AL 2002-4

OCC ADVISORY LETTER

Subject: Financial Action Task Force
Guidance for Financial Institutions in Detecting Terrorist Financing

TO: Chief Executive Officers and Compliance Officers of National Banks and Federal Branches, Department and Division Heads, and Examining Personnel

This advisory letter transmits the Financial Action Task Force's (FATF) "Guidance for Financial Institutions in Detecting Terrorist Financing," dated April 24, 2002. The goal of the guidance is to help ensure that financial institutions do not unwittingly hide or move terrorist funds. Financial institutions are in a position to detect suspicious transactions that, if reported, may later prove to be related to terrorist financing. FATF indicates that identifying terrorist financing activity is unlikely, absent dealings with known terrorists or terrorist organizations. As a result, financial institutions should focus on ascertaining whether transactions are unusual, suspicious, or otherwise indicative of criminal or terrorist activity. The guidance describes the general characteristics of terrorist financing, provides case studies, and provides a list of the characteristics of financial transactions that have been linked to terrorist activity. The guidance is available at [http://www1.oecd.org/fatf]. Also available on that Web site is the February 1, 2002 "Report on Money Laundering Typologies for 2001-2002," a report on the methods and trends of money laundering and terrorist financing.

If you have any questions, please contact your supervisory office or the Compliance Division at (202) 874-4428.

_____

David G. Hammaker
Deputy Comptroller for Compliance

Attachment

Financial Action Task Force on Money Laundering

Groupe d'action financière sur le blanchiment de capitaux

Guidance for Financial Institutions in Detecting Terrorist Financing

24 April 2002

FATF Secretariat
2, rue André-Pascal
75775 Paris Cedex 16
France

Contact@fatf-gafi.org

Table of Contents

Guidance for Financial Institutions in Detecting Terrorist Financing Activities

Introduction

1. At its extraordinary Plenary meeting on 29-30 October 2001, the Financial Action Task Force on Money Laundering (FATF) agreed to develop special guidance for financial institutions to help them detect the techniques and mechanisms used in the financing of terrorism. The FATF subsequently brought together experts from its member countries to gather information on and study the issue of terrorist financing as part of its annual exercise on money laundering methods and trends. One goal of this exercise was to begin establishing such guidance for financial institutions that could be issued along with the annual FATF Report on Money Laundering Methods and Trends. Material derived from the exercise, along with contributions from the Egmont Group and other international bodies, was used in developing the present document. The information contained in it represents a first attempt to provide necessary guidance for financial institutions in this area.

2. The goal in providing this guidance is to ensure that financial institutions do not unwittingly hide or move terrorist funds. Financial institutions will thus be better able to protect themselves from being used as a conduit for such activity. To help build awareness of how terrorists, their associates or those who support terrorism may use the financial system, this document describes the general characteristics of terrorist financing. The accompanying case studies illustrate the manner in which competent law enforcement authorities or financial intelligence units (FIUs) are able to establish a terrorist financing link based on information reported by financial institutions. Annex 1 contains a series of characteristics of financial transactions that have been linked to terrorist activity in the past. When one or several of these potentially suspicious or unusual factors is present in regard to a specific financial transaction – especially when the individual or entity may appear on one of the lists of suspected terrorists, terrorist organisations or associated individuals and entities (see Annex 2: Sources of Information) – then a financial institution would have cause to increase its scrutiny of the transaction and any associated individuals or entities. In certain instances, this scrutiny could result in reporting the transaction to authorities under applicable suspicious or unusual transaction reporting systems.

Terrorist financing and risks to financial institutions

3. A financial institution that carries out a transaction, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organisations, or that the transaction is linked to, or likely to be used in, terrorist activity, may be committing a criminal offence under the laws of many jurisdictions. Such an offence may exist regardless of whether the assets involved in the transaction were the proceeds of criminal activity or were derived from lawful activity but intended for use in support of terrorism.

4. Regardless of whether the funds in a transaction are related to terrorists for the purposes of national criminal legislation, business relationships with such individuals or other closely associated persons or entities could, under certain circumstances, expose a financial institution to significant reputational, operational, and legal risk. This risk is even more serious if the person or entity involved is later shown to have benefited from the lack of effective monitoring or wilful blindness of a particular institution and thus was to carry out terrorist acts.

Reinforcing existing requirements

5. Consideration of the factors contained in this guidance is intended to clarify, complement and / or reinforce already existing due diligence requirements, along with current policies and procedures imposed by national anti-money laundering programmes. It should be stressed, however, that this guidance does not constitute an additional rule or regulation. Rather it represents advice from the operational experts of FATF members as to factors associated with financial transactions that should trigger further questions on the part of the financial institution. The FATF encourages all financial institutions to consider these factors along with policies, practices and procedures already in place for ensuring compliance with appropriate laws and regulations and for minimising reputational risks. It should be noted as well that, while the characteristics indicated in this document may apply specifically to terrorist financing, most of them may also apply in identifying suspicious transactions generally. Financial institutions in many jurisdictions may already be aware of these characteristics through existing guidance notes or other sources.

6. In providing this guidance, the FATF intends it to be consistent with applicable criminal and civil laws, as well as relevant regulations, to which financial institutions may be subject in their particular jurisdiction. It should be noted however that this guidance does not replace or supersede any obligations under the current national laws or regulations. In particular, implementing the measures proposed by this guidance should not be construed as necessarily protecting a financial institution from any action that a jurisdiction might choose to take against it. Furthermore, this guidance does not supersede or modify requirements imposed by national or regional authorities, which call for the freezing of assets of individuals and entities suspected of being terrorists or terrorist related, as part of implementing relevant United Nations Security Council Resolutions (see Annex 2: Sources of Information).

