positive or negative elements which describe situations or elements which are characteristic of a reliance context” rather than attempting to define outsourcing or agency. Specifically, FATF said it was considering “taking a more flexible approach for reliance where the third party is a part of a financial group” and considering encouraging countries to require financial groups “to have an AML/CFT programme at the group level, which was applicable to all branches and majority-owned subsidiaries.” Another proposed change would state that reliance on a third party would not be limited to third parties in countries which met the FATF standards when the reliance was

between financial institutions belonging to the same financial group that maintained an effective group compliance programme.

The over-arching theme of these changes is to recognise the status of international financial groups, defining what requirements are needed to be considered

a group and specifying more clearly the reliance that one group member can place on another group member in another jurisdiction. It is essentially an updating of the FATF standards – not meant to make a substantial change in the requirements but enabling them to be applied in a wider way that reflects the structural changes that have happened since the last revision in 2003, say FATF officials. The changes, which officials insist are still under debate, provide for an updating of the way in which financial institutions “ought to take account of country risk in terms of whether the country in which a third party is located is one where the AML is sufficiently well developed for reliance to be permitted.” But the main change has been to accommodate financial groups within this “so as to define really not just reliance, which used to be thought of as between a financial institution and, for example, an introducer in another country, but to define what’s required when the financial institution is relying on another financial institution within the same group.”

The suggested changes in the formal FATF Recommendations in this area have proved broadly welcome to banks and other financial institutions. In its contribution to the consultation, the International Banking Federation (IBFed), the representative body for a number of key national banking associations, said

“The over-arching theme of these changes is to recognise the status of international financial groups”

“reliance can and should be used to complement and ease some of the burdens for customer due diligence” and “could have a number of benefits.”

IBFed says it would eliminate duplication of effort, delays and barriers for customers and help streamline CDD, adding that “failure to increase use of reliance will hamper efficient and effective banking services, both domestically and internationally.” But it warned that third party CDD did not work well across borders as

“financial institutions do not feel comfortable relying on the customer due diligence performed outside the local jurisdiction” while the concept “is not used extensively in either the UK or the US.”

More work to be done then before third party reliance becomes a standard tool in the equipment available to the AML forces, but the FATF changes will surely help it along.

Unclear targets – PEPs

Mutual evaluation reports on countries’ compliance with the Financial Action Task Force 40+9 reveal inconsistencies in the approach to Recommendation 6 on politically exposed persons (PEPs). The differences, in part, reflect deficiencies in implementation [1] but ambiguity and incompleteness in the FATF standard are also to blame, says Sevinj Novruzova.

Foreign PEPs – wherever they are?

The FATF Glossary defines PEPs as “individuals who are or have been entrusted with prominent public functions in a foreign country...” It is clear that currently only foreign PEPs fall within scope but does this mean only those who *live outside* the jurisdiction or should it cover foreign PEPs who live inside as well? While this imprecision exists in the standard countries may feel entitled to follow the narrower interpretation: Germany, Greece, Luxembourg and the Netherlands were all marked down on compliance with Recommendation 6 during their evaluations for exempting foreign PEPs living within their borders from enhanced due diligence even though this approach is envisaged by the Third EU Money Laundering Directive (art 13, para 4). [2]

Identification of PEPs – whoever they are

The FATF proposal to revise Recommendation 6 to impose an obligation on financial institutions (FIs) to determine not only if a customer but also the beneficial owner of an account is a PEP is sensible. [3] The FATF Methodology used by mutual evaluation assessors also refers to ‘potential customers’ – those who have applied to open an account – but the same phrase does not feature in the current Recommendation 6 proposal: it should.

Always a PEP or risk-based after a year

The language of Recommendation 6 suggests an open-ended approach, not setting any limit on how long an individual should be viewed as a PEP once they have left office. However, a one-year interval post departure is to be highlighted in the Interpretative Note on PEPs, which accords with the time-frame in the implementing measures for the Third EU Directive [4] and the Austrian one-year model that was identified as best practice during an FATF plenary [5]. After a year enhanced due diligence would only be mandatory if the regulated entity believed that the ex-PEP continued to represent a higher risk. The RBA may, in time, come to replace the notion of ‘once a PEP always a PEP’.

