

It wouldn't be the first time that a flush of reactive zeal got the better of regulators' judgement. The result in Europe, with anti-money laundering (AML) measures as with many other financial services sector regulations, is a shuffled partial retreat but no surrender. It is a shift from what Jackie Harvey, an AML specialist at Newcastle Business School in the UK calls a "fear-based approach" to compliance, marked by the reporting of 'unusual' rather than 'suspicious' activity, towards a risk-based approach.

Risk mitigation is, after all, an easy sell. "If you're not secure, you're in the newspaper, and you don't have a business anymore," Serge Moreno, head of global information risk management, ING Bank, recently told a seminar organised by Comsec Consulting. "It's the first and basic requirement for doing business." Yet, it is not clear that the level of threat to bank's systemic (or literal) security justifies the regulatory sledgehammer often applied to it. Harvey claims there is little proof to substantiate money laundering numbers that have been "repeated so often they've become accurate".

"No-one's denying that money laundering happens," Harvey says. "But it's assumed to be enormous – that we need more and more powers to combat it. But there's no proof about the numbers." The International Monetary Fund estimates that global money laundering is worth between 2% to 5% of global GDP, however



Coming clean

Banks are basing anti-money laundering (AML) measures on questionable incidence data, say some analysts. They also maintain that AML solutions have not adequately addressed terrorist finance, the basis for much of the AML legislation. Shayla Walmsley investigates.

these are 1999 figures. Harvey is not alone in questioning the scale of the risk putatively addressed by legislation such as the Patriot Act in the US and EU directives on AML. Peter Alldridge, a professor at London University and adviser to the UK parliament and the European Commission on AML, is critical of the regulatory approach to date. He argues that it addresses a problem that doesn't exist – at least not

on the scale anticipated by regulators – and that it doesn't work. "Money has been laundered for many years without any damage to financial institutions," he says. "BCCI didn't go under because of money-laundering. It went under because it stole its customers' money.

"Can you have a serious impact on the incidence of money laundering with attempts to control it?" he asks,

somewhat rhetorically. Roy Harari, managing director, Comsec Consulting UK does not think so with the current strategies. “The chances of success are not great,” he says. “Over five years, [UK enforcers] haven’t paid their own salaries.” Harari identifies one major problem with present approaches to money laundering – the fact that they focus almost exclusively on external risk. In fact, he says, the risk is more likely to come from, or at least involve, insiders. Take the various “Leumi affairs” involving one of Israel’s largest banks; a clerk is now on trial for embezzling money described by the Tel Aviv fraud unit in a recent report as “not kosher and possibly laundered” from foreigners’ bank accounts.

Wrong focus

“Money laundering in many cases requires co-operation from someone within the bank itself, and while all statistics indicate that the majority of other potential threats to organisations’ information and assets still comes from within the organisation, banks still dedicate the majority of their prevention and detection efforts to tackling external sources of risk,” says Harari. “There is higher awareness and investment than in the past, but in general terms the investment proportion between internal and external risk potential is still wrong.” Some of the strongest legislation has been introduced putatively to tackle the issue of terrorist finance. The third European AML Directive, to be

introduced this year, echoes much of the anti-terrorist emphasis of the US Patriot Act passed in 2001 in the aftermath of 9/11. It will not only end anonymously held accounts and apply checks to transactions valued above EUR 15,000, but will also impose checks on “politically exposed persons” – albeit in contradiction of its own risk-based approach.

Yet, the issue of terrorist financing is

not entirely unproblematic. Alldrige saves his harshest criticism for the regulators who he says have missed the point. “They like to talk about terrorist financing but terrorism just doesn’t cost very much,” he says. “The attacks in London in July 2005 cost – maximum – GBP 3,000 [USD 5,900]. An 18-year-old can borrow that from a bank. The idea that you’ll have an impact by following money flows is difficult to substantiate.” Even if money

Private banking comes under the spotlight

In his latest book, “The Washing Machine – Money, Crime & Terror in the Offshore System” (*Duckworth*), Nick Kochan, who has written extensively on bank fraud, business crime and intelligence for the *Financial Times* and *The Economist*, expounds on how non-bank channels including the arms and diamond trades are used to finance terrorist or illegal activities.

He argues that today’s AML policies are “convenient and cheap” for governments as most of the onus is placed on “the legitimate banking and financial system.” Yet, he says, intelligence agencies working with police are likely to be “more effective” in preventing terrorist trade than banks, as most of this trade occurs in the “underground economy”.

Kochan also outlines how practices within the private banking business helped facilitate money laundering in the 1990s. Nigerian government lawyers named 36 banks, including leading US, Swiss and UK firms, in

response to allegations that former Nigerian president Sani Abacha allegedly used international bank accounts to transfer funds he had taken from the national treasury. Kochan points to international banks’ failure at the time to conduct adequate security and identity checks on individuals and companies to ensure that details they gave were correct.

He is also critical of the ‘secretive’ nature of private banking, given that banks helped set up “special name” accounts and shell corporations. He says private banks were “hugely embarrassed” by the findings of the US Senate’s Permanent Subcommittee on Investigations’ 1999 report, “Private Banking: A Case Study of Opportunities and Vulnerabilities.” This resulted in the establishment of the Wolfsberg Principles on Private Banking, which required banks to investigate the “bona fides” of politically exposed persons before giving them a bank account.



flows are followed, banks often fail to spot the weak point. In any case, according to Harvey, “terrorists will shift cash regardless of legislation”.

