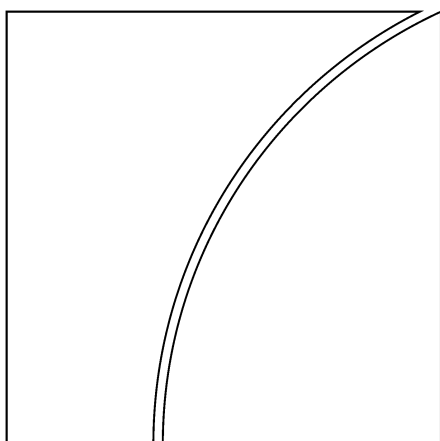


# Basel Committee on Banking Supervision



## **Sharing of financial records between jurisdictions in connection with the fight against terrorist financing**

April 2002



BANK FOR INTERNATIONAL SETTLEMENTS



# **Sharing of financial records between jurisdictions in connection with the fight against terrorist financing**

## **Summary of a meeting of representatives of Supervisors and Legal Experts of G10 Central Banks and Supervisory Authorities on 14 December 2001, Basel, Switzerland**

### **(a) Introduction**

1. On 14 December 2001, bank supervisors and legal experts of G10 central banks and supervisory authorities met at the BIS to discuss how to prevent the abuse of the financial system when it is used to finance terrorism, and, specifically, issues relating to the sharing of financial records between jurisdictions to assist in the fight against terrorism. The meeting provided an opportunity for participants to review international developments directed at terrorism, and to consider specific assistance that central banks and banking supervisors might provide. The participants discussed measures that had been taken in their jurisdictions to combat terrorist financing and surveyed mechanisms for the sharing of financial records between national jurisdictions. In many of the countries represented at the meeting, legislation has been or is in the course of being amended to provide for sanctions to deter terrorist activities, including measures to deter terrorist financing.

2. All participants fully embraced the goal of combating terrorism and shared the view of the Chairman of the Basel Committee that measures to impede terrorist financing are critical. The participants agreed with the Chairman that the Basel Committee should add its voice condemning terrorism to that of the United Nations Security Council and the Financial Action Task Force of the OECD.

3. Participants agreed that the size and geographical scope of the international financial system make it imperative to significantly improve coordination and collaboration between all the parties involved if measures to identify and prevent terrorist financing are to succeed. Central banks and bank supervisors are typically not in the front line of these efforts. Nevertheless, because terrorism is a threat to financial stability, the participants agreed that central banks and banking supervisors should lend their expertise and resources to those that are more directly involved, including treasuries, judicial authorities and law enforcement authorities such as financial intelligence units. The collaboration needs to operate both at a domestic level between all parties concerned and also, to the extent possible, at an international level. This means that gateways need to exist for information to be transmitted within and across national borders.

4. Participants reported that even at the domestic level there had been clear evidence of intelligence failures because different strands of information had not been centrally collected and analysed. Many countries have created inter-agency task forces in order to remedy this problem and have become more effective in halting terrorist financing (including improving their responses to the lists of suspected terrorist names being circulated).

5. The focus of the 14 December 2001 meeting was on banking activities and on the possibilities of preventing the global financial system from being misused to support terrorist activities. The participants noted that this cannot be achieved unless financial services providers have effective "know your customer" (KYC) and customer due diligence (CDD) procedures and that some of the methods that might be used by terrorists to move money, such as the postal giro network and private wire transfer systems, may not be within the

jurisdiction of central banks or banking supervisors. This underscores the need to introduce or improve KYC and CDD standards for all categories of institutions that provide financial services.

6. Participants emphasized the need to share information about terrorist financing - including the identities of those who might use the global financial system to support terrorism and the patterns of financing activities associated with such support - between different national jurisdictions. Discussion focused on two mechanisms for information flows (a) from a governmental body in one country to a governmental body in another country, using an official gateway or some less formal channel and (b) within a single financial group (i.e. between a financial entity operating in one country and its head office or parent institution in a different country).

