

How Can Sound Customer Due Diligence Rules Help Prevent the Misuse of Financial Institutions in the Financing of Terrorism?

Charles Freeland*

When the author first joined the Basel Committee Secretariat in 1978, the idea that bank supervisors had a role to play in the prevention of money-laundering would have been greeted with astonishment. Some ten years later, when Basel first discussed the topic in earnest, there was still a body of opinion that this was a matter for law enforcement and supervisors should stick to the core tasks they were charged with. Nonetheless, the Basel Committee (BCBS) agreed, principally at the insistence of the United States, to issue a statement alerting banks to their ethical responsibilities in the prevention of the criminal use of the banking system. At that time the principal concern was to make it more difficult and costly for drug gangs to launder the proceeds of their crimes. That statement,¹ relatively short by today's standards, laid down four principles that banks should follow:

- Identify their customers
- Refuse suspicious transactions
- Co-operate with law-enforcement agencies
- Train their staff and introduce compliance procedures.

This statement exerted quite wide influence at the national level in the major industrialized countries and was additionally one of the triggers for the formation of the Financial Action Task Force (FATF). With the creation of the FATF, the BCBS took the view that the baton could be passed over to a body with the necessary wider competencies. Although invited to participate in the FATF, the BCBS declined on the grounds that its views could be adequately represented by the individual bank supervisors who became members.

But times change. In 2000, one of the BCBS's specialist task forces, the working

* Deputy Secretary General, Basel Committee on Banking Supervision. Charles Freeland is writing here in his personal capacity. The views expressed in this article do not necessarily represent the views of the Basel Committee or the Bank for International Settlements.

¹ *The prevention of the criminal use of the banking system* (1988).

group on cross-border banking, decided to revert to the issue principally as a result of a series of scandals involving banks' relationships with corrupt dictators such as Abacha and Salinas (now termed 'Politically Exposed Persons' (PEPs)) as well as with the Russian Mafia. The working group on cross-border banking is something of a hybrid animal – it was originally created as a joint working group of the BCBS and the Offshore Group of Banking Supervisors (OGBS) to discuss issues relating to the implementation of the Basel Concordats that govern the responsibilities of bank supervisors in their supervision of international banking groups and their cross-border establishments. As a result, it is co-chaired by the OGBS chairman, Colin Powell, and the author. Its deliberations focus mainly on practical issues such as exchanges of supervisory information, cross-border inspection rights and corporate structures that impede banking supervision. A key product of this work, which will be reconsidered at the end of this article, is the creation of a platform for information exchanges between bank supervisors that is designed to improve supervisory coordination and enable home-country supervisors to exercise consolidated supervision. Such information exchanges have always been impeded by bank secrecy legislation and practices that are regarded by some private banking centres as a competitive necessity in order to prevent information on customer accounts in cross-border entities from being passed to home-country tax authorities. Hence, the supervisory Concordats developed by the Basel Committee have had to balance the need for adequate gateways with the need for adequate protection of information received.

The reason why the cross-border group became concerned about the risks to banks in this area was not only its concern about PEPs (initially called 'potentates'). A survey of know-your-customer (KYC) standards around the world revealed that, despite the FATF's successful initiatives in its member countries, many countries still had no KYC standards at all. The BCBS has the ability to set rules for banks and bank supervisors that, through its influence as a standard-setter and with support from the IMF and World Bank, can have a much broader reach than the FATF. In addition, the FATF's focus is on criminal activity, in its early years especially those activities involved in laundering the proceeds of drug sales, whereas the BCBS is concerned with the risks to banks from a much wider range of unsuitable customers – the PEPs issue is a case in point. Moreover, the BCBS saw a need to respond to the call by the G-7 to strengthen defences against abuse of the financial sector by producing a benchmark for Customer Due Diligence (CDD) standards for banks, as well as a need to act on requests from many emerging market supervisors for guidance in this area.

The BCBS's working group on cross-border banking's expertise in offshore centres and international banking meant that it possessed the qualifications for identifying the risks being posed to international financial institutions. Several of its members are FATF participants. The BCBS therefore agreed with the group's proposals that it address KYC rules for banks. This title was subsequently amended to Customer Due Diligence (CDD) standards to reflect the wider and continuous duties of the banker in protecting a bank's good name.

