Money Laundering bulletin

The monthly briefing service for anti-laundering specialists

Mike Ellicott
Informa UK Ltd, Telephone House, 69-77 Paul Street,
London EC2A 4LQ, United Kingdom

Telephone: 020 7017 5392
Email: mike.ellicott@informa.com

informa
law

www.informaprofessional.com/mlb

Money Laundering bulletin

The monthly briefing service for anti-laundering specialists

Going fourth

A fourth EU Money Laundering Directive is in prospect: on 1 February the European Commission sat down with private sector stakeholders to hear feedback on their experience with the existing EU legislation "in the context of the forthcoming review of the third AML Directive (2005/60/EEC)". [1] No time-frame was mentioned but it won't be till after the Financial Action Task Force (FATF) completes its review of the 40+9 Recommendations, scheduled for next year. In its note to the meeting, the Commission referred to "prior impact analyses" and "good coordination with the FATF's own standards revision process." Participants [2] were delighted – the note actually says they "welcomed" this approach. The Commission has learnt the importance of engaging with the regulated sector, in no small part due to HM Government's efforts in this regard. The proof of earnest will be in the shape of any final draft legislation that goes to ministers but there should be plenty of opportunity to air dissatisfaction before fixing on black letter law. Irritations there are aplenty: some were identified in a Deloitte study of the Third Directive [3] and the Commission refers to these in its note. Customer due diligence (CDD), for example, is frustrated by the lack of publicly available information on beneficial owners, with data protection concerns not encouraging reliance on third parties. One stakeholder, not identified, pointed to the "enormous resources needed" to reach back to the ultimate beneficial owner, not least in the case of trusts, but also (specifically mentioned) in the shipping business, and often for US clients since US legislation does not cover non-financial professionals. A member of a City of London trade body observed to *MLB* that as the OECD (Organisation for Economic Cooperation and Development) was pressuring governments to cooperate on tax transparency and share information on beneficial owners that way, why shouldn't they open up the data to the private sector as well. The Commission alludes to "establishment of publicly consultable registers", currently optional under FATF Recommendations 33 and 34. Blowing away the corporate and trust veils is likely to prove an uphill task in some jurisdictions but if the EU pushes for it the US, for one – think Delaware, Nevada, Wyoming – will find it harder to avoid cracking open their own onshore secrecy jurisdictions. *MLB* attended a US conference a couple of years ago where it was said that even US law enforcement are sometimes unable to penetrate right through domestically created corporate structures.

Online CDD is hindered by the uneven conventional identifier information available on the Web and stakeholders suggested recourse to alternative sources, eg, mobile phone operators: most people don't share their mobile very much and perhaps it could serve as an authentication device – a bank could send a unique code to the phone before a transaction

March 2011
Issue 181

IN THIS ISSUE

was authorised. ID checks might also be referenced to the IP address of an account-holder's computer. Is either a mobile phone of IP address unique to the account-holder? As the old joke goes, no one on the Internet knows you're a dog, which is to say, just because the individual has access to the right mobile and computer is not conclusive proof of identity but it serves to increase confidence. Technology is evolving all the time – voice biometrics, facial recognition and fingerprint reading via new smartphones are likely to improve remote identification and verification accuracy by a massive factor in the next few years.

Beneficial ownership ID problems are mirrored in the PEP (politically exposed person) space. The Deloitte study mentions continuing dissatisfaction at the lack of publicly available information; stakeholders believe that the definition of "persons known to be close associates" is too wide. The Commission note is conspicuously silent on this point, which suggests that there is not much to hope for in terms of official lists of who works for governments and for the public authorities they control. There is not a lot to be done in a democracy if the elected representatives of whichever stripe refuse to assist so the commercial PEP list database providers' revenue streams are probably safe.

Perhaps 'equivalence' offers a better chance for movement. The EU list is not held in high regard; it's a clear case of 'all are equal but some are more so than others'. How exactly did Russia make the cut? But then, it is a full member of FATF. And how, exactly, did that happen? Erm... The Commission note that "there were calls for a more up to date list which had binding effect."

Other matters raised by stakeholders included how to verify originator information on incoming SWIFT messages, and concerns about making tax crimes a predicate for money laundering, though *MLB* submits that following the financial crisis, and knowing the broken state of exchequers around the world, this is as good as settled.

Bribery & corruption – new law but is it all just talk and hands up who banks Gaddafi?

The wait is nearly over, surely. Eleventh hour finessing of the 'adequate procedures' (to prevent bribery) guidance, which HM Government committed to issue three months ahead of implementation of the *Bribery Act 2010* isn't expected to add much to the draft version. [4] The real question is whether all the brouhaha is justified. In the current straitened economic environment can the UK afford the moral high ground? If the real agenda is always political one must expect the coalition government to prioritise re-election over any other consideration, which does not translate into threatening the profitability of British companies by disadvantaging them in the international marketplace for bribes. If the choice is between bunging a few million sterling to a person of influence overseas and not securing a significant contract that will guarantee jobs and votes, it would be a more than unusually principled politician who would object to payment of the bribe. But the shiny new legislation is the toughest in the world – far beyond the US *Foreign Corrupt Practices Act* (FCPA), which only addresses illicit payments to foreign public officials, it covers commercial to commercial as well and makes no concession for facilitation payments. Hasn't HM Government boxed itself into a corner by putting it on the statute book? No. The simple answer is to undercut enforcement – the regulatory impact assessment to the bribery bill envisaged only 1.3 criminal prosecutions a year and Lord McNally, Minister of Justice, told Parliament that the budget for Serious Fraud Office (SFO) policing of the new guidance is UK£2m a year, which, a lawyer pointed out, to *MLB* amounts to less than the value of a bribe in the larger cases.

SFO was adopting a pragmatic approach – Director Richard Alderman, who was formerly head of legal at the defunct Assets Recovery Agency, has championed civil settlements and encouraged firms to come forward and confess if they come across corruption in their business, pay a penalty and so draw a line and avoid risk of debarment from tendering for large public contracts (under the terms of the EU Procurement Directive) that a conviction would bring.

The model has a pleasing logic – corporates will do the right thing because they face multiple threats of exposure – whether by their own advisers filing bribery suspicious activity reports (SARs) to the Serious Organised Crime Agency (SOCA) (which are accessible by SFO) or disgruntled employees blowing the whistle. The SFO will require them to carry out and pay for their own investigation under its direction, put in the necessary anti-bribery and corruption (ABC) systems and controls and pay a fine. All this at little or no cost, indeed, a gain to the public purse. The plan was proceeding nicely until it ran into the *Innospec* case [5] and Lord Justice Thomas, who was scathing in his criticism of the SFO's approach to civil settlements in bribery and corruption cases [6]: at paragraph 38 of his sentencing remarks he said, "Those who commit

such serious crimes as corruption of senior foreign government officials must not be viewed or treated in any different way to other criminals. It will therefore rarely be appropriate for criminal conduct by a company to be dealt with by means of a civil recovery order... It is of the greatest public interest that the serious criminality of any, including companies, who engage in the corruption of foreign governments, is made patent for all to see by the imposition of criminal and not civil sanctions." Opinion amongst lawyers, to whom *MLB* has spoken, is that Thomas LJ will be called in for a quiet word or, as one QC put it, "He'll have to be put back in his box. The country simply can't afford long, expensive corruption trials." Watch this space for judicial guidance on civil settlements. But if he is right and firms are able simply to pull out the cheque book, pay a fine – all right, plus hefty fees for upgrading their ABC controls - and promise not to do it again, won't that effectively decriminalise bribery? "Yes," said a partner in City law firm.

The Middle East – PEP risk crystallises

Political stability (of a sort) in the Middle East and North Africa in recent history is a sorry tale of pandering to despots, which inevitably means bribery and corruption. The West has quietly overlooked human rights abuses and the absence of the democratic values it supposedly holds so dear at home for the sake of peace and oil – not necessarily in that order. Over four decades plus of repression, the youthful populations in Arab states – a third of Egyptians are under 15 years of age [7] - have grown increasingly restive just as telecommunications have become affordable for almost everyone and social media has taken off. This potent mix of disaffected citizenry, now able to share their grievances despite the best efforts of official censors, had to blow at some point: Europe and the US are left watching from the sidelines and just as the diplomats scramble to make sense of the changing landscape so must the financiers. Some countries have moved swiftly: Switzerland seized the opportunity to trumpet integrity by freezing the funds of Zein al-Abidine Ben Ali, the ousted Tunisian president; the EU has done likewise. But the real question to be asked is how any financial institution is able to countenance running accounts for Ben Ali, Mubarak, Gaddafi and any number of other heads of state in the region in the first place? As Anthea Lawson, head of the kleptocracy campaign at Global Witness wrote on *FT.com* on 23 February, "If there is enough evidence of corruption to freeze Mr Mubarak's or Mr Ben Ali's funds now that they have been forced from office, why was it not sufficiently obvious at the point when they were accepted?" She goes on, "What questions did these banks ask about the money they were accepting? Did they reassure themselves that it had been legitimately earned?" MLROs and senior management in the wealth divisions of major institutions will be frantically combing their enhanced due diligence files on Middle Eastern PEPs for assurance that the source of funds rationale squares with the official salary of, say a Libyan colonel. Perhaps the UK Financial Services Authority is prescient and, sensing the turmoil coming, opted to delay publication of its thematic review of high risk areas, which covers how banks treat PEPs, accordingly.

UK SARs retention policy not 'necessary and proportionate' – Information Commissioner

Away from the turbulent Middle East and back in July 2009, the House of Lords EU Committee published its report on Money Laundering & Terrorist Financing [8], which raised concerns that ELMER, the UK SARs database, might fall foul of data protection and human rights legislation for holding personal details of mere suspects. On its recommendation, the Information Commissioner reviewed SOCA's (home of the UK financial intelligence unit) model; his report, recently published on Parliament's website [9], is comforting in its praise for the exemplary cooperation from SOCA personnel and assessment that "[t]he security, policy and procedures in relation to SAR Online [the internet reporting mechanism] appear sufficiently robust." However, neither were the peers wrong to be worried in light of the European Court of Human Rights decision in *S and Marper v UK* [10], which found that indefinite retention of biometrics like "fingerprints... and DNA profiles of persons suspected but not convicted of offences... fail[ed] to strike a fair balance between the competing public and private interests..."

The Information Commissioner noted that the first data protection principle under the *Data Protection Act 1998* (DPA) requires that individuals understand how their personal data will be processed by those who hold it. He questioned "whether these fair processing requirements are being met in those cases of no concern retained on a system indefinitely without the knowledge of those individuals to whom those [suspicious activity] reports relate." The finding doesn't seem to square with SOCA's evidence that SARs are automatically deleted after 10 years unless they have been amended or updated, in which case the deletion date is reset to six years after that occurrence. If a SAR

has been fully exploited and is no longer needed it may be deleted before 10 years, according to SOCA. Whichever is right, the Information Commissioner has further reservations about compliance with data protection principles three ('personal data shall be adequate, relevant and not excessive') and five ('personal data should not be kept longer than is necessary').

He goes on to make five recommendations, four require positive action: one, SOCA "develops, implements and actively manages a record retention and deletion policy which addresses the requirements of the DPA and HRA [Human Rights Act] on necessity and proportionality"; two, the plan for this policy should be completed within three months of the presentation of the his report, which means by 18 April 2011 [11]; and that the ELMER upgrade should support the new policy and give effect to it in 2011.