Rationalising the inner circle

The FATF Glossary definition of a PEP does not include family members and close associates; instead it states that business relationships with these parties involve similar reputational risks to those encountered when dealing with PEPs. In view of the fact that a corrupt PEP’s family members or close associates will often undertake transactions and apply for goods and services on their behalf, these categories of persons [6] should be explicitly included in the PEP definition as secondary PEPs [7]: uncertainty over how far EDD should extend will persist as long as they are not. Proportionality could be built into the ‘Methodology for Assessing Compliance with the FATF 40 Recommendations and FATF 9 Special Recommendations’ by specifying EDD on secondary PEPs only if the transaction has a direct link to a PEP.

Qualification of family members of PEPs is a persistent challenge since the composition may change significantly and without notice. A customer’s own situation may also alter – he or she may become a PEP

following promotion, election or marriage. Failure to apply enhanced due diligence may result, equally, from ineffective KYC by the regulated entity or a deliberate concealment by the individual of their occupation or social status.

Higher and higher

Recommendation 6.2 does not specify a level of seniority for triggering the PEP requirements, which leaves open questions like whether the manager of a local bank branch – an important figure in many communities – should be treated as a PEP and the circumstances in which senior management should seek advice from compliance about taking on a customer. Some jurisdictions have either not provided any interpretation or simply said that approval may be determined at compliance, branch, or board of director level. [8]

In some jurisdictions, the AML/CFT compliance officer may also be a senior manager. The AML/CFT compliance officer should be involved in the PEP approval process, at least in cases of higher risk, for two important reasons: first, they are often best-placed to advise why a person should not be accepted, regardless of the size of the account; and second, it ensures proper engagement and information-sharing between the business and compliance. The AML/CFT compliance officer will have access to broader information on the customer base; suspicious transaction reports filed across the group, terminated customers, and, in some cases, those who have been denied accounts. It is not clear if the role of senior management is intended to be limited to the initial approval or whether it extends further into the customer relationship, for example, to removing a name from a PEP list.

Onboarding is just the beginning

The term “enhanced ongoing monitoring” is not explained but the FATF could do so via its methodology for assessing compliance with the 40+9. It would likely reflect the expectation of continuing review of the PEP customer’s transactions against their anticipated account activity profile as well as periodic updating of client information. Enhanced ongoing monitoring should also entail senior management reappraisal of all PEPs; maintenance of PEP relationships should, ultimately, be their direct responsibility. [9]

Notes

1. ‘Horizontal Review of Moneyval’s Third Round of Mutual Evaluation Reports’, December 2010, p64 (www.coe.int/t/dghl/monitoring/moneyval/publi

- [cations/3rdHorizontalreview_en.pdf](http://www.coe.int/t/dghl/monitoring/moneyval/web_ressources/WB_PEPs_en.pdf)); ‘Stolen Asset Recovery: Politically Exposed Persons’ – A Policy Paper on Strengthening Preventive Measures, World Bank, p53. (www.coe.int/t/dghl/monitoring/moneyval/web_ressources/WB_PEPs_en.pdf)
2. See the FATF mutual evaluation reports of Germany (19 February 2010), Greece (29 June 2007), Luxembourg (19 February 2010) and the Netherlands (25 February 2011) available at www.fatf-gafi.org. Article 13, para 4 of the Third EU Directive only requires enhanced due diligence on “politically exposed persons residing in another Member State or in a third country” (http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_309/l_30920051125en00150036.pdf)
 3. The Forty Recommendations, Annotated with current agreed outputs from Expert Groups (version of 6 July 2011), p5 – not publicly available.
 4. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_214/l_21420060804en00290034.pdf
 5. Recommendation 6: Implementation Issues, FATF Working Group on Terrorist Financing and Money Laundering, p5 – not publicly available.
 6. FATF is silent on the definition of ‘close associates’ but both the United Nations and EU have addressed it. Under the UN Convention Against Corruption (UNCAC), the term encompasses persons or companies clearly related to individuals entrusted with prominent public functions. [See UN General Assembly, ‘Interpretative notes for the official records (travaux préparatoires) of the negotiation of the United Nations Convention against Corruption’ (A/58/422/Add.1), para 50.] Directive 2006/70/EC says ‘close associates’ shall include: (a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations with a PEP; (b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement, which is known to have been set up for the benefit de facto of a PEP.
 7. In contrast to the FATF 40+9, the Directive 2005/60/EC and UNCAC PEP definitions include family members and close associates.
 8. See Mutual evaluation report of Germany (19 February 2010).
 9. See approach advocated in ‘Stolen Asset Recovery: Politically Exposed Persons’, *ibid.*, p7, 13.