The working group was producing a draft set of standards at exactly the time that

the Wolfsberg Group's first document was being prepared. In each case, the principal trigger was the Abacha affair. The BCBS's consultative paper² did not address money-laundering or suspicious transaction reporting directly. Rather its focus was on risk management for banks in their customer relationships. The paper focused on four specific risks; reputation risk, legal risk, operational risk and concentration risk (essentially liquidity/funding risk). Plainly, the most sensitive of these is reputation risk. A key distinction was drawn between initial identification of each new customer and ongoing monitoring of existing account activity.

The reaction of the supervisory community to the BCBS's draft was wholly supportive, including enthusiasm from some countries that one would not have put high on the list of those interested in probity. The FATF was also supportive and the Wolfsberg Group provided constructive comments. But some banks and banking associations were less enthusiastic. They raised two principal concerns that we sought to address in the final version of the paper that was issued in October 2001. One was the regulatory burden issue – and that is a very justifiable concern. We tried to respond to that by introducing a risk-based approach – identifying higher-risk customers or customer activities that merit heightened due diligence, and reducing the burden of monitoring the identities and activities of 'ordinary' retail clients. Indeed, the paper makes clear that while customer identification procedures are needed, they should not be so restrictive as to deny banking services to people who are financially or socially disadvantaged – and the same for ongoing monitoring. A second concern related to the clause requiring banks to backdate their customer identification procedures to existing clients. This could be very burdensome for banks serving small retail customers. Although there is still in the final version a requirement to undertake regular reviews of existing records and to monitor the activities of long-standing clients, there is now no obligation for banks to demand customer identity documentation from existing customers.

So what has all this to do with the fight against terrorist financing? Well, first, the bank needs to know who its customers are if it is to be able to respond to requests from law-enforcement or intelligence authorities concerning accounts in the names of known terrorists or terrorist organizations. By definition, however, terrorists may be reluctant (and that reluctance is likely to be greater in the future) to open an account under their true names. They will thus try to hide behind anonymous accounts or 'fronts' making use of trusts, charities, nominees, corporate vehicles, profession intermediaries, and so on. The CDD paper gives clear guidance to banks on how to prevent such fronts from being used by criminals, including of course terrorists. This is a complex area in practice, but the principle itself is clear: the bank must make every effort to establish the beneficial owner(s) of all accounts and persons who conduct regular business with it.

² *Customer Due Diligence for Banks*, January 2001. Although the document was targeted at banks, it expresses the view that similar guidance needs to be developed for all non-bank financial institutions.

The key to preventing terrorists from using banks has to be in the initial customer identification process. Once an account is open, it will rarely be feasible for a bank to identify unusual account activity by a terrorist. The patterns of account activity by the Al-Qaeda perpetrators of the 11 September tragedy are by no means abnormal for a person with an irregular source of income such as a consultant, or a student with occasional parental support. Account profiling is therefore unlikely to identify a terrorist customer. What would of course help would be a tip-off from another source, maybe an intelligence source, or the observation by an alert staff member that the customer's behaviour is suspicious. Another pointer could be that the origin or destination of funds is a terrorist organization. However, one cannot expect banks to monitor every transaction of what would likely be classified as a low-risk customer. What one can do, and what the BCBS's CDD paper does, is to insist that banks maintain account and transaction records for at least five years so that the audit trail can be followed and the origins or source of funds followed if required.

The BCBS paper lays down clear guidelines for customer acceptance and customer identification procedures to be followed by banks in the opening of new customer accounts. It advises individual supervisors to establish strict standards for the documentation that should be required – and prohibits the use of anonymous accounts. It does not specifically list the categories of documents that banks should demand to see. There was an annex attached to the January consultative paper that gave examples of the types of documentation that could be admitted. However, the working group excluded this from the final October version because it felt that more attention was needed to the issue. It is now planning to provide more detailed guidance on customer identification procedures in due course, and to use that opportunity to update the October paper with any further guidance on CDD that has emerged from consultations in other bodies. To take one example, the FATF and the Wolfsberg Group have made certain proposals for the completion of the field for the originator's name in the transmission of wire transfers. The BCBS will probably want to establish a best practice guideline for that issue in due course.