Fourthly, the noble lords will also have been pleased that the Information Commissioner queried the "pressing social need" for reporting all transactions when the threshold for suspicion is very low. The HL EU Committee had questioned the value of reporting trivial criminal offences in its report [8, paragraph 110] and asked the government to look at amending the *Proceeds of Crime Act 2002* to include a *de minimis* exclusion. Lord Marlesford raised the matter again on 7 February 2011; Home Office minister Baroness Neville-Jones replied, "We are considering the [HL EU Committee report] and will work with SOCA and other partners to provide a detailed response in due course." Whether it will be soon enough to meet the Information Commissioner's three-month time line is another question.

The minister was a little more specific in answer to Lord Marlesford's other enquiries, advising that as at 26 January 2011, ELMER held 1,733,862 entries and that 116,810 have been removed since it became functional in the year 2000. No local authorities are currently able to access the SARs database directly, she said. The HL EU Committee report had noted that Nottinghamshire County Council used ELMER to investigate housing benefit fraud unrelated to serious organised crime. Agencies outside SOCA are able to access ELMER via the Moneyweb portal; the Information Commissioner found that 2,200 individuals were accredited to look at the SARs.

Another 'stripper'? [12]

"The bank is in great shape, has good momentum, and is superbly positioned for the future." Peter Sands, CEO of Standard Chartered must be pleased with that the way his institution weathered the financial crisis: profit before tax was up 10% in the half year to 30 June 2010 to US$3,116m. One cloud on the horizon though is how the US will view its past Iranian business against OFAC (Office of Foreign Assets Control) obligations. The interim statement suggests that all might not have been done by the book: "[d]iscussions [with US authorities] are continuing and the Group is conducting a review of its historical business and related activities relevant to its US sanctions compliance predominantly with respect to Iranian business. The Group cannot predict what the outcome will be."

Unintended consequences

Sanctions, proliferation finance and a US Under Secretary for Terrorism and Financial Intelligence with a notably robust sense of mission to stop Iran building a nuclear bomb – all serious matters one would reasonably think, and of course, reading through the US embassy cables released by Wikileaks, this is the general sense but *MLB* was amused to come across the following snippet from a conversation between Under Secretary Stuart Levey and James Robertson, Head of Financial Crime, HM Treasury in November 2008: "In response to U/S Levey's question as to why HMG [HM Government] doesn't just shut them [the Iranian banks operating in London] down, Robertson replied that, in fact, after being subjected to increased regulatory scrutiny, one of the banks has become the best run bank in the UK. HMG can only close banks for being poorly run or undertaking illegal activity directly (not through its parent)." [13]

Notes

1. http://ec.europa.eu/internal_market/company/docs/financial-crime/20110218-report_en.pdf
2. http://ec.europa.eu/internal_market/company/docs/financial-crime/20110218-list_en.pdf
3. http://ec.europa.eu/internal_market/company/docs/financial-crime/20110124_study_amld_en.pdf
4. www.justice.gov.uk/consultations/docs/bribery-act-guidance-consultation1.pdf
5. *R v Innospec Limited* [2010] EW Misc 7 (EWCC)
6. www.judiciary.gov.uk/Resources/JCO/Documents/Judgments/sentencing-remarks-thomas-lj-innospec.pdf
7. https://www.cia.gov/library/publications/the-world-factbook/geos/eg.html

8. www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/132/13202.htm
9. www.publications.parliament.uk/pa/ld201011/ldselect/ldeucom/82/8202.htm
10. Application Nos. 30562/04 and 30566/04, 2008
11. The House of Lords ordered the Information Commissioner's report to be printed on 18 January 2011.
12. Lloyds TSB (www.treas.gov/press/releases/tg458.htm, 'Who would be a banker?' *MLB* February 2009), Credit Suisse (www.treas.gov/press/releases/tg452.htm, 'Another stripper exposed', *MLB* February 2010), ABN AMRO (www.ustreas.gov/offices/enforcement/ofac/civpen/penalties/01032006.pdf) and again after it was taken over by RBS (www.justice.gov/opa/pr/2010/May/10-crm-548.html, 'Overcast', *MLB* June 2010) and Barclays (www.treas.gov/offices/enforcement/ofac/actions/20100818.shtml, 'The hit list', *MLB* September 2010) have all been fined for stripping originator information from wire messages that would have allowed US financial institutions to identify that the payments were destined for OFAC-sanctioned entities.
13. http://213.251.145.96/cable/2009/01/09LONDON50.html

***Timon Molloy**, Editor*

Sanctions screening – from art to science, an industry revolution

Watchlists are nothing new but they remain among the most potent and dynamic challenges facing the regulated sector: how can an organisation be sure that its filters are catching parties and payments proscribed under sanctions laws? One way is to create a data set, drawn from the names (with fuzzy variations) on one or more of the sanctions lists and fire it at the filters to see which entities are blocked. The principle is sound but the approach to building a valid subset of names to test is far from simple, says **Ian Horobin** of Omnicision, "For a start you need to be sure that the list you are using is completely up to date." He has developed software that monitors the government sites, like OFAC [US Office of Foreign Assets Control] and HM Treasury, continually, 24/7 by 365, to detect any changes to their list files. Immediately a revision appears it is automatically downloaded, validated and stored. "A notification is then generated, also automatic, which goes out to clients by email, SMS and now on Twitter @Omnicision." This direct sourcing cuts out any delay between publication on the website and receipt of the same change by official email. "Sometimes the saving can be 10 or 20 minutes but, on occasion, hours if the government email server is running slowly, giving a valuable early start for internal list change processes." There are other valuable by-products of continuous monitoring, says Horobin: a complete history of the lists is archived for referral and comparisons – especially useful in any compelled lookback. "We are also able to tell, for example, the average number of days between Sanction List updates (on average every seven calendar days for OFAC SDN) and look at when in the week a list change is most likely to occur (Monday is by far the quietest day for OFAC)." (Such patterns are explored in a sample report at the end of this article.) Using these findings, an organisation would be able to take a probabilistic view on resource allocation in its sanctions compliance area.

Conventional filter assurance testing is predicated on a manual data set build and analysis but even if no list update interrupts the process, there is still the issue of how to make a truly representative selection of names. The only approach that can claim mathematical rigour is to take a statistically valid sample of the entries as they appear in the list(s) and the fuzzy derivations. Sampling is essential, says Horobin, since it would be impossible to test all permutations of every name – "If we take just the four common lists – OFAC, HM Treasury, EU and United Nations – there are approximately 42,000 exact matches in total; adding 100 different fuzzy variations that may occur in any combination up to 4 at a time results in 4.2×10^{12} combinations." The population of possibilities grows with each new fuzzy derivation or new name that is added to the list – a size of problem that is only going to grow with time, says Horobin. The RBS decision notice [1], for example, highlighted a problem with detection of names occurring on two lines: "We are able to plug in both

this sort of finding and any other fuzzy derivations as required to create the whole population from which to test – automatically." The software has been developed as a cloud computing application, ie, it sits online, accessible in straight HTML pages via a secure internet connection – there is no client-side installation. Once the statistically valid sample of exact names and fuzzy variations is generated, it is downloaded, in any format, ready to be flushed through those filters. Results – all synthetic data as there is no need for customer account or transaction details – are then uploaded into the application, for an almost instant assessment of how well the filters are performing.

The fuzzy tests used within the application cover a broad range of situations to test both the intentional and unintentional changes that may be made to customer and payment data. For example, a common typographic mistake for some names is to use an 'a' instead of an 'e', "These tests are generated via the relevant algorithm plug-in from our library, which we will either already have available or write for the purpose - a very quick process."The results assessment will report if, and how well, the individual filters measure up: did, for example, the claimed 'a-e transcription' check pick out instances that featured in the sample and if so, how many of them and where did the failure points occur? If filters turn out to be less effective than a threshold set by the client, in line with its risk appetite, questions may need to be asked of the screening solution configuration or the screening solution vendor.

The plug-in library, which expands steadily as new fuzzy derivations arise, neatly illustrates the consortium approach that Horobin is keen to foster: "By sharing experience of the quirks and problems in data presentation, which we are able to replicate through algorithms, clients are able to anonymously share and build on each other's experience to help audit and operational assurance of filters." In the same vein, the software enables organisations to benchmark their filters' performance against those of their peers, on an anonymised basis, as long as they also agree to feed their own results into the process.

Aside from the benefits of being able to provide quick, robust and efficient assurance, Horobin is also keen to promote the overall efficiency benefits that can be gained: "Through automation we are able to let organisations formalise their risk appetite and efficiently tune filter performance – in effect providing the ability to minimise false positives whilst providing the proof of adherence to risk appetite."

Up until now, the regulated sector has had no scientific way to determine if its sanctions filters are working as intended. "Through use of applied statistics, we have made it possible, for the first time, to align the decisions made about screening to the firm's risk appetite," says Horobin, which should catch the attention of regulators. If he succeeds in collectively raising the standard of screening, it will mean fewer false positives and negatives and significant cost savings – one alert that would be guaranteed escalation.

Sanctions list analysis

The following report assesses the content and update characteristics of the UK HM Treasury and US Office of Foreign Assets Control (OFAC) Special Designated Nationals (SDNs) sanctions lists:

- HMT: www.hm-treasury.gov.uk/d/sanctionsconlist.csv
- OFAC SDN: www.treasury.gov/ofac/downloads/sdn.xml

Summary

- Total names on the OFAC SDN and HMT Sanction Lists have grown 10% over the last 9 months;
- Average of 8 calendar days between changes for HMT and 7 calendar days for OFAC;
- Average number of names or AKAs (Also Known As) added or removed at each change: 12 for HMT and 28 for OFAC SDN (this does not include changes to existing names). The difference in the number of changes reflects the differing size of the lists;
- Most common dates to update: HMT - Monday, Wednesday and Friday; OFAC - Tuesday, Wednesday and Thursday;
- As of 21/1/2011, the date of the OFAC notification regarding use of weak AKAs [2], if an organisation were to implement this approach it would equate to circa 17% reduction in AKAs that must be screened.