## **(b) Official gateways for cross-border information sharing**

7. The participants identified three official gateways for sharing information between national jurisdictions:

- (i) The classical gateway, usually embodied in a treaty for mutual legal assistance ("MLAT"), provides a legal basis for transmitting evidence that can be used for prosecution and judicial procedures. This is of course not confined to financial crime. This gateway, which typically involves formalised procedures, is not customarily used for supervisory or regulatory matters.
- (ii) The second official gateway involves a communication between financial intelligence units (FIUs) or other bodies set up to fight financial crime. The FIUs, with the task of receiving and analysing suspicious transaction reports on an ongoing basis and maintaining close links with police and customs authorities, are presently mostly engaged in tracking terrorist funds and following up reports of potential terrorist accounts. FIUs share information between themselves informally in the context of investigations, usually on the basis of memoranda of understanding (MOU). The Egmont Group of FIUs has established a model for such MOU. Unlike the MLAT, this gateway is not ordinarily used for obtaining evidence, but it is used for obtaining intelligence that might lead to evidence.
- (iii) The third official gateway is the supervisory channel. In relation to banking activities, the information is normally of a general character, designed to monitor the soundness of the banking group. Increasingly in the recent past, however, enquiries have related more to specific asset or liability accounts because of concerns about reputation and legal risk. A recent example concerns accounts for politically exposed persons. The ability to share information is often defined in the legal framework under which the supervisor operates, but it may also be supported by a MOU. Unlike the MLAT, the MOU is not a treaty and usually is not binding on the governments. Instead, it reflects the mutual understanding of the signing supervisory authorities' policies. The MOU may be especially valuable where other types of entities, such as securities or trading firms, are within the jurisdiction of a specific authority, because that authority could share information on customer transactions throughout a larger segment of the financial market. Information communicated through the supervisory gateway usually is communicated for supervisory purposes only, and may therefore not ordinarily be used as evidence, nor be shared widely among governmental entities.

8. While each of these gateways is used to communicate financial information across a national border, the information received through each respective gateway serves a different purpose. Of course, these purposes may also complement one another with respect to an overall objective like fighting terrorism. If a prosecutor needs information to prosecute a criminal case of terrorism, the prosecutor will ordinarily use a MLAT. If a FIU in a host country learns information suggesting that a branch or subsidiary of a banking group has an account for a known terrorist organisation, the FIU may pass that intelligence information to the FIU in the home country for the group. If a bank supervisor in the jurisdiction where such a branch or subsidiary has the account learns about it, then that host supervisor may well pass the information along to the home supervisor for the Group. The overall fight against terrorism needs coordination among prosecutors, financial intelligence units, and banking supervisors in the affected jurisdictions. While the spirit and level of cooperation demonstrated in the aftermath of September 11<sup>th</sup> far exceeded past experience, many of the participants in the meeting felt that further work needed to be done to coordinate between interested governmental bodies, within a jurisdiction and, particularly, across national boundaries.

9. The participants felt that this need was demonstrated recently in the case of the circulation of “control lists” of individuals suspected to be involved in terrorism. In particular, both the circulation of the lists within financial groups and the reporting mechanisms for feedback did not operate uniformly. Participants were of the view that the FIU channel is in most cases the most effective gateway in such circumstances. The efficiency of this gateway would, however, be impaired if the involved authorities did not collaborate closely. A breakdown in communication could occur between FIUs, or between an FIU and a banking supervisor within the same country. The participants believed that further work delineating sharing arrangements is desirable, particularly with respect to the fight against terrorism.

### **(c) Information flow from a financial entity to its head office/parent**

10. The first line of defence against terrorist financing is for those involved in terrorism to be denied all support, which includes a denial of access to the financial system. Strenuous efforts have been made over recent years to prohibit the use of the financial system by criminal elements and these efforts are now being reviewed to ensure they reflect the terrorist threat. The identification of the customer is key and this is the object of the Customer Due Diligence paper issued in October 2001 by the Basel Committee on Bank Supervision. That paper emphasises the significant risks, notably reputational risk, for banks that do not have sufficient KYC procedures. The procedures should apply both to the initial identification process and the ongoing monitoring of higher risk accounts. Responsibility for this task lies with the banks’ compliance officers under the overall direction of top management and subject to review in the supervisory process.

