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).

European Journal of Law Reform, Vol. 4, No. 2

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 paper[2] 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

that it does not know. The principles enacted in the USA PATRIOT Act prohibiting a bank from maintaining a correspondent relationship with a bank located in a 'non-cooperative' jurisdiction appears to be a sound – if not necessarily watertight – precaution. But there is a risk that countries without developed banking systems, whose banks need their correspondent relationships to link with the principal world markets or whose (innocent) citizens are active users of Hawala to transmit funds abroad, may be harshly penalized through no fault of their own. Indeed, there are countries, such as Somalia, that have no banking infrastructure and whose banking system is based entirely on Hawala-type relationships. The BCBS paper does not go so far as to ban correspondent banking relationships (except with so-called 'shell banks'). But it says that banks must decide whether they can rely on a correspondent to conduct adequate due diligence of its customers in the same manner as an introducer[3] – and hence it must apply the criteria that are laid down for eligible introducers in determining whether to enter into or to sustain a correspondent relationship.

It is a legitimate question to ask what the BCBS itself has been doing since 11 September to support the anti-terrorism efforts of the US government and others. First, it accelerated the issue of its CDD paper and, in doing so, took pains to ensure that it represents a response to the newly-identified threat (though, in truth, few changes were made to the document). Second, the BCBS's Secretariat has been assisting the authorities in the transmission of the US 'Control List' of suspected terrorists to banks in the major countries. It has not been creating the list directly, but has acted as a conduit in taking the initial US list, adding additional names identified by non-US authorities and circulating a consolidated list to the authorities that make up its members. Those authorities have then passed on the list at their discretion to the financial institutions within their jurisdictions. The lists were also made available via the European Central Bank to countries in the European Union that are not members of the Basel Committee. Not all supervisors have been enthusiastic about this process – some have expressed doubt about the accuracy and comprehensiveness of the list, and have voiced fears that circulating lists will create complacency among banks about customers that do not appear on the list.

An important issue in this context and one that is of considerable interest to the working group on cross-border banking is the extent to which the monitoring of customer due diligence needs to be applied on a global basis. The four risks identified in the CDD paper apply to a bank wherever it is operating – certainly to its overseas branches and very probably to subsidiaries under its effective control. There is a section in the paper that addresses the need for banks to be able to implement the CDD standards imposed by their home-country regulator on a global basis, and for home-country supervisors to be able to ensure that the standards are being adequately applied through on-site examination on equivalent verification procedures.

---

[3] An introducer is an entity that channels suitable customers to a bank. In some countries, this is a regular and frequent source of new customers. The BCBS paper sets out strict criteria for the acceptability of introducers.

Since the Control Lists began to circulate, this debate has become more pertinent because it has raised questions about a bank's ability to respond on behalf not only of its head office and domestic banking network, but also of its offices abroad. Some banks seek to ensure that they maintain a centralized customer database – if only to save on IT costs – and hence are in a position to 'search' for identified customer names across their global customer base. Some do not make that attempt – and, even if they do, there will be individual units which for various reasons may not wish their own customer base to be accessible from the head office. Others may use a numbered account system to disguise the names of, say, their private banking clients in offshore centres or their high net-worth clients in a private banking centre such as Switzerland. It is clear, however, if a CDD principle is to be effective, that a bank should be in a position to respond to an official request as to whether it has the account of a named customer in any of the locations in which it operates. This means that its offices abroad must be capable of responding to enquiries from head office about named account holders. In the specific case of the Control List, many banks have circulated the List to their offices abroad and asked for notification of any matches. This means that the Lists have reached some outlying countries whose supervisors/central banks have not received them.

Another issue relates to the 'search' capability. One of the lessons learnt since the Control Lists have been circulating is that, while all banks would normally have their account-holders in an electronically searchable form, relatively few banks have the beneficial owners so recorded. It seems that many banks have the supporting documentation to identify the recorded beneficial owner separately from their principal customer base. Hence a search of the Control List can be extremely time-consuming if banks are to search, as they should do, the beneficial owners of accounts that they hold.

There is also a question about the means by which banks should react with respect to matches with the Control Lists. This involves the legal area, because in most cases some form of confidentiality legislation will apply and any exchange of information will be subject to treaties or Memoranda of Understanding (MOUs). Where there are suspicious transaction reporting rules and Financial Intelligence Units (FIUs) to which suspicions can be reported, the gateway would seem to be clear-cut. However, some FIUs may not have the powers to communicate directly with FIUs in other countries, such as FINCEN in the United States. It may, in such cases, be more efficient if the banks respond to their own supervisor, who can communicate suspicions to the Federal Reserve Bank of New York. This channel may also be required in the case of countries which have not yet established FIUs (though these are becoming fewer). However, as a general rule, the supervisory information channel is not well suited to suspicious transaction reporting, since it is designed for the communication of problems concerning the bank's own activities and is often subject to a series of criteria designed to protect the confidentiality of any information transmitted concerning individual customers and accounts. As often in the case of information-sharing, the most sensitive issue, as mentioned earlier, is the matter of tax confidentiality and the need to protect information about customer

accounts from being passed to home-country authorities. But that protection can, at the same time, inhibit the bank supervisor from passing information to other official bodies, such as the FIU.

The author's view on the prospects for success in the fight against terrorist financing is that co-operation is needed on an unprecedented scale, not only between the private and public sectors, but within the public sector too. It is no secret that different official entities within the United States had information which, if pooled, would have alerted them to the 11 September terrorist attacks. Such information was not shared with others who could have added to it, partly for reasons of professional jealousy between the different agencies. Now, in the United States and elsewhere there is unprecedented collaboration at the official level with at least two major US inter-agency task forces. This effort is leading to intelligence successes, which have thankfully, at the time of writing at least, contributed to the absence of further terrorist events, though there have been some close calls. But, at the financial level, it seems that success has been more limited. While some quite substantial sums have apparently been frozen, many of the audit trails have petered out in impenetrable areas in the Middle East or in financial centres, often at a high political level. It is not surprising that the financial trail is not a simple one – Osama bin Laden reputedly went to Afghanistan originally to advise the Taliban on the best means of marketing and laundering the proceeds of their opium crops. He is known to operate a sophisticated financial machine and to have associates well versed in underground banking methods.

In the future, it is going to be even more difficult to identify or to track the financing of terrorism, for the perpetrators have now been warned. Only so much can be done by the private sector – it needs to develop closer links with and receive tip-offs from the public sector on an ongoing basis. It has been said that customer privacy will not be the same again after 11 September, and this trend is being reinforced by initiatives by the OECD and others to increase fiscal transparency and force offshore financial centres to adopt stricter prudential and disclosure standards. Banks must certainly remain alert to terrorism – just as they must remain alert to all forms of criminal activity by their customers – but they can only supplement the efforts being made by the intelligence and police authorities, and not substitute for them. If there is to be real coordination, the public sector needs to share information more readily with the private sector than it has traditionally been willing to so. It has in the past been very much a one-way information flow and banks making Suspicious Transaction Reports (STRs) to FIUs have often wondered whether they have ever been investigated. The sharing of Control Lists with the financial institutions is an encouraging sign that the public sector is willing to be more open, and appreciates that it needs assistance from the banks and other financial institutions if it is to defend properly its people against these terrible threats.

It is necessary, though, to close on a sombre note. Banks and bank supervisors have rarely faced a responsibility as grave as they do now. Failing to conduct due diligence in present circumstances could have deadly consequences, putting thousands or conceivably hundreds of thousands of lives at risk. There is no place to hide on this issue.