Nick Kochan
Investigative journalist & freelance writer

079 7329 7490
author@kochan.co.uk

The case for a new discipline in fighting terrorist finance

The term is as emotive as it is ominous. 'Terrorist finance' sends a shiver through any manager of a bank, any compliance officer, any police or customs official. The use of your bank by a terrorist to finance his activity is unthinkable. The opprobrium from the public and powers-that-be is likely to be disastrous for years to come.

Doing nothing in the face our ongoing threat from terrorist financing is not an option. But what? That is the bank's dilemma.

First, understand that conventional anti-money laundering tools do not suffice. TF and AML are emotively linked. The rhetoric post September 11 muddied the waters. Systems that detect terrorist money are differently programmed to those set to ring at a money laundering suspicion.
Why and where is the difference? Just as speeding cameras are programmed to detect the behaviour of vehicles, so bank systems, with basic AML software, detect the erratic or unusual behaviour of money. But to continue the analogy with money laundering systems, we are now asking cameras not just to detect if the car is going too fast, but also if the driver is drunk.

Where is the difference? First, the terrorist dollars are likely to be packaged in small parcels so that they do not cause the creation of a suspicious activity report. It comes as no surprise to professional trackers of terrorist money that transactions by the 9/11 terrorists attracted not a single SAR.

Second, the terrorist uses the financial system in exactly the same way as most honest users, that is to move money in a straight line from one point to another. The result, terrorist money in its vanilla package will be lost amidst the many millions of innocent transactions.

We need to think outside the box. The wise bank must consider how it could figure in the terrorist's plans. Notice, I say 'could'. Money launderers are virtually certain to use banks, for the simple reason that that is where the money is. The same certainly does not apply for terrorists. But that should not be allowed to be an excuse to lower your guard against the possibility that they might. And that bank might be yours.

The internal campaign against terrorist finance needs to have at least three dimensions to be successful. The first element involves the institution in undertaking a study of its global structural exposure to terrorism. The second, requires an examination of the nature and behaviour of the potential terrorist customer. The third, demands a scrutiny of existing ATF systems, in particular the bank's effectiveness in monitoring databases and other established data sources.

The first level I have just described will inform the others. Terrorist operations vary from country to country across the globe. No country and no financial institution should consider itself free from some element of terrorism, if only because terrorists will spot the vulnerability and exploit it. But countries have different roles to play in the terrorist network. The sponsors of a terrorist will be in one country, the conduits for the movement of money in a second country, the quarter masters of terrorist money in a third, and the operatives on the ground in yet a fourth.

Banks must understand to what form of financing local branches might be exposed. The risk of a misunderstanding here is great. Once terrorist finance enters a bank's system, the entire bank is

079 7329 7490
author@kochan.co.uk

affected. Worse still, a detection failure in a small remote part of the bank can have repercussions for the entire institution.

How do different geographies affect financing? The example of Islamic terrorist financing is apt. In Saudi Arabia, terrorist funds are known to have been packaged as charities. Those charitable funds have moved through the Dubai banking system which has correspondent banks in the United States. Global banks who understand the passage and packaging of terrorist money will control their risks. You will likewise be forewarned if your ATM system is immune to access by a quartermaster using an ATM card issued out of Eastern Europe.

Profiles of the financial behaviour of individual terrorists also minimises banking risk. The prudent bank does not merely keep a close watching brief on terrorist activity in each of its markets, but it builds customer profiles to enhance its systems for reporting suspicions. The transient lifestyle of the terrorist suggests that he is unlikely to have a bank account, related standing orders and the like. He is also likely to receive erratic but relatively large payments rather than smaller and regular ones.

But past behaviour need not be a guide to the future. Al Qaida and its offshoots have proved skilful at staying one step ahead of expectations. So the London bombings on 7 July 2005 were carried by locally-grown terrorists who had regular jobs and conventional banking relationships. Their use of the banking system provided no easy clues as to their intentions.

Banks should also know that their customers in geographies where terrorist risk is greatest may be compromised. Companies are used by terrorists to move money across borders and wealthy company directors may make attractive clients until they are shown to be connected with these conduit companies. There is no substitute for scrutiny of the customer and of his financial sources.

The third, and final piece of the bank's armoury against infiltration by terrorist finance is its use of external and internal databases of known and suspected terrorists. These are most effective when banks have developed the communication tools to both access and convey information accurately and quickly.

The war against money laundering goes on, but in today's anxious environment, terrorist finance needs to be treated as a battle all of its own. Neither society at large, nor the financial system and its individual players can lower their guard or contemplate defeat.