Whether or not they accept official numbers on the incidence of money laundering, banks have to comply with AML legislation. In the US, regulators have already issued USD 22 million in non-compliance fines, according to consultancy Mercator. For Investec, the risk-based regulatory approach formalised what had in any case been the bank’s modus operandi. “Not much changed for us [as a result of the risk-based approach being introduced],” says Investec’s money laundering reporting officer, Simon Wilkin.

There appears to be a divergence between a risk-specific approach and an enterprise-wide approach in terms of translation between banks and solution vendors. Banks needed to solve a problem – compliance with regulation. Vendors need to sell (and keep selling). They have moved on from providing box-ticking software and with typical prescient market savvy, are looking at the leverage regulation can give them to embed enterprise-wide systems.

Mercator recently published a report claiming that spending at the high end of the vendor market would increase 20% in the financial services industry by 2010 (compared with 5% outside that sector). “Banks have been forced to become more sophisticated,” says Rosemary Turley, marketing director at financial crime and compliance

Simon Wilkin, Investec

We don’t know how our risk assessments appear compared to those of our peers. It’s difficult to review because our products, clients and distribution methods will be different to those of another bank.

products and services vendor, Norkom. “In the early days there was a frenzy of activity and a variety of systems. There was nothing wrong with that. It met a need, but banks also didn’t know any better. Now they are thinking: ‘If I have to invest, what else can I look for?’” Turley says the majority of banks have multiple systems in place in various divisions – and that will continue. “They’re looking for commonalities, working with existing technologies, infrastructures and hierarchies in place,” she explains. “Banks have always built previous systems by system, not by business. Systems need to identify common points of information across the business. They want to integrate detection, not restructure the company.”

Swedish bank SEB, for instance, recently signed an agreement for the installation of Erase AML technology that works across channels, products

and (in this case) 18 countries in three regions. Even if they do not buy wholesale revamps, risk-based approaches involve banks scouting risk across more than just operations and over time. Exposure is neither static nor only localised. Norkom claims to have addressed this problem with a customer due diligence system, which has been adopted by European bank Fortis, that monitors risk assessments made at account-opening through the lifecycle, based on incoming transactional and behavioural data.

Potential for risk everywhere

“The important thing is to monitor the risk,” says Wilkin of Investec. “You record the risk but then you have to review it regularly. The danger is that the risk isn’t what you thought it was. You also need to consider all the potential risk sites. Consider it



Roy Harari, Comsec Consulting

Money laundering in many cases requires co-operation from someone within the bank itself ... [yet] banks still dedicate the majority of their prevention and detection efforts to tackling external sources of risk.

everywhere – in product forums and product development, for instance. You need to consider these risks, even if you decide there is no risk.” (“That’s the difficulty of our job,” Moreno of ING stated at a seminar organised by Comsec Consulting. “We have to make sure there’s silence – and how do you measure silence?”)

So does the return (compliance) justify the banks’ investment in solutions for detecting money laundering? It is difficult to tell – firstly, because banks are understandably reluctant to detail their expenditure and, secondly, because high figures are not necessarily a proxy for compliance. They could, for example, signal corporate inefficiency. Analyst firm Celent estimates that financial institutions in Asia, Europe and the US spent a total of EUR 4.5 billion on AML programs in 2005. One AML vendor that wished to remain anonymous commented on financial-i’s blog, *FinancialTech Insider*, that while AML software provided a decent detection

system, it was difficult to tell “how much it [helped] curb/reduce/identify deliberate money-laundering acts”.

What is still lacking, argues Wilkin – and what regulation has done nothing to address – is a benchmark to measure success. “We don’t know how our risk assessments appear compared to those of our peers,” says Wilkin. “It’s difficult to review because our products, clients and distribution methods will be different to those of

another bank. It’s impossible to benchmark, really. We’re a small bank. I mean, how would we measure ourselves against a Merrill Lynch?”

What is certain is that the regulation will keep on coming, although it is more likely to be in the form of piecemeal amendments and minor re-thinks than in a fresh avalanche. The problem for banks is not AML regulation per se, but that it’s a continuous and constantly changing process. It is not just about systems and solutions. It also involves changes in regulations, policies and processes. “It’s not that I have an AML wish list,” says Wilkin, “but what I would like to see is a period of consolidation to enable us to bed in changed policies and procedures.” The head of risk at a UK subsidiary of one of Israel’s three largest banks says there will always be more regulation. “But we don’t expect any dramatic changes. We’ll still be looking for the same things, with the same monitoring. We’ll still flag issues up and, if need be, report them.” //

Bloggers on terrorist financing

David Nordell, founder and CEO of New Global Markets, a start-up company developing a comprehensive customer intelligence system for industries that are vulnerable to money laundering and terror financing, and regular contributor to “*The Terror Finance Blog*,” stated in a comment on financial technology blog, *FinancialTech Insider*, that the sums of money being laundered or used to promote and finance terrorism are indeed large. “However, the whole use

of government blacklists is largely counterproductive and designed to make the regulators look as if they are doing something (to quote one very senior compliance official at a European Tier-1 bank, the blacklists are ‘lousy’),” he stated.

Nordell claims that the whole regulatory regime is designed to give the appearance of action rather than to identify or catch criminals and terrorists, both because it forces compli-

ance officers to file huge numbers of useless suspicious transaction reports (STRs), and because it leaves national financial intelligence units swamped with so much paper that they can’t even prioritise what to investigate. According to Nordell, when it comes to large sums of money used in criminal or terrorist activity, non-bank channels such as money transfer networks or mobile phone systems are used.