HMT sanctions

Date range included: 7/4/2010 - 2/2/2011
Number of days on which changes were made: 38

Growth of Primary Names & AKAs
Overall growth: 10%
Primary name growth: 17%

Chart 1 – HMT – Primary names & AKAs

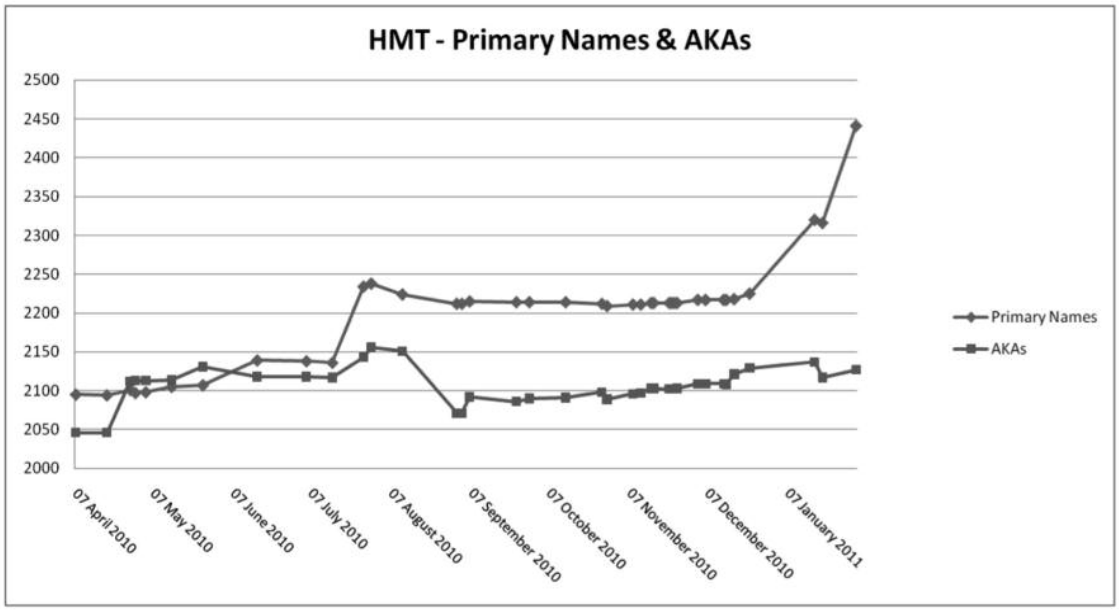


Chart 2 – HMT – Total names

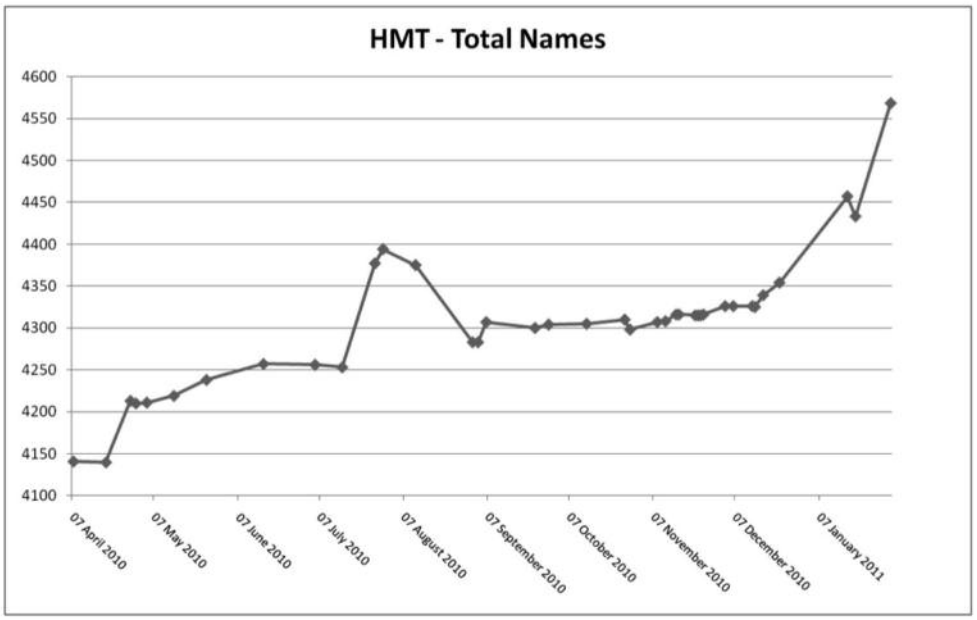


Chart 3 – HMT Updates – Day of week

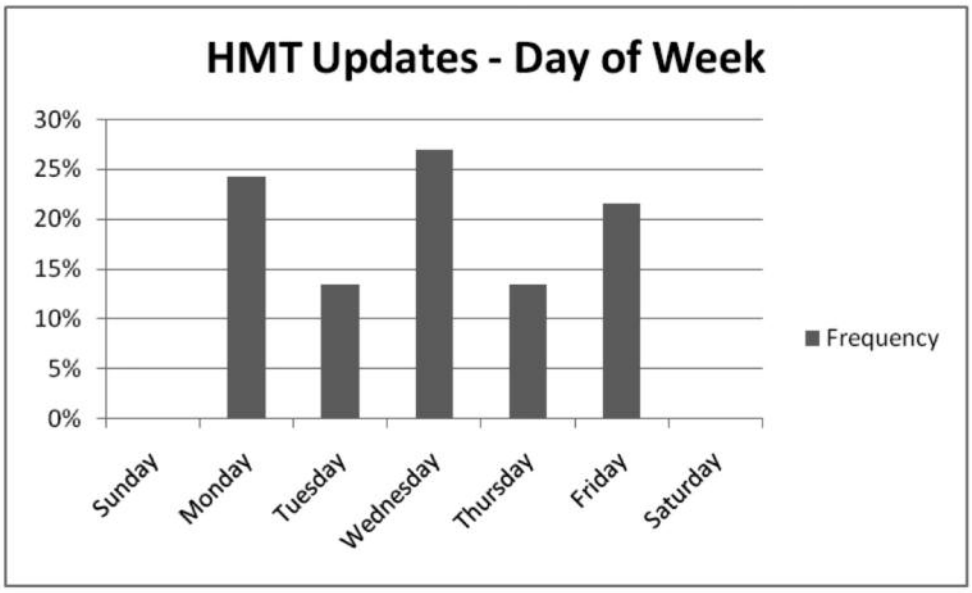
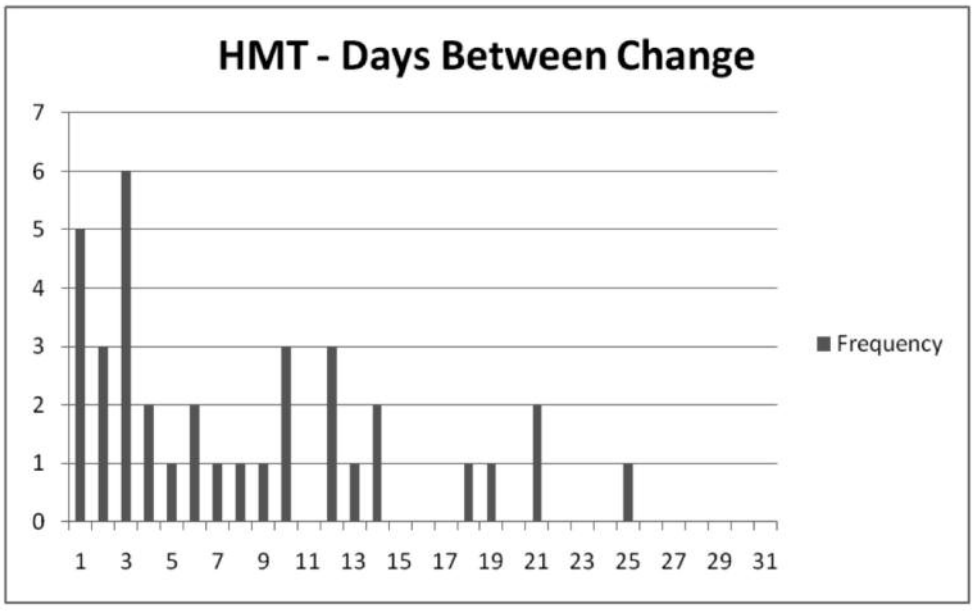


Chart 4 – HMT - Days between change



Average of 8 calendar days between each list change.

Volume of change – the average number of names or AKAs added or removed: 12 (this does not include changes to existing names).

OFAC SDN

Date range included: 16/4/2010 - 1/2/2011
Number of days on which changes were made: 41

Total Names (Primary, Strong & Weak AKAs)
Overall growth: 10%
Primary name growth: 8%

Chart 5 – OFAC SDN Total Names (Primary, Strong & Weak AKAs)