11. The monitoring of reputational risk needs to be conducted for an institution on a worldwide basis. For that reason, the CDD paper stresses that the risk management process must embrace all foreign branches and subsidiaries, even if they are subject to lower KYC standards in some jurisdictions. Banks require a centralised risk management system that is overseen by the group’s chief compliance officer. The centralised risk management system can utilise one of two approaches in obtaining its information:

- (i) The first is the creation of a centralised database or register at the parent bank. However, many foreign branches and subsidiaries are not permitted to transmit the customer files outside of their jurisdiction. In some cases, this may be forbidden by the law of the jurisdiction in which the branch or subsidiary is located. In other cases, particularly where offshore centres offering private banking services are

concerned, the local branch or subsidiary may maintain that its business with nationals of its home country will be handicapped if financial records containing customer names find their way back to the authorities at the headquarters of the parent bank. The reason for this is usually tax-related, but there are other reasons why customers may wish to keep their financial records confidential.

- (ii) In the second approach, a centralised database would not be maintained at the parent bank, but information would be kept at branches and subsidiaries and made available to the parent bank on request, or at the initiative of the branches and subsidiaries when the reputation or liability of the group could be threatened by the relationship. This approach would allow financial groups to determine their own organisational structure, yet branches and subsidiaries would be expected to maintain rigorous risk management systems for due diligence purposes, and the adequacy of these systems would be reviewed by home supervisory authorities. In the case of a relationship with a person believed to be involved in terrorism, the participants felt the relationship should be disclosed to the centralised risk manager. The participants felt that a banking group should require such disclosure as a matter of policy.

12. Participants recognise that the Basel Committee already has taken a number of steps to persuade banks to adopt centralised risk management systems. However, they felt that further attention should be paid to this practice in the light of recent developments, with specific reference to the ability of the group compliance officer to access names of all the bank's customers in its overseas branches and subsidiaries, especially if any of those names were suspected to be associated with terrorism.

#### **(d) Conclusions**

13. Participants suggested that the Basel Committee add its voice condemning terrorism to that of the United Nations Security Council and the FATF. The Basel Committee should also acknowledge that terrorism threatens financial stability, and the threat needs to be met with collective actions to identify and halt terrorist financing.

14. The participants believed that adequate means for group wide centralised risk assessment is essential, as the provision of financial services to terrorists would expose the group to material reputational and legal risk. Furthermore, best practices of consolidated home country supervision require that a home country supervisor must know if any foreign branch or subsidiary of a group for which it acted as consolidated supervisor were providing financial services to terrorists. This kind of significant supervisory information needs to reach the consolidated supervisor, in the view of the participants, and must flow across the national border.

15. Participants suggested the Basel Committee consider further work to be done on best practices for controlling reputational and legal risk arising from a relationship with a terrorist organisation by any part of a banking group, such as by remitting the matter to the Cross-border Banking Working Group<sup>1</sup> to provide additional guidance regarding, for example,

---

<sup>1</sup> In October 2001, the Basel Committee released the Customer Due Diligence for Banks paper that was drafted by the Working Group on Cross-border Banking. This paper explored the risks associated with customer account relationships and established essential elements of know your customer standards, which highlighted

the appropriate roles and responsibilities of individual offices and subsidiaries of a banking organisation and those of its centralised risk management function in detecting and communicating any relationship with a possible terrorist organisation, and to consider the responsibilities and practices to be followed by supervisory authorities to ensure that bank processes in this regard work effectively.

16. Participants suggested further that the Basel Committee consider asking the legal experts of the G10 central banks and supervisory authorities and/or other legal experts (including, if appropriate, FIU experts) to explore current impediments to (i) sharing information on terrorist financing and develop guidelines for passing information across borders to other interested parties, particularly in the case of sharing information between host and home supervisors, and (ii) treating financial groups as single entities for the purpose of sharing information within the group. Other areas for additional work could include developing best practices for the sharing of information by an FIU with a banking supervisor within the same country where the banking supervisor acts as the consolidated supervisor for a banking group where a component of that group has a financial relationship with an identified terrorist, as well as best practices for collecting and sharing information where no FIU exists within a particular country.

---

the importance of an effective centralised risk management program to effectively control reputational, compliance and legal risks.