Sevinj Novruzova (sevinj.novruzova@fiiu.az) is a senior legal advisor at the Financial Monitoring Service under the Central Bank of the Republic of Azerbaijan.

Diary dates

Global Investigations

19–20 September 2011
Grange St Paul's Hotel, London
www.c5-online.com

ACAMS 10th Annual Anti-Money Laundering Conference

19–21 September 2011
Las Vegas, US
www.acamsglobal.org

Anti-Money Laundering and Counter-Terrorism Financing Conference

27 September 2011
Central London
www.conferencesandtraining.com/anti-money-laundering

The 2011 MLROs and AML Professionals Summit

3–4 October 2011
The Lancaster Hotel, London W2
UK £400+VAT for the two days with networking dinner
Website: www.compliancer.com

World Bribery & Corruption Compliance Forum 2011

5–6 October 2011
London
www.informaglobalevents.com

SARs and Courts Orders Masterclass

6 October 2011
Pinners Hall, London EC2N
www.bba.org.uk

Money Laundering Induction Workshop

12 October 2011
Pinners Hall, London EC2N
www.bba.org.uk

Anti-Money Laundering Professionals Forum 5th Annual AML European Conference

17–18 October 2011
Drapers' Hall, City of London
www.amlforum.com

Money Laundering and Financial Crime Prevention 2011

10th Annual Conference
18 October 2011, Central London
www.cityandfinancial.com

OFAC Boot Camp

1–2 December 2011
New York Marriott Downtown, New York
www.americanconference.com

www.moneylaunderingbulletin.com

www.i-law.com/financialcrime

Editor: Timon Molloy • Tel: +44 (0) 20 7017 4214 • timon.molloy@informa.com

Editorial board: Jonathan Fisher QC – Member and Financial Crime Team Leader, Essex Street • Denis O'Connor – Director, Association for Financial Markets in Europe • Adriana van der Goes-Juric – Chair, Anti Money Laundering Professionals Forum

Production editor: Catherine Quist • catherine.quist@informa.com

Printed by: Halstan Printing Group

Marketing: Naeemah Khan • naeemah.khan@informa.com +44 (0)20 337 73847

Sales: Mike Ellicott • Tel: +44 (0)20 7017 5392 • mike.ellicott@informa.com ISSN 1462-141X © Informa UK Ltd 2011

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. If you wish to obtain back issues, please contact our subscriptions department tel 020 7017 5532 or fax 020 7017 4781. **Published 10 times a year by:** Informa Law & Finance, 1/2 Bolt Court, London EC4A 3DQ • tel 020 7017 5000 • fax 020 7017 4601. www.informaprofessional.com **Copyright:** While we want you to make the best use of *Money Laundering Bulletin* we also need to

protect our copyright. We would remind you that copying is illegal. However, please contact us directly should you have any special requirements. While all reasonable care has been taken in the preparation of this publication, no liability is accepted by the publishers nor by any of the authors of the contents of the publication, for any loss or damage caused to any person relying on any statement or omission in the publication. All rights reserved; no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or

by any means, electrical, mechanical, photocopying, recording, or otherwise without the prior written permission of the publisher. Registered Office: Mortimer House, 37–41 Mortimer Street, London W1T 3JH. Registered in England and Wales

No 1072954. This newsletter has been printed on paper sourced from sustainable forests.

informa
law & finance
an informa business