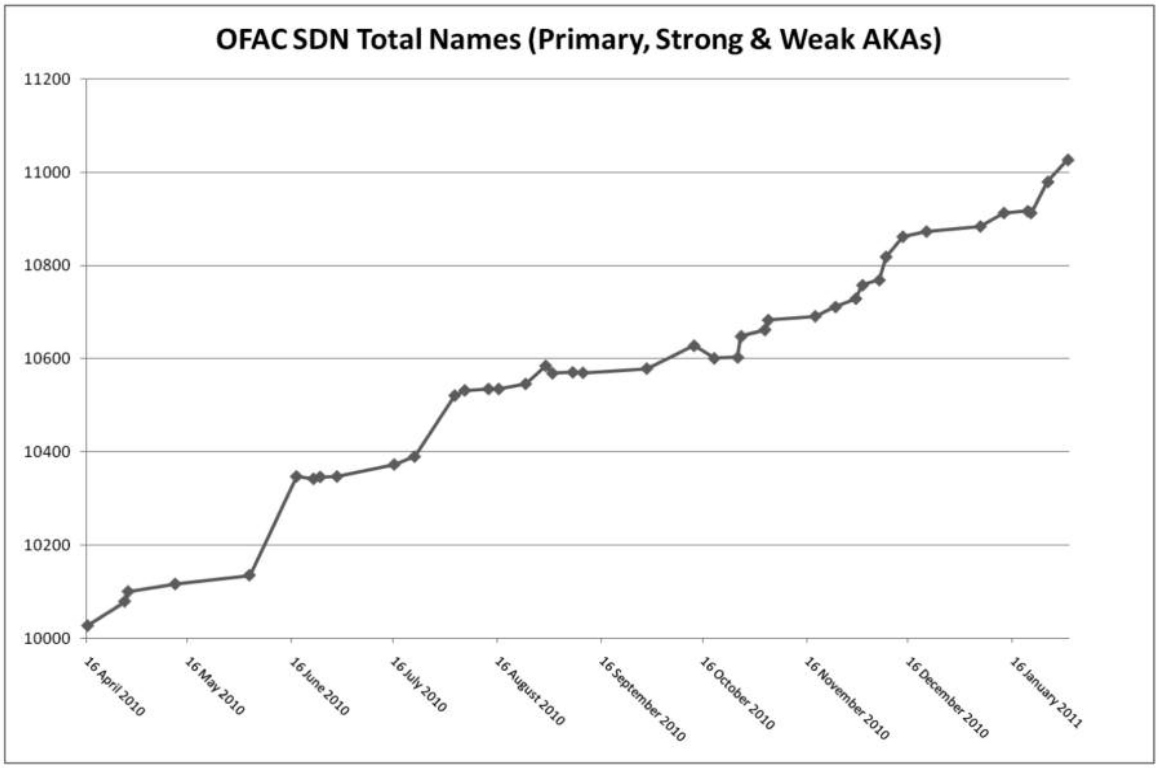


Chart 6 – OFAC SDN – Strong AKA v Weak AKA

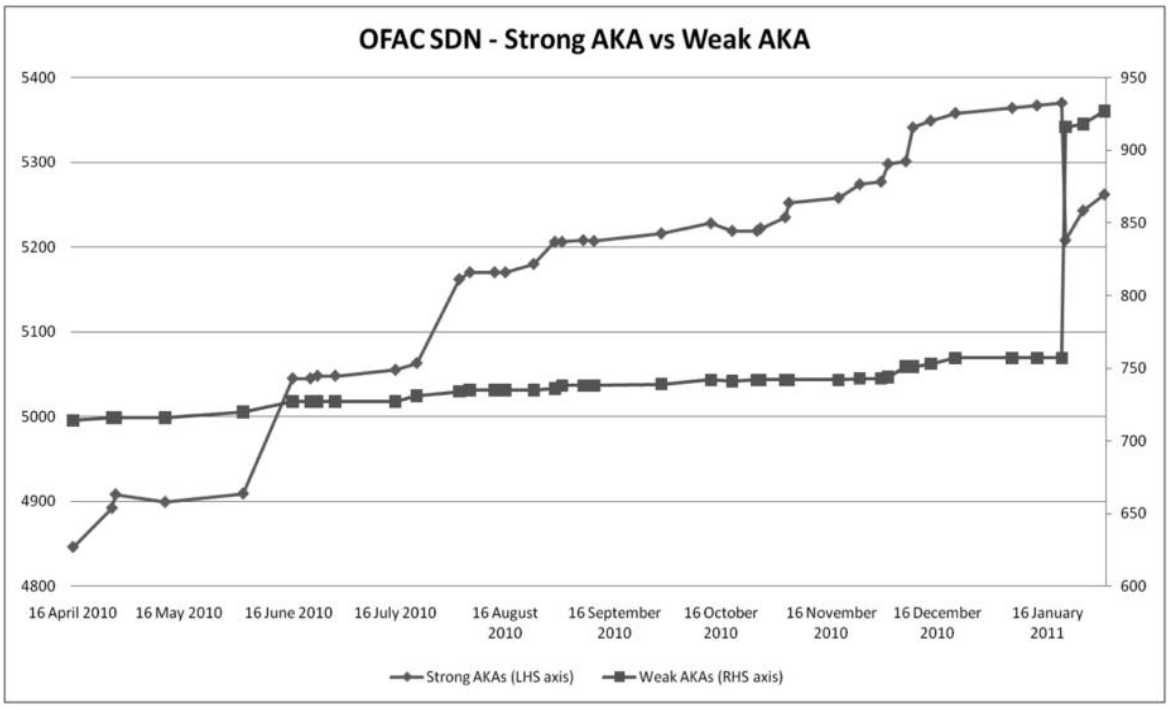


Chart 7 – OFAC SDN Updates – Day of Week

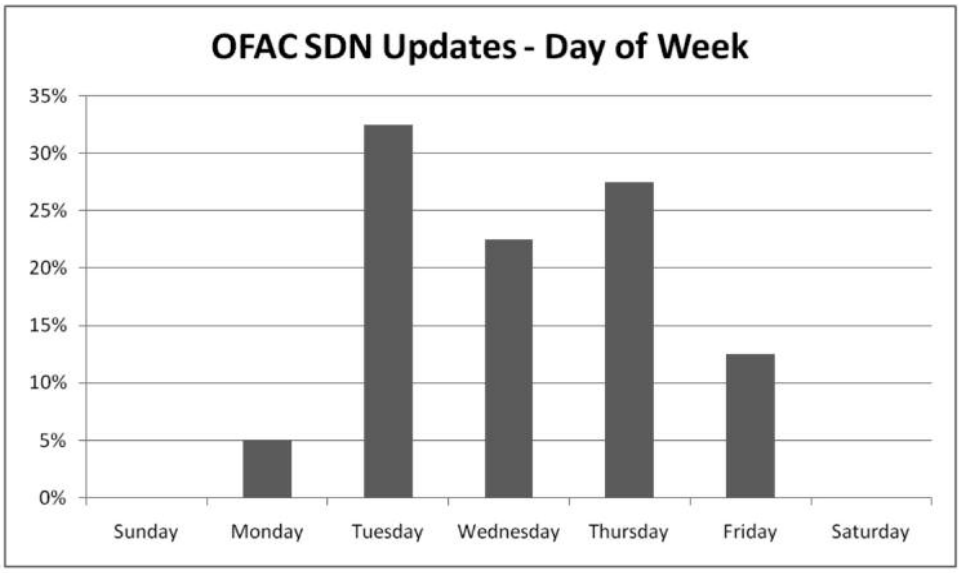
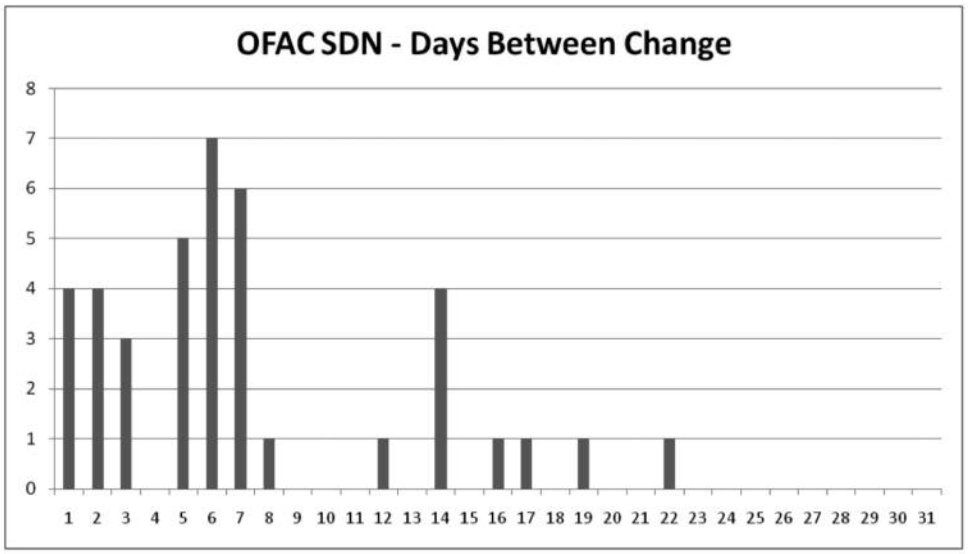


Chart 8 – OFAC SDN - Days between change



Average of 7 calendar days between each list change.

Volume of change – the average number of names or AKAs added or removed: 28 (this does not include changes to existing names).

Notes

1. www.fsa.gov.uk/pubs/other/rbs_group.pdf
2. www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/weak_strong_alias.aspx

Ian Horobin *(+44 (0) 1252 673723, i.horobin@omnicision.com) is the founder of Omnicision, which provides product neutral consultancy services to companies exposed to financial crime.*
Reporting by Timon Molloy.

Push back

"Frustration, that's the feeling I sense in the regulated sector just now," **David Blackmore**, Director of DB Risk and Compliance Services Ltd sighed when *MLB*'s editor caught up with him on Threadneedle Street. After more than 30 years in banking, he's not one to pull a punch and mention of the *Shah* case [1], yet to come to trial, is calculated to make his fists clench: "I'm still appalled that the bank has to go through this ridiculous charade when there's adequate case law to show that suspicion is a very low threshold." The government scores a "big black mark" in his book, nor is the tally improved by the coalition's reformation of the financial crime agencies: "They seem to be getting rid of the most experienced talent." Blackmore cites the departure of the entire top management of the UK Financial Intelligence Unit late last year and notes that the Serious Fraud Office recently lost two leading figures – Charlie Monteith, a senior policy advisor who worked on the *Bribery Act*, and Robert Amaee, who led the anti-corruption and proceeds of crime units.

"If the knock-on of all this slimming down is improved quality at the end of the day, well and good but the record is not encouraging." The organisational disruption and decline in police numbers promise "more opportunity for criminals and less surveillance just at a time [of economic stress] when motivation [to commit offences] is increasing." The prospect of being caught is set to diminish but "one of the main aims of criminal law is not just to punish but to deter." The central point one has to keep in mind, he believes, is that "everything the current government does is subsumed to the bigger objectives of reducing the deficit and the bloated client-State. The huge expansion of the public sector has itself been the growth engine of financial crime, especially fraud," says Blackmore, "No wonder the 2010 KPMG Fraud Barometer and research by CIFAS and others puts the public sector as the principal victim of financial crime, way above financial services!"

The Financial Services Authority is at least doing its part by tacking money laundering charges onto insider dealing indictments [2]. Yes, but it disappoints on progress with the thematic review of high risk areas in 27 banks, for which read PEPs, correspondent banking and wire transfers - "It looks as though the final report may not be out until Q3 of this year at the earliest. I can't imagine why when the field work was all done months ago."

Publication will be closely watched, not least by the editorial board of the Joint Money Laundering Steering Group (JMLSG), which has yet to respond to the regulator's move on sanctions compliance: "I think they will have to amend the [JMLSG] Guidance; we now have Part 3 plus RBS [3]." The FSA Decision Notice on RBS's breach of systems and controls around sanctions raises the bar, setting out an expectation that firms screen all beneficial owners and directors of corporate entities. "If one allies these findings to the recent Financial Action Task Force paper on trust and company service providers [4], it should be blindingly obvious that financial institutions have to get their act together and do it." The implication then is that many are not: "Firms may just be screening signatories of corporate clients and not the other directors or beneficial owners. That might have been okay up to the RBS decision but no longer in my view. I think it's likely that FATF will upgrade their 40 Recommendations in this direction and I would not be surprised to find they'll incorporate the UN Anti-bribery Convention as well."

The necessary systems changes are likely to be expensive and take time to effect; one more reason, perhaps, why the financial sector is pleased over the delayed release of the 'adequate procedures' guidance around the *Bribery Act*. A possible answer to concerns about how prosecutors will exercise their discretion may be to look to the US authorities' application of the *Foreign Corrupt Practices Act* (FCPA): "The US Department of Justice welcomes prior approaches from firms for guidance; it then publishes this, on a no names basis, on its website so that other firms can understand whether particular behaviour is safe or not." Blackmore doesn't see why something similar can't be provided around the UK Act. "The delays in implementing this long-overdue reform could and should have been avoided with a modicum of lateral thinking by the MoJ [Ministry of Justice] and the SFO [Serious Fraud Office] over their high-level, woolly and practically-ineffective draft guidance issued to date. As teacher said, 'Must do better!'"

Notes

1. *Shah and another v HSBC Private Bank (UK) Ltd* [2010] EWCA Civ 31. See 'Twin peaks – leading

cases in 2010', MLB Dec/Jan 2011; 'Suspicion on trial' and 'Not so sure about Shah', *MLB* April 2010
2. See, for example - www.fsa.gov.uk/pages/Library/Communication/PR/2011/019.shtml
3. www.fsa.gov.uk/pubs/other/rbs_group.pdf
4. www.fatf-gafi.org/dataoecd/4/38/46706131.pdf

David Blackmore *may be contacted on +44 (0)2476 466492 or +447803 073380, david@dbriskandcomplianceservices.co.uk. Report by Timon Molloy.*

Derrick ponders… Sally's secondment

Where should the secondee file a SAR, with their sending firm or where they are presently working? The position is not always clear-cut as ***Derrick Paterson*** *explains.*

As an MLRO for an accounting firm, I have had several discussions about secondments. In a secondment, the employee of one business acts as the employee of another business. The seconding business will normally receive a monetary payment from the receiving business. However, the benefit received by the seconding business may be in some other form. It may be professional development of the secondee, making him or her a more valuable employee. It may be the increased value of the receiving business to the sending business, as a subsidiary, joint venture, investment, customer or supplier.

Trust and company service providers (TCSPs) fall within the UK anti-money laundering (AML) regime. The provision of trustees, directors (including those serving as interim directors), partners and company secretaries falls within the definition of TCSP. For the purposes of this article, a secondee is someone fulfilling a role that would not trigger the provision of trust or company services. The government has issued some guidance for interim directors. The guidance indicates that the government takes a risk-based view. But there is no guidance available on secondments.

Let's consider a business, Cabbage LLP, seconding a member of staff, Sally, to another business, Radish PLC. If neither Cabbage nor Radish is within the regime there is no AML issue.

Case 1: Cabbage (seconding) not regulated, Raddish (receiving) regulated

If Radish (for example, a high value dealer) is within the regime but Cabbage (for example, an actuary) is not, then Sally should be treated the same as any temporary member of staff in Radish: she should receive AML training appropriate to the role and seniority and should make internal reports to Radish's MLRO. There is no issue if Sally does not work exclusively on Radish's business, since reports need only be made where knowledge or suspicion arises during the course of business in the regulated sector. Thus, a suspicion arising from the conduct of Cabbage's business will not be reported to Radish.