Nobody should be under any illusions that conducting customer due diligence is a simple task – it is one that is full of contradictions. The culture of banking is engrained in the desire to attract customers and profit from providing banking services. As with retailers selling products that are not suitable for all, there needs to be a highly-developed social conscience to prevent banking services falling into the wrong hands. Ex post, it can be relatively easy to judge that a customer should not have been accepted – ex ante, with the pressure on to welcome and even reward new customers, the task is more challenging. There are behavioural differences to respect, for example, in relation to well-heeled customers from other countries. The compliance officer or risk manager in charge of customer due diligence will be in constant conflict with the incentives provided to customer service units dedicated to personal, private or offshore banking. There may also be conflicts of culture with regard to what may or may not be regarded as acceptable behaviour by foreign customers. This may go way beyond the bank – for example the UK is currently grappling with the diplomatic ramifications of the freezing of an account linked to a

Qatari Minister who received 'facilitation payments' for a UK defence deal. The UK's Treasury and Home Offices are apparently in favour of the freeze, while the Defence and Foreign Ministers oppose it. One can only sympathize with a bank that gets involved in such a tug of war.

Fortunately, conflicts of this kind are not likely to arise with regard to terrorist financing. However, there are other aspects that complicate the issue for the financial sector. One of the difficulties in providing guidance to banks in the fight against terrorism is to define what is a terrorist or a terrorist organization. There is often a thin line between terrorists and freedom fighters and a good number of current and recent Heads of State were once regarded as terrorists. The EU definition is more subtle 'persons who finance, plan, facilitate or commit terrorist acts', and it goes on to define a terrorist act. Nonetheless, it is a difficult issue on which the private sector needs guidance from the authorities, and it is not guidance that the supervisors can easily provide. Rather, the financial sector needs to receive information from police and intelligence as to the terrorists and terrorist organizations on the 'black list'. This is even more true in the case of charities and foundations. Many innocent-sounding organizations that may raise money from legitimate sympathizers who believe they are contributing to a humanitarian cause have, in the past, been channelling at least a portion of the funds they have raised to terrorist uses.

Much has been made by the media and by professional writers of the fact that terrorism is different from money-laundering because it is the **use** of the funds that is criminal not their **source**. However, it may be wrong to place too much emphasis on this factor to explain why banks are unable to identify customers engaged in terrorism. There has not, to the author's knowledge, been a significant terrorist organization to date that has funded itself wholly from legitimate means. Al-Qaeda has been heavily involved in the marketing of drugs as well as other lesser crimes such as credit card fraud. Terrorist organizations are certainly not beyond robberies, kidnapping, extortion, and so on as a means of financing their illegal activities. Building and maintaining an effective terrorist organization costs a great deal of money – in the case of Al-Qaeda hundreds of millions. Hence, successfully denying all criminals access to the financial system will hit the terrorists too. What may be more challenging will be the identification of charities and other fund-raising organizations that support terrorism. Many of the contributors to what are usually set up with innocent sounding titles may not be aware that their money is being channelled into a terrorist organization.

One concern that arises in the present hunt for Al-Qaeda money is that the terrorists will turn increasingly to parallel underground banking systems. Attention has been focused on the Hawala system – but it is by no means the only one for money transmission. Western Union type transfer systems, travellers cheques, even credit cards can be an effective means of financing individual terrorists if not whole terrorist cells. Much has also been made of the need to crack down on correspondent banking relations. Effectively, a respondent bank is relying on its correspondent to have conducted due diligence of each of its customers, because there is no way the respondent bank can monitor the probity of all transactions originating from sources



<http://www.springer.com/978-1-4020-1152-8>

Financing Terrorism

Pieth, M. (Ed.)

2002, IV, 220 p., Hardcover

ISBN: 978-1-4020-1152-8