Nick Kochan
Investigative journalist & freelance writer

079 7329 7490
author@kochan.co.uk

Politically exposed persons

published in The Wall Street Journal

Regulators across Europe are tightening the pressure on every participant in the financial system to raise their anti-money laundering controls as fears grow about terrorist financing. Banks are being forced to invest heavily in new technology, staff training and improved compliance procedures. These will feed through into improved due diligence and quicker checking of customer profiles, and of sources of funds.

Regulation of banks' anti-money laundering system is being driven by The European Union which is currently conducting a consultation throughout the banking community for a Third Directive on money laundering. This has five key components.

First, banks must scrutinise more closely the 'beneficial ownership' of funds. Second, they are prohibited from opening 'anonymous accounts, anonymous passbooks or accounts in fictitious names'. Third, they must give additional due diligence when customer 'has not been physically present for identification purposes.' Fourth, banks are discouraged from accepting correspondent banking relationships with 'shell' banks, that is institutions lacking a physical presence anywhere in the world. Finally, banks must tighten their checks on politically exposed persons (PEPs) and other individuals on international black-lists.

The investigation of PEPs puts particular strain on banking technology as the term is extremely wide-ranging. The Directive defines the PEP as 'Natural persons who may involve a reputational risk and who or who have been entrusted with prominent public functions, such as heads of State or of Government, senior politicians, senior Government, judicial or military officials, senior executives of state-owned corporations, important party officials and close family members or close associates of all of these.'

Scrutiny of the kind envisaged by the Directive will expose banks to considerable expenditure on technology. This will greatly exceed anything anticipated by banking regulators, governments or the banks themselves. The UK Government, for example, has advised banks and financial institutions to budget £120 million to comply with its money laundering laws. This is a gross underestimate, says Martyn Bridges, a director of Bridges and Partners, a UK consultancy. 'Those figures don't cover 10% of the true cost. The cost to UK banks would be up to a billion pounds a year, assuming that everyone complied, which they won't.'

Nigel Morris-Cotterill, chairman of Anti-Money Laundering Network, speaking from Kuala Lumpur, Malaysia, says that 'one UK high street bank has already spent $30m on technology. The £120 million is a drop in the ocean compared to the technology costs that they want banks to meet.' Morris-Cotterill was not prepared to name the bank. Jeremy Thorpe, the director of the British Bankers Association responsible for money laundering, speaking from London, said that the UK Treasury's figure was a 'huge underestimate' and he thinks banks should budget at least £250 million for compliance with the European Union Directive.

These massive banking budgets will be spent on two forms of technology. The first, called rules-based technology, enables banks to examine lists of individuals whom the US Treasury and the Bank of England, among other international financial regulators, have designated high risk money

079 7329 7490
author@kochan.co.uk

launderers or terrorists. List-based checking is used by smaller banks, or savings or mortgage banks says Morris-Cotterill. 'It is doubtful whether a savings bank needs this degree of sophistication. They probably already.have sufficient data and they can interrogate the database. They need relatively simple interchange facilities.'

Smaller banks do not need their own list-checking software, says David Douglas, chairman of the UK consultancy Arbiter, which acts as an oursourcing agency for banks. 'Mortgage institutions with large quantities of low value clients buy in list-checking facilities rather than spend heavily on time and software. Once they have done a search on all their existing clients, they are likely to use the software only occasionally when they have new clients.'

Global banks with multiple branches in many countries which complete huge numbers of transactions, require much more sophisticated systems. These are based on mathematical algorithms and must be capable of monitoring transactions against an account or customer history to see if a transaction falls outside an existing pattern or creates a new pattern that is suspicious.

This technology has been pioneered by experts in artifical intelligence, says David Porter, the head of risk at UK consultancy Detica. But Porter warns that 'a piece of software needs time to work out patterns of banking behaviour. Until that is established, it is likely to be very sensitive to suspicious reports and throw out numerous false positives.' False positives are results that are incorrectly adjudged suspicious. Porter advises banks that regulators are impatient with banks facing teething problems with their systems. 'The regulators will come down heavily if they find a bank neglected to follow up a suspicious report, even if its systems are not calibrated correctly and they are pouring out huge numbers of reports which are almost all useless. Banks should not be lulled into a false state of security by having the latest technology. The people who can operate it are just as critical.'

Ironically, the complications that banks now face with anti-money laundering technology are substantially of their own making. Today's complex systems only replace the tried-and-tested checks the bank manager used to apply when he had a dubious customer. Paul Pacifico, a director of Penumbra Partners, a London-based consultancy, says, 'If you look into a customer's eyes, you can see if he is honest, and if money he presents to you is clean. But that contact has gone, so banks are forced to automate their checks. Now they are having to find new ways of monitoring customer transactions.' The British Bank Association's Thorpe says the risk is exacerbated by growing turnover of bank staff, which means tellers do not even recognise customers that they do meet in the branch, let alone the majority that now come nowhere near a bank's offices.

Banks who fail to make the investment in technology and human resources appropriate to the gravity of today's heightened state of suspicion, face a two-fold risk. First, regulators, like the UK's Financial Services Authority, are imposing heavy for systems failures. Second, the institution who is fined will suffer damage to its reputation among customers and counterparties. The worst outcome, but least predictable, is the discovery of terrorist money in a bank's books. Banks would say that can happen in the best-run institution.