Case 2: Cabbage (seconding) regulated, Raddish (receiving) not regulated

If Cabbage (for example, a law firm) is within the regime but Radish (for example, a shoe retailer) is not, the starting point is: Cabbage will be paid for the work undertaken by Sally at Radish; is the service provided by Cabbage within the regime? If the answer is yes, then suspicions arising from the provision of that service must be reported. This is not a problem for employees other than Sally, who will treat Radish as any other customer, but what about Sally? If Sally is required to report knowledge and suspicions arising from her work at Radish because this is also work for Cabbage, then Radish's business comes into the reporting regime by the backdoor. The government's guidance on interim managers suggests that the answer is yes, Sally must report knowledge and suspicion to Cabbage's MLRO.

Some MLROs hold that, provided Sally can be totally divorced from Cabbage's management and support structure, then Sally can be treated as if he or she were not an employee whilst working as part of Radish's management and support structure. A business trying to create this argument would be well advised to seek legal advice in constructing the secondment contract. In addition, consideration needs to be given to the position of Sally. If the court (rather than Cabbage's management) considers Sally to be within the AML regime, Sally will be criminal liable if she fails to report knowledge or suspicion of money laundering.

Case 3: Cabbage (seconding) regulated, Raddish (receiving) regulated

If both Cabbage (for example, an external accountant)

and Radish (for example, a bank) are within the regime, there will still be some issues. To whom should Sally report? Cabbage's MLRO may take a similar approach to that discussed above where Radish is not within the regime, that Sally is no longer a part of Cabbage's business and that all reporting is a matter for Radish. A more pragmatic approach might be:

- Where the knowledge or suspicion arises from matters related to Cabbage's business, reports should be made to Cabbage's MLRO. For a full-time secondee, these should be few and far between;
- Where the knowledge or suspicion arises solely from matters related to Radish's business, reports should be made to Radish's MLRO;
- Where the knowledge or suspicion arises solely from a combination of matters related to Cabbage's and Radish's business, it is likely that the final straw that gives rise to the suspicion will come from Radish's business. Thus the report will be made to Radish's MLRO. However, care needs to be taken. When part of the suspicion rests on confidential information that Cabbage holds on its other clients, there should be reservations about disclosing this to an employee (the MLRO) of Radish. This is despite the *Proceeds of Crime Act* (POCA) *sections 337* and *338* stating that SARs are "not to be taken to breach any restriction on the disclosure of information (however imposed)". In these cases it may be better to make disclosure through Cabbage's MLRO. There should be no analogous issue where the confidential information is held by Radish about its customers since Cabbage would often be in a position to see it through its advice or services to Radish;
- Sally should be able to report to Cabbage's MLRO if he or she believes that this is appropriate. This may be the appropriate where Sally believes that Radish's procedures do not require a report to be made but Cabbage's do. It may also be appropriate when the suspicion relates to Radish's senior management.

I leave you with two parting points.

Firstly, if Cabbage's MLRO wishes to leave all or part of the processing of SARs to Radish's MLRO, he or she would be advised to do so only in the lack of knowledge or suspicion that there are flaws in Radish's AML processes.

Secondly, there should be no misunderstanding by Cabbage, Radish or Sally about what is expected of Sally. Cabbage may rely either on an understanding of the law or the secondment contract for the agreement between itself and Radish. It would make sense, in all circumstances, for Cabbage to brief Sally about each secondment and the procedures that will apply.

The purpose of this article is to pose questions and instigate discussion. It does not represent advice. ***Derrick Paterson*** *Dip (AML) FCA MICA is an independent AML consultant. He may be reached on+44 (0) 7732 744 56, derrick.paterson@hotmail.co.uk*

Name check: the legality and practicality of lists

Sanctions lists present multiple practical difficulties – around accuracy, transliteration, false positives, timeliness of updates, to name a few – but they can prove equally contentious at the policy and judicial levels. ***Alan Osborn*** *reports.*

Economic sanctions against al-Qaeda and the Taliban were agreed by the United Nations Security Council (UNSC) 12 years ago (Resolution 1267) and at first enjoyed strong and uncritical support. It was a new kind of sanctions regime, targeting named individuals, businesses and organisations that supported al-Qaeda rather than focusing on countries, as before. Two years later, UNSC Resolution 1373, a response to the attacks of 11 September 2001, was aimed at potential terrorists not covered by the 1267 regime, though in this case the UN left it to member countries to determine the targets.

Initially, these two resolutions seemed to betoken a welcome global consensus in the fight against terrorism. But the past 10 years have brought some disappointment for sanctions-backers as the initial political impetus faded after the Iraq war. At the same time the measures have come under rising attack in national courts, especially in France and other European countries, where numerous weaknesses and inconsistencies in the legal underpinning for the measures have been exposed. Particular grievances included the lack of any procedure for appealing against an appearance on the UN blacklists and the fact that evidence for a listing was kept secret, though in

these and other cases the UN subsequently acted to address many of the concerns.

FATF view

"All countries have issues with the sanctions, whether political or practical," said Vincent Schmoll, principal administrator of the Financial Action Task Force (FATF). The UN resolutions on sanctioning (or asset-freezing as the FATF calls it) have been incorporated in the FATF's Special Recommendation III and a country, which baulks at signing up for this "will be looked at under one of our processes and be identified as a problematic country that doesn't cooperate," he said.

"A complicating factor in Europe is that the UN resolutions are implemented at a European level, and the European mechanisms by themselves are not sufficient - they need to be supplemented to be fully in compliance with the FATF and the UN," Mr Schmoll said. The problems were different for developing countries, which, for economic reasons, had to be helped to prioritise the sanctions and "phase them in gradually according to their means," he said.

Mr Schmoll agreed that there had been problems generally. "There are a lot of requirements now, including things that have been issued by the UN in successor resolutions, and new requirements that have been put on countries. Money is not getting frozen. I can't give examples but rarely have we found situations where everything is100% OK," he said.

The FATF administrator said there were "not too many examples of blatant disregard for the asset-freezing measures." Many countries were doing their best. "The US is a good student on this because they've got the mechanisms but even they are not 100% perfect. In Europe, a number of countries have been waiting for the European measures and when they came the FATF found they were not sufficient, so we're talking about things that haven't been dealt with yet, they are not necessarily negligent," he said.

EU and UN: the *Kadi* case

Nothing better illustrates the complex, nuanced and often contradictory attitude of the European Union (EU) towards the UN sanctions than the now famous *Kadi* case. Yassin Abdullah Kadi, a wealthy Saudi businessman, was placed on the UN blacklist by a number of EU countries in 2001 but appealed to the European Court of Justice (ECJ) whose Court of First Instance (CFI) upheld the listing in 2005, only for this to be overturned in 2008 by the full ECJ on the grounds that Mr Kadi's human rights had been infringed. In overturning the CFI ruling, the full court said its judgement "must be considered to be the expression, in a community based on the rule of law, of a constitutional guarantee stemming from the EC Treaty [of European Union] as an autonomous legal system, which is not to be prejudiced by an international agreement."

This ruling proved highly unsettling to lawyers and others engaged in interpreting and applying the UN resolutions. The esteemed Columbia Journal of European Law commented that "the ECJ's *Kadi* judgment leaves us with a number of open questions regarding its effects on the structure of the international legal order. Indeed, the question must be asked whether the primacy of UN Charter obligations is jeopardised."

But this case had further to run and indeed is still active today. The ECJ's 2008 ruling was effectively stayed for three months "to allow the [EU] Council [of Ministers] to remedy the infringements found" and shortly afterwards the European Commission told Mr Kadi that it would adopt legislation with a view to maintaining his listing. In September last year, the ECJ General Court (which replaced the CFI in December 2009) annulled the regulation freezing Mr Kadi's funds, which, it said, had been adopted in breach of his rights of defence "and constitutes an unjustified restriction of his right to property." At the time of writing this annulment was expected to be appealed yet again by the European Commission, the Council of Ministers and the UK Government.

The American way

There have been no similar legal pitfalls in the US where the administration established its own list of persons and organisations suspected of helping finance terrorism through Executive Order 13224, signed by President Bush in 2001. There are differences between the US and the UN blacklists in the names of those accused – the US list covers other crimes such as drug trafficking, overlaps with other federal programmes and has over 4,000 entries, or more than eight times as many as the UN. There are also difference in the operation of the sanctions – the US allows for appeals and gives explanations of why names have been added. "We publish the full names and backgrounds of the individuals and companies, and the reasons for the listing, and issue press releases every time a name is added," said a spokeswoman for the terrorist finance division of the US Treasury. "All major US financial

institutions subscribe to this list and all have interdiction software in place and that's one of the reasons our financial sanctions have been so effective," she said.

Although most of the names on the original (and subsequent) UN blacklists were provided by Washington (at least partly reflecting its superior intelligence-gathering networks), there have been suspicions that not all the American target names were accepted by the UN, hence introduction of the so-called 'Bush list'.

Practical politics

Whatever the accuracy and relevance of the UN blacklist, there is no doubt that there has been increasing pressure to have it amended for political reasons. Last year, after an 18-month formal review, the Security Council announced the removal of 45 names from the list. This followed calls from the Afghanistan government for a relaxation of the sanctions in an effort to woo Taliban moderates and help peace talks with insurgents in the country. But there have also been pressures in the other direction: Russia is thought to have opposed delisting because of links between the Taliban and independence groups in Chechnya.

Missing details

Particularly in Europe, adherence to the sanctions has thrown up a number of operational problems. "Credit institutions have encountered considerable difficulties with the practical implementation of financial sanctions," a spokesperson for the European Banking Federation (EBF) told *MLB*, charging among other things that "the lists provided by the UN still too often do not contain enough elements of information which could enable credit institutions to properly identify sanctioned persons and organisations." The EBF has sought improved information and regular review since "these lists tend to increase rapidly in volume without any regular official process of assessment, revision, verification or deletion of the data content." The EBF also wants faster responses from the authorities and an exemption for banks from any liability when acting in good faith.

Implementation obstacles on the ground

The European Association of Public Banks (EAPB) has similar concerns about the effects of sanctions on its (mainly German) commercially active banks. One specific issue, according to Julien Ernoult, an EAPB advisor, is that "the only legally binding list in the EU is the paper version of the EU Official Journal so that although there is an electronic database, it is not legally recognised, and many banks face high compliance costs to integrate such lists into their monitoring systems."

Dirk Smet, communications manager of the World Savings Banks Institute (WSBI), said the know your customer requirements are difficult for banks with small savers sending small amounts of money from, say, Brussels to Karachi: "In these countries people don't always have an ID card, nor an address and we can't apply the same rules as for others. It doesn't make these people terrorists. Other proofs of identity should be taken into account, an electricity bill for instance," he said.

Mr Smet was optimistic that a new "lighter regime" being introduced by the FATF would help. He noted the FATF had accepted that "low capacity countries" (LCCs) have characteristics that "severely constrain their capacity to implement AML/CFT measures." These include competing priorities for scarce government resources, the lack a skilled workforce to implement government programmes and a significant informal sector, and cash-based economy. Luis Urrutia Corral, FATF President, said recently that "efforts to build strategies and establish mechanisms that continue to help low capacity countries implement the FATF standards" is a current priority for the organisation.

Money on the move

As a race, we are driven to find new (and hopefully better) ways to do old things, writes ***Sue Grossey****. As Franklin Roosevelt counselled: "It is common sense to take a method and try it. If it fails, admit it frankly and try another. But above all, try something." This drive to innovation is exemplified in the arena of financial services, and to address these new developments, the Financial Action Task Force (FATF) has recently published an update to its earlier report on the (ab)use of new payment methods by money launderers. The original report, issued in October 2006 [1] and 44 pages long only, was in essence an introduction to the subject, describing the new payment methods (NPMs) and outlining their vulnerabilities. This new report – "Money Laundering Using New Payment Methods"[2] – is much more substantial, at 117 pages, and compares the potential risks described in the 2006 report to actual risks based on new case studies and typologies.*

For those of us used to more traditional ways of moving our money around, the FATF report starts with some helpful scene-setting and definitions. As it points out, the focus of its interest is not remote banking in general (as "depository financial institutions have offered remote access to customer accounts for decades") but rather "the use of [new technologies] by banks outside of traditional individual deposit accounts and by non-banks, some of which do not fit traditional financial service provider categories and therefore sometimes fall outside the scope of regulation despite providing financial services such as the carrying out of payments or holding accounts." The popularity of NPMs is easy to understand, as they meet "the demand for more convenient or safer ways to pay for online purchases [or] a desire to provide access to financial services for those excluded from traditional financial services (eg, individuals with poor credit ratings, minors, but also inhabitants of under-banked regions)."

The naming of parts

There are three main NPMs discussed by the FATF report: prepaid cards, Internet payment services, and mobile payment services. Since the publication of the 2006 report by FATF, all three methods have developed significantly.

Prepaid cards come in two varieties: closed-loop and open-loop. Closed-loop cards are limited in their use, such as merchant-issued gift cards and transport cards (eg, the Oyster card in London). The issuer of the card or its service provider typically operates the network on which the cards can be used. Their use to money launderers is similarly limited, except as temporary value storage cards (although the FATF report does feature two case studies where closed-loop cards were used). Open-loop cards are much more flexible as they can be used across a broader range of locations (even internationally) for a wider range of purposes, eg, payroll cards and general purpose "cash cards" for individuals without a bank account or credit card. These cards are usually associated with a card payment network, such as Visa or MasterCard, which permits them to be used in the same manner as a debit card to make purchases or to get cash from an ATM. Their use to money launderers is obviously much more extensive. Although data is still sketchy, the use of prepaid cards seems to be most prevalent in the US, where 17% of consumers have one. As for Europe, a 2009 survey by an international payments processing firm described Italy as "the most advanced prepaid market in Europe", while the UK market was considered "established" and those of Germany and Austria only "embryonic".

Internet payment services (IPS) can be provided by both financial institutions and firms outside the financial services sector, and they can operate in conjunction with or independently of a bank account. There are three main types of IPS: online banking (which is not examined by FATF's report); prepaid Internet payment products ("where firms who may not be credit institutions allow customers to send or receive funds through a virtual, prepaid account, accessed via the Internet"); and digital currencies ("where customers typically purchase units of digital currencies or precious metals which can either be exchanged between account holders of the same service or exchanged against real currencies and withdrawn"). It is here that matters start to become both confusing and risky, as the boundary between IPS and traditional financial services is blurred: "Internet payment services are increasingly interconnected with different new and traditional payment services. Funds can now be moved to or from a variety of payment methods, ranging from cash, money remittance businesses (eg, Western Union), NPMs, bank wire transfers, and credit cards. Furthermore, some IPS providers have started to issue prepaid cards to their customers, thus granting them access to cash withdrawal through the worldwide ATM networks." It is not hard to see why a criminal might lick his lips at the laundering possibilities.

Finally, mobile payment services can be likewise broken down into categories. The key distinction to make is between those systems that simply allow users of traditional financial services to access their accounts and information from their mobile phones (and which are not covered in this report), and those systems that are not linked to accounts on which due diligence has presumably been undertaken. The latter come in two flavours: mobile payment services (which "allow non-bank and non-securities account holders to make payments with mobile phones – payment service providers may be non-traditional financial institutions with widely varying controls and supervision measures") and mobile money services (whereby "subscribers are able to store actual value on their mobile phone, using phone credits or airtime as tender for payment – such systems offer versatility but may often fall out of regulation and prudential supervision altogether").

Risk or reward?

Although FATF is more used to pointing out money laundering risks, its report does acknowledge that, in

some senses, the proliferation of NPMs is actually a weapon in the fight against laundering: "Where NPM providers are subject to AML/CTF [anti-money laundering / counter terrorist financing] obligations and appropriately supervised for AML/CTF purposes, NPMs can make payment transactions more transparent and help prevent corruption or other abuses. NPMs can shift customers from the unsupervised or even illegal sections of the payments market (eg, hawaladars, underground banking services) into the formal sector… A transaction carried out through a NPM will always generate an electronic record, whereas cash does not. Even where customer due diligence (CDD) measures are not applied (ie, where the customer remains anonymous), the electronic record can, in some cases, still provide law enforcement with at least minimal data such as an IP address or the place where a payment was executed or funds withdrawn."

However, three main areas of risk are identified:

- "**Absence of credit risk**: NPMs are generally pre-paid [which] means that service providers may have fewer incentives to obtain full and accurate information about the customer and the nature of the business relationship;
- **Speed of transactions**: [which] can complicate monitoring and potentially frustrate efforts to freeze the funds;
- **Non-face-to-face business relationship**: which FATF Recommendation 8 identifies as presenting 'specific' ML/TF risks due to increased impersonation fraud risk and the chance that customers may not be who they say they are."

FATF has updated its risk matrix for assessing the risks associated with individual NPMs, and now recommends considering: CDD requirements; record-keeping; value limits; methods of funding; geographical limits; usage limits; and segmentation of services (ie, who provides the services involved, and whether they are overseen and coordinated). And numerous "risk mitigants" are suggested to reduce these risks, ranging from anti-impersonation checks to monitoring and value limits.

It ain't what you do, it's the way that you do it

The FATF report then moves on to case studies, which were submitted by the 37 countries that responded to its questionnaire on NPMs. These case studies are presented under three typology headings: third party funding; exploitation of the non-face-to-face aspect of NPMs; and complicit NPM providers or their employees.

Third party funding is popular with criminals, as all three types of NPM have the potential to be funded by third parties. In an American case in 2009, for example, a number of defendants were charged with running a drug trafficking ring in a prison and receiving payment outside the prison through prepaid cards. Gang members outside the prison allegedly established prepaid card accounts in the names of the defendants, who allegedly instructed their customers – their fellow prisoners – to pay for the drugs by having family members outside the prison deposit payments into the defendants' prepaid card accounts. And over a three-year period in Canada, an individual sold stolen goods on a commercial website. The proceeds passed through an IPS account attached to his commercial website user accounts, and he sold over 9,000 items for more than US$459,000.

The non-face-to-face nature of NPMs is a great advantage for criminals: "In a number of cases NPM products were used to launder illicit proceeds gained from fraud following identity theft or from stealing money from bank accounts or credit/debit cards using computer hacking or phishing methods. Since the bank accounts or credit and debit cards were held in the names of legitimate customers, the criminals were able to use them as reference accounts for the funding of prepaid cards or IPS accounts. In such instances, the NPM providers could not detect that the transactions were actually not initiated by their legitimate customer, or detect any other suspicious activity. In other cases, stolen or fake identities were used to create NPM accounts, which were also used as transit accounts in the laundering of illegal proceeds, or to commit both criminal activities (eg, fraud) and money laundering at the same time." FATF recognises that NPM providers cannot be held entirely responsible, but also suggests that they could do more to detect suspicious activity: "Although in many of the case studies, the IPS or prepaid card provider could not have detected suspicious activity, some shortcomings in some providers' identification and verification processes and monitoring systems is likely to have contributed to the illegal activity going undetected for some time."

In an interesting case from 2006 in the US, two defendants used stolen credit card account numbers to fund 'virtual prepaid cards', which provide an account number, expiration date, and card verification value but no physical card – intended for consumer non-face-to-face transactions. The defendants then used these 'virtual cards' to overpay their tuition at a university in the US.

The university then issued a refund cheque for US$31,045 – a neat laundering method for the criminals. And in Japan in 2009, an individual illegally accessed victims' Internet bank accounts and instructed the computer system to remit ¥740,000 to a digital currency exchanger to get e-currency units. He then sold some of the e-currency units to another digital currency exchanger, and instructed the exchanger to deposit the (real) money into bank accounts that he had opened fraudulently.

Finally, FATF notes that as fit and proper tests are not generally required by providers of NPM services, the sector and its staff are vulnerable to infiltration or takeover by criminals. In one 2007 case in the US, an employee of a national chain convenience store embezzled more than US$375,000 from his employer by fraudulently loading the value onto prepaid cards. He processed routine transactions that involved adding value to prepaid card accounts which appeared to be held by actual customers, but did not take in funds to cover the transactions. Although these transactions were processed by the prepaid card company, the defendant ensured that the transactions were not being recorded internally to avoid the detection of his embezzlement.

The FATF report then provides several useful lists of red flag indicators of suspicious activity relating to the three main categories of NPM, and also describes the different approaches to the legislation, supervision and oversight of NPM services in the countries that responded to its questionnaire. It concludes with some recommendations for this rapidly-evolving sector that recognise the difficulty of taking the right AML/CFT approach with products which are designed primarily for efficiency and ease of access: "Decision makers should carefully consider: whether the AML/CFT benefit justifies the potential extra costs and efforts that may arise for institutions as well as for supervisors, financial intelligence units (FIUs) or other agencies; [and] whether there is a risk that specific measures might lead to significant disadvantages for NPM customers (eg, regarding cost or convenience of the service) and whether these potential disadvantages might tempt some customers to make their payment transactions through unregulated payment service providers instead."

For those of us still using our cheque-books and amazed by our Oyster cards, these NPMs will seem unfamiliar and perhaps frightening. But moving with the times is compulsory; even if we don't use these NPMs ourselves, we must recognise that many others already do – among them, money launderers. We don't want to be caught out like Sir William Preece, chief engineer of the Post Office, who declared confidently in 1876 that "the Americans have need of the telephone, but we do not – we have plenty of messenger boys."

Notes

1. www.fatf-gafi.org/dataoecd/30/47/37627240.pdf
2. www.fatf-gafi.org/dataoecd/4/56/46705859.pdf

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

Beyond reproach – international organisations

In all major countries, the agencies responsible for law enforcement are subject to scrutiny of their own activities – either by an external authority or by an internal department acting in response to complaints. The importance of this in the anti-money laundering (AML) sector can hardly be exaggerated, writes ***Alan Osborn****. Once an organisation is found to have harboured corrupt or incompetent elements, its authority may be destroyed forever. By and large, the supervisory machinery operated by national governments for AML appears adequate, at least on paper. But what of organisations that are beyond the reach of the conventional investigators and regulators in the different countries – not because they are unduly cunning or secretive but simply because they are not beholden to the laws of any single country in which they may operate?*

Organisations the operate in a supra-national capacity include the various agencies of the United Nations, the World Bank family, proto-official think-tanks such as the Organisation for Economic Cooperation & Development [OECD] (including the Financial Action Task Force [FATF], the world's leading AML agency), the institutions of the European Union (EU), and other regional political and economic bodies. Shouldn't these bodies be subject to the attentions of the Financial Intelligence Unit (FIU) or other such authority in the country in which they operate? Can they be overseen, and should they?

Leaving aside for the moment the fact that these organisations are, by their nature and by statute, often

immune from national legislation, the truth is that they seldom, if ever, engage in the kind of activity that the FIUs examine.

In the US, for example, the lead AML agency, the Financial Crimes Enforcement Network (FinCEN), only has authority over financial institutions. "These are generally depository institutions or money service businesses, casinos, mutual funds, some insurance companies and so on. So we don't generally have any oversight over organisations like that (international organisations) unless they have an actual bank doing business," said Steve Hudak, head of public information at FinCEN. "The World Bank is not a financial institution under our definition," he added, despite the billions of dollars it disburses.

Financial Action Task Force

At FATF in Paris, the suggestion that there could be cause for an AML investigation by an FIU into the work of international organisations like the OECD itself or the World Bank was dismissed out of hand. "A body like us does not do money laundering because it does not do financial transactions," said Vincent Schmoll, principal administrator at FATF. "These are policy-making organisations, not financial institutions or law offices," he said. Organisations like FATF and the World Bank "can be considered intergovernmental organisations - the actual members of the organisation are not the 20 or so people in the secretariat here but the individual delegates from the member countries, who are responsive on a day-to-day regular working basis," he said, "Nobody from the private sector or anybody like that is involved."

World Bank

That said, the World Bank clearly handles enormous money flows, much of it directed to private organisations and companies, and has a huge staff. What does it do to ensure that all is in order here? In reply to questions posed by *MLB*, the Bank stressed that it was committed to combating money laundering and the financing of terrorism and ensured that internal measures and procedures were in place to comply with the relevant international best practices. "Although the World Bank's risk profile is different from that of commercial financial institutions, the Bank still has appropriate measures in place for its internal operations to mitigate the risks associated with money laundering and financing of terrorism," the bank said in its statement. "The World Bank uses the FATF 40+9 Recommendations as a guide in designing systems and procedures for ensuring that the organisation's internal operations have appropriate controls to mitigate the risks associated with money laundering and financing of terrorism," it said.

International Finance Corporation

The World Bank's private sector lending arm, the International Finance Corporation (IFC) is the largest multilateral source of loan and equity financing for private sector projects in the developing world. The organisation said in a statement that "AML/CFT [combating the financing of terrorism] is taken very seriously in IFC's due diligence process and investment decision-making", adding that these procedures were applicable to all the IFC's financial products and advisory services activities.

The AML/CFT programme includes staff training, automated screening, and client and project due diligence, said the IFC. Additionally, an AML/CFT review committee (made up of representatives of a number of IFC departments) "provides further review should possible AML/CFT issues be raised during the course of IFC's client relationships." The IFC has a designated senior risk officer for AML matters.

"We know that working with reputable sponsors is critical," said Vincent P. Polizatto, chief credit officer in IFC's credit review department, "therefore, all sponsors and clients are screened against various lists using automated systems." IFC teams also conduct integrity due diligence in the marketplace. "Prior to commencing onsite due diligence, a comprehensive AML/CFT questionnaire is completed by the client. This is followed by management interviews, validation, and assessment during the due diligence visit. Appraisal documents used to make investment decisions contain the findings/conclusions of the due diligence," said Mr Polizatto.

United Nations

Where the activities of the UN and its various agencies are concerned there is an active programme against money laundering and terrorist financing carried out by the Vienna-based United Nations Office on Drugs and Crime (UNODC). The office does not have a dedicated unit charged with overseeing the activities of the UN's own personnel but all UN projects and programmes are audited by the Office of Internal Oversight Services (OIOS), based in New York and set up to assist the UN Secretary-General "in fulfilling his internal oversight responsibilities in respect of the resources and staff of the [UN] organisation through monitoring, internal audit, inspection, evaluation and investigation." While no

OIOS report to date relates specifically to money laundering, an official said that if evidence of such behaviour were found "the staff are fired immediately – the UN really doesn't like this kind of thing."

European Union

The European Union is similarly watchful for evidence of money laundering and oversees this internally through the European Anti-Fraud Office (OLAF), which is responsible for the fight against fraud, corruption and other illegal activities in the EU. "The concept of illegal activities affecting the EU's financial interests includes laundering of the proceeds of Community [EU] fraud (as defined in Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering)," said Pavel Borkovec, OLAF spokesman.

He noted that under the second protocol to a Convention on the protection of the financial interests of the European Communities, member countries were required to take steps to prevent EU funds being used to assist money laundering or to help crimes that would generate dirty money, which would then require laundering. Under its terms, member states have to protect EU funds by establishing money laundering as a criminal offence; ensuring legal persons can be held liable for fraud, active corruption and money laundering, and when found liable, ensure that they may be punished by effective, proportionate and dissuasive sanctions; and enable the confiscation of the proceeds of fraud.

In practice, OLAF works closely with national law enforcement bodies and judicial authorities and is a part of CARIN (Camden Asset Recovery Inter-Agency Network), an informal group that aims to tackle money laundering and other crimes through the exchange of information.

Once a possible crime is discovered by OLAF, the matter is referred to the national judicial authorities. A recent example is the investigation by OLAF into unlawful use of parliamentary allowances by Tom Wise, a UK member of the European Parliament, which led to criminal charges for money laundering and false accounting being brought by the UK police. During the court hearing, and after negotiations, a judge quashed the money laundering charges, but upheld the false accounting charge, landing Mr Wise with a two-year prison term.

Some large international organisations place themselves at the heart of the fight against money laundering without actually subjecting their own operations to regulation. One such is the European Bank for Reconstruction & Development (EBRD), owned by 61 countries, the European Union and the European Investment Bank, whose mission is to help countries across central Europe and in central Asia become open, market economies. "Although the EBRD is not regulated, as such, it is nonetheless close to the forefront of, and helps to promote, developments in both strategy and delivery," said spokesman Anthony Williams. "The EBRD takes the AML, CFT and anti-corruption themes very seriously - both internally, in its numerous investments in its countries of operations, and in its promotion of AML and other initiatives," he added.

Serbia – road blocks

Serbia's ambition to join the European Union (EU) is proving problematic on a number of fronts, with the country's control of money laundering a major hurdle. ***Mark Rowe*** *and* ***Zlatko Conkas****, in Novi Sad, report.*

February 2010 saw a wave of 50 arrests in Serbia in connection with a US$27 million money laundering and tax evasion investigation. The accused, Serbian police allege, were members of a group of company bosses suspected of creating forged sales and services documents, which generated "illegal turnover of €4 million."

Formal charges have yet to be laid against most of the men but the arrests, along with some high-profile seizures of homes and cars by the government's Directorate of Management of Temporarily Seized and Confiscated Assets (under Serbia's Ministry of Justice) prompts the obvious question: is this a sign of rigour by the authorities, or of endemic weaknesses that promoted widespread financial crime in the first place?

The European Commission described money laundering in Serbia "as a cause for concern" as recently as November last year in its Serbia 2010 Progress Report. [1] Brussels however welcomed a revised action plan for implementation of an anti-money laundering (AML) strategy, and the fact that Serbia's FIU (financial intelligence unit), the Administration for the Prevention of Money Laundering (APML) - part of the finance ministry - held further training events for its staff and carried out awareness-raising activities for suspicious

transaction reporting entities. In June 2010, Serbia acquired observer status in the Eurasian Group on Combating Money Laundering and Financing of Terrorism, a region FATF-style regional body (FSRB).

However, the Commission report concluded that the practical results of Serbia's fight against money laundering have been few and its FIU lacks capacity to systematically identify suspicious cases. "Cooperation between competent authorities has continued to show shortcomings," its authors wrote, "Reporting remains poor, in particular outside the banking sector, with the real estate sector and currency exchange offices being of most concern. An effective system for monitoring and analysing cash transactions is not in place. The judiciary and law enforcement services lack expertise in handling money laundering cases and financial investigations."

A spokeswoman for the European Commission's internal market directorate general added: "An effective implementation of the EU acquis [all EU law] in the area of anti-money laundering is an indispensable and crucial element for all accession talks to the EU."

The key Serbian law governing money laundering is the March 2009 *Law on the Prevention of Money Laundering and the Financing of Terrorism* – this governs the competencies of the FIU, while Article 231 of the Criminal Code of Serbia defines money laundering as a criminal offence.

Under the AML law, the FIU has the power to freeze transactions for up to 72 hours, and order monitoring of an account for as long as three months following a freezing order - if there are reasonable grounds to suspect money laundering or terrorist financing.

Another statute, the *Law of the National Bank of Serbia 2009*, includes guidelines for assessing the risk of money laundering and terrorist financing in financial transactions. 'Red flags' identified include: significant and unexpected geographic remoteness of the client's location from where they do business; frequent and unexpected establishment of similar business relations with several banks; entry into several short-term voluntary pension fund membership agreements; and unexpected goods or services purchases in foreign countries; it cites as an example "the importation of bananas from Siberia".

Despite this progress, Dr Mark Galeotti, of the Centre for Global Affairs, New York University, told *MLB*: "Serbia is a pretty problematic case. Criminality had become so deeply entrenched that it created a problem between the modernisers who wanted something to be done and an established rump that is much more overtly criminal – that makes it very difficult to really know what is going on. The AML measures have to take place in the wider context of taking on organised crime." The underlying challenge is that money laundering in Serbia is generally of the darker variety. "It's not really about crime in white collar jobs," he said, "The sort of money laundering that takes place in Serbia is generally sharp-end stuff – people trafficking, guns and drugs."

The most recent assessment of Serbia by the Council of Europe's Moneyval Committee, its third evaluation round, was published in February 2010. The report highlighted progress since the previous 2005 evaluation, noting that the new 2009 anti-money laundering and terrorist financing law had been accompanied by substantial amendments to criminal legislation around the liability of legal entities and the seizure and confiscation of the proceeds of crime. It also described Serbia's money laundering offence as "largely in line with international standards" and noted that it had been successfully tested in practice, with several convictions achieved. The report noted the strengthening of Serbia's financial intelligence unit (FIU) and judged it generally effective, although understaffed in light of added responsibilities under the 2009 law. Customer due diligence and record keeping requirements are also now broadly in line with the international standards.

However, the report also identified shortcomings in Serbian legal definitions of terrorist financing: the current system for investigation, prosecution and adjudication of different types of money laundering and terrorist finance offences is characterised by practical difficulties in cooperation and communication between competent authorities. In particular, there were concerns about the operational autonomy and independence of the prosecution service and the heavy workload and under-resourcing of the judiciary, specialised law enforcement services and supervisory bodies. In consequence, the laws authorising provisional measures and confiscation appear to have been little used. The report also found that Serbia's complex legal framework hindered the authorities from taking "the necessary preventive and punitive measures" to freeze and seize terrorist-related funds or other assets without delay, in accordance with relevant United Nations resolutions. Another key shortcoming, according to the Moneyval report, is that while banks have increased their reporting of suspicious transactions (the most recent data from the US Department of State is that in 2007 the APML received 2,034 suspicious transaction reports, and 2,087 in 2008, the vast majority filed by commercial banks), "there is a low level of understanding and implementation of the reporting requirement by non-banking financial institutions."

Moneyval also doubts whether detection of cross-

border movement of currency is adequately pursued: Article 67 of the 2009 Law requires any person who crosses the state border carrying physically transferable payment instruments valued at €10,000 or more to declare this to the competent customs body.

A progress report released by Moneyval in December 2010 underlined that Serbia continued to make progress across the board but with some key caveats. It noted, for instance, that Serbia's new anti-money laundering and combating the financing of terrorism (AML/CFT) rulebook, which remains the only implementing regulation governing suspicious transaction reporting, does not address in detail the reporting of terrorist financing.

Similarly, the report said that it was not clear whether all financial institutions had developed lists of indicators to assist in identification of suspicious transactions. Moneyval also had concerns, for example, about Serbian attempts to criminalise terrorist financing, and its failure to issue guidance on the risk-based approach for setting customer due diligence policies.

Aleksandar Vujicic, the APML's director, dismissed these reservations; he told *MLB*: "The fact that 132 persons in Serbia are currently accused of money laundering says the opposite." Serbia's legislation was now sufficiently comprehensive, he said, and its police, prosecutors and courts equipped to "send a message to society that these crimes are not worth committing in Serbia." The APML would continue to play an active role, he added: "A systemic solution, not occasional actions can and will lead to significant results. Two years ago there were only two judgments for money laundering in Serbia, of which one was final and now that number has increased to 13 judgments, of which six are final."

The chief official (state secretary) at the Ministry of Justice, Slobodan Homen agreed: "The increase in number of cases and judgments in the past three years is encouraging," he said, a sign that there was "political will" to tackle the problem. A good example was 'Balkan Warrior', an international anti-organised crime initiative led by prosecutors and police forces from Serbia, Montenegro, Slovenia, Croatia, Italy and Uruguay. A key target is the criminal network of Serbian drug boss Darko Saric, which has spread into many Balkan countries. The project has been a success, leading to indictments for both money laundering and predicate crime. In April 2010, Serbia's state prosecutor office charged Darko Saric and 19 supporters (including lawyers and businessmen) with drug trafficking offences, including conspiracy to commit criminal acts, unauthorised distribution of narcotics, falsification of documents, illegal possession of arms and explosives, assisting an offender and unlawful manufacture, possession, carrying and transportation of weapons and explosives. Money laundering charges followed in August: "Darko Saric and eight others were charged with laundering more than €20 million of drug trafficking money," said Homen. The investigation revealed that the group had "purchased more than 10,000 land acres in Serbia's province of Vojvodina, four hotels and many companies using narcotics trafficking money."

The case, he said, "shows how the drug trafficking money was laundered and invested in construction, agricultural land and catering" in Serbia. Financial investigations continue and new charges are expected. 'Balkan Warrior' demonstrated "the true image of Serbia's orientation in the fight against all forms of crime, including money laundering," Homen asserted.

Notes

1. http://ec.europa.eu/enlargement/pdf/key_documents/2010/package/sr_rapport_2010_en.pdf

Ecuador – the calm after the storm

For those doubters who claim that the Financial Action Task Force (FATF) does not have much clout, the case of Ecuador makes instructive reading, writes **Pacifica Goddard**. In February 2010, the Paris-based standard setter issued a stinging criticism of the South American state [1], listing Ecuador as a state with serious anti-money laundering/ counter terrorist financing (AML/CTF) deficiencies, in company with the likes of Angola, Ethiopia and North Korea.

Ecuador, FATF said, was among the "jurisdictions with strategic AML/CFT deficiencies that have not committed to an action plan developed with the FATF to address key deficiencies as of February 2010… Despite the FATF's efforts, these jurisdictions have not constructively engaged with the FATF or a [FATF-style regional body]… and have not committed to the international AML/CFT standards."

FATF suggested that Ecuador work with it and GAFISUD (Financial Action Task Force on Money Laundering in South America) to address a series of

failings. First, it had to adequately criminalise money laundering and terrorist financing; second, it needed to establish and implement adequate procedures to identify and freeze terrorist assets, while implementing the same for confiscation of funds laundered; and third, it needed to reinforce AML/CTF efforts in the financial sector. Although Ecuador had engaged with FATF and GAFISUD, it had "not delivered a clear high-level political commitment to address these deficiencies."

All of which makes for a poor school report. Initially the Ecuadorian government responded with shock and indignation. Ecuador's Association of Private Banks (ABPE) and even the President Rafael Correa claimed that the assessment was motivated by FATF objections to the country's economic ties with Iran.

"What arrogance! And why? Because we have relations with Iran. That's it," President Correa said at his weekly town hall meeting after FATF's public statement. "This is imperialism in its most base form... This has nothing to do with the struggle against money laundering or the fight against the funding of terrorism." President Correa spoke publicly of possibly cutting all ties with FATF.

Experts were not convinced, however. Dr Catalina Carpio, Director of CONTYCOM CIA LTDA, a law firm in the capital Quito, which focuses on AML, dismissed this rhetorical reasoning. "They put us on the FATF blacklist for not having a law against the financing of terrorism and because we didn't pass [reforms proposed by FATF's]… evaluation of 2007. The government of Rafael Correa politicised the theme, saying that it happened because of the negotiations with Iran; this was their populist argument to strengthen themselves politically in front of the majority of Ecuadorians, who know absolutely nothing about the laundering of assets," she said.

And it is true, until 2005 Ecuador had no specific AML laws. Pedro Ceballos, a lawyer with Ortega Moreira, Ortega Trujillo &Associates, explained: "Before the approval of the [2005 money laundering] law the prosecution of money laundering in Ecuador was directly attached to the now extinct article 74 of [Ecuador's] 'drug law', which carried a prison term of between four and eight years for money laundering connected with narcotics trafficking. Other crimes that might lead to money laundering (such as smuggling, frauds, etc) were not included."

Before 2005, the only recourse for prosecutors faced with money laundering ancillary to crimes other than drug trafficking, was to secondary legislation directed at concealment of illegally acquired and sold goods and services rather than the money they generated. 'Rules for Concealers' in the 44th article of the Penal Code carried a maximum sentence of one quarter of that applied for a predicate offence.

Ceballos illustrated how the law worked: "Before 2005 if 'A' had an illegal whisky smuggling business that gave him a small fortune, everything that his sons 'B' and 'C' did with that money (which came from the illegal activity) could not be addressed as a money laundering issue. 'B' and 'C' could only be treated as concealers of the whisky smuggling crime of 'A' and their sanction could only go up to one quarter of the sanction given to 'A'."

However, this situation was significantly improved under the *Anti-Money Laundering Act (Ley Para Reprimir el Lavado de Activos)* of October 2005, supplemented by Decree 1328 of 24 April 2006, which contained 'Anti-Money Laundering Regulations'. The legislation is 'all crimes' and money laundering carries up to nine years in prison.

Ecuador also launched its Financial Intelligence Unit (FIU), the Unidad de Inteligencia Financiera, in 2006, under a National Council against Money Laundering (El Consejo Nacional Contra el Lavado de Activos - CNCLA), which devises and approves plans to prevent money laundering in the country. The CNCLA is presided over by Attorney General Diego García, and includes representatives of the country's internal revenue service, the customs service, the national police, the public prosecutor, as well as the government's Department for the Control of Business Organisations and the Department of Banks.

Dr Carpio says that the FIU has been reasonably effective, for instance in suspicious transaction report training. It has also monitored, as required by law, compulsory notifications on the creation of new financial institutions such as brokerage houses, trusteeships, cooperatives, notaries, property and commerce registrars, and real estate agencies. "The FIU has made a lot of efforts to execute these policies, especially in the last two years," said Carpio.

But progress has not been sufficient for FATF. In particular, Ecuadorian legislation still does not contain any reference to terrorist financing.

Carpio blamed regional politics: "The laws don't address the financing of terrorism as such, because the opinion of the Ecuadorian government is that the [leftist] FARC (The Revolutionary Armed Forces of Colombia) are to be thought of as an insurgent group, not as terrorists." Foreign relations with the right-wing

Columbia government remain frosty because of its tacit backing of FARC, and, noted Carpio, "if the Ecuadorian government officially referred to the FARC as terrorists, they would have to get involved in the fight against them as well as officially support actions by Colombia and the United States against them." There are nonetheless articles that sanction terrorism within Ecuador's penal code, she said.

Despite this central issue, and the heady anti-FATF rhetoric, Ecuador has addressed some of the organisation's primary concerns, for example, by improving procedures for both freezing and seizing illegal assets. The government has also reformed its prosecutorial system, increasing the integration (and, hopefully, efficiency) of district attorneys; 12 from the FIU have been instructed to look at money laundering, human trafficking and drug trafficking as interconnected rather than isolated activities, with the ultimate goal of more effectively and speedily identifying and pursuing serious criminals. In March last year, the government sent judges, attorneys and police to the US embassy to receive specialised training in recognising and fighting money laundering.

The reforms reaped dividends: during its June 2010 plenary, FATF removed Ecuador from the blacklist. In October it explained: "In June 2010, Ecuador made a high-level political commitment to work with the FATF and GAFISUD to address its strategic AML/CFT deficiencies. Since June, Ecuador has taken steps towards improving its AML/CFT regime, including by tabling a revised AML/CFT law." However, FATF also noted that "certain strategic AML/CFT deficiencies remain," including all those set out in February 2010, but that "Ecuador will work on implementing its action plan to address these deficiencies."

Asked to comment, an FATF spokesperson said that the agency was "not in a position to provide any additional details at this time. We are continuing to work with Ecuador, and the FATF will again discuss the situation regarding Ecuador at our [February 2011] plenary meeting."

Ceballos believes that Ecuador is doing a very good job: "From the insider's point of view, Ecuador's current financial system does not easily permit money laundering; there are strictly controlled procedures over deposits and huge transactions are watched meticulously. The FATF should also know that Ecuadorian police enforcers yearly destroy millions of dollars of drugs that have been confiscated, and that many illegal drug facilities are discovered and destroyed…"

Ceballos acknowledged that strong laws alone are not enough: "The main problem facing prosecution of AML crimes has to do with the behaviour of certain prosecutors and judges. Many cases of money laundering do in fact go through a deep investigation stage but few end in condemnatory sentences. The process is often influenced by the economic power that those involved in the crime have on the community."

To combat money laundering with more than just words he recommended the government appoint additional better trained and prepared prosecutors and judges, on higher salaries and provide them with greater security. "Also, many money laundering crimes come from international drug trafficking, so we need more mutual collaboration between the various countries of the region, particularly with our neighbour Colombia."

Notes

www.fatf-gafi.org/dataoecd/34/29/44636171.pdf

Editor: Timon Molloy • Tel: 020 7017 4214 • Email: timon.molloy@informa.com
Editorial board: Jonathan Fisher QC – Member and Financial Crime Team Leader, 23 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: Frida Fischer
Marketing: Naeemah Khan • Tel: +44 (0) 203 377 3847 • Email: naeemah.khan@informa.com
Sales: Mike Ellicott • Tel: +44 (0) 20 7017 5392 • Email: mike.ellicott@informa.com
Renewals: Helen James • Tel: +44 (0) 20 7017 5268 • Email: helen.james@informa.com
Subscription orders and back issues: Please contact us on 020 7017 5540 or email subscriptions@informa.com.
For further information on other finance titles produced by Informa Law, please phone 020 7017 5540.
Printed by Premier Print Group
ISSN 1462-141X

Published 10 times a year by Informa Law, Telephone House, 69-77 Paul Street, London EC2A 4LQ. Tel 020 7017 5000. Fax 020 7017 4601. http://www.informa.com

Informa UK Ltd. Registered Office: Mortimer House, 37/41 Mortimer Street, London, W1T 3JH.
Registered in England and Wales No 1072954.
This newsletter is printed on paper from sustainable forests.