Determining when increased scrutiny is necessary

7. Financial institutions are encouraged to develop practices and procedures that will help to detect and deter those transactions that may involve funds used in terrorist financing. The increased scrutiny that may be warranted for some transactions should be seen as a further application of the institution's due diligence and anti-money laundering policies and procedures and should lead, when appropriate, to reporting of such financial activity as suspicious or unusual under applicable transaction reporting regimes for a particular jurisdiction. To ensure that the practical steps are taken to increase scrutiny of certain transactions when necessary, it may be useful for a financial institution to review its practices in this area as part of its general internal and external audit processes.

Example 1: Front for individual with suspected terrorist links revealed by suspicious transaction report

The financial intelligence unit (FIU) in Country D received a suspicious transaction report from a domestic financial institution regarding an account held by an individual residing in a neighbouring country. The individual managed European-based companies and had filed two loan applications on their behalf with the reporting institution. These loan applications amounted to several million US dollars and were ostensibly intended for the purchase of luxury hotels in Country D. The bank did not grant any of the loans.

The analysis by the FIU revealed that the funds for the purchase of the hotels were to be channelled through the accounts of the companies represented by the individual. One of the companies making the purchase of these hotels would then have been taken over by an individual from another country. This second person represented a group of companies whose activities focused on hotel and leisure sectors, and he appeared to be the ultimate buyer of the real estate. On the basis of the analysis within the FIU, it appeared that the subject of the suspicious transaction report was acting as a front for the second person. The latter as well as his family are suspected of being linked to terrorism.

8. The manner in which a financial institution may choose to apply this Guidance will vary depending on the extent of the risk determined to exist by each institution as a general matter, given its normal business operations. It will also vary according to the individual factors of each case as it

occurs. Financial institutions should exercise reasonable judgement in modifying and implementing policies and procedures in this area. This Guidance should not be interpreted as discouraging or prohibiting financial institutions from doing business with any legitimate customer. Indeed, it has been designed solely as a means of assisting financial institutions in determining whether a transaction merits additional scrutiny so that the institution is thus better able to identify, report (when appropriate) and ultimately avoid transactions involving the funds supporting or associated with the financing of terrorism.

Example 2: Individual's account activity and inclusion on UN list show possible link to terrorist activity

An individual resided in a neighbouring country but had a demand deposit account and a savings account in Country N. The bank that maintained the accounts noticed the gradual withdrawal of funds from the accounts from the end of April 2001 onwards and decided to monitor the accounts more closely. The suspicions of the bank were subsequently reinforced when a name very similar to the account holder's appeared in the consolidated list of persons and/of entities issued by the United Nations Security Council Committee on Afghanistan (UN Security Council Resolution 1333/2000). The bank immediately made a report to the financial intelligence unit (FIU).

The FIU analysed the financial movements relating to the individual's accounts using records requested from the bank. It appeared that both of the accounts had been opened by the individual in 1990 and had been fed mostly by cash deposits. In March 2000 the individual made a sizeable transfer from his savings account to his checking account. These funds were used to pay for a single premium life insurance policy and to purchase certificates of deposit.

From the middle of April 2001 the individual made several large transfers from his savings account to his demand deposit account. These funds were transferred abroad to persons and companies located in neighbouring countries and in other regions.

In May and June 2001, the individual sold the certificates of deposit he had purchased, and he then transferred the profits to the accounts of companies based in Asia and to that of a company established in his country of origin. The individual also cashed in his life insurance policy before the maturity date and transferred its value to an account at a bank in his country of origin. The last transaction was carried out on 30 August 2001, that is, shortly before the September 11th attacks in the United States.

Finally, the anti-money laundering unit in the individual's county of origin communicated information related to suspicious operations carried out by him and by the companies that received the transfers. Many of these names also appeared in the files of the FIU. This case is currently under investigation.

9. It should be acknowledged as well that financial institutions will probably be unable to detect terrorist financing as such. Indeed, the only time that financial institutions might clearly identify terrorist financing as distinct from other criminal misuse of the financial system is when a known terrorist or terrorist organisation has opened an account. Financial institutions are, however, in a position to detect suspicious transactions that, if reported, may later prove to be related to terrorist financing. It is the competent enforcement authority or the financial intelligence unit (FIU) then that is in a position to determine whether the transaction relates to a particular type of criminal or terrorist activity and decide on a course of action. For this reason, financial institutions do not necessarily need to determine the legality of the source or destination of the funds. Instead, they should ascertain whether transactions are unusual, suspicious or otherwise indicative of criminal or terrorist activity.

Characteristics of terrorist financing

10. The primary objective of terrorism according to one definition is "to intimidate a population, or to compel a Government of an international organisation to do or abstain from doing any act".[1] In contrast, financial gain is generally the objective of other types of criminal activities. While the difference in ultimate goals between each of these activities may be true to some extent, terrorist organisations still require financial support in order to achieve their aims. A successful terrorist group, like any criminal organisation, is therefore necessarily one that is able to build and maintain an effective financial infrastructure. For this it must develop sources of funding, a means of laundering

[1] Article 2, *International Convention for the Suppression of the Financing of Terrorism*, 9 December 1999.

those funds and then finally a way to ensure that the funds can be used to obtain material and other logistical items needed to commit terrorist acts.

Sources of terrorist funds

11. Experts generally believe that terrorist financing comes from two primary sources. The first source is the financial support provided by States or organisations with large enough infrastructures to collect and then make funds available to the terrorist organisation. This so-called State-sponsored terrorism has declined in recent years, according to some experts, and is increasingly replaced by other types of backing. An individual with sufficient financial means may also provide substantial funding to terrorist groups. Osama bin Laden, for example, is thought to have contributed significant amounts of his personal fortune to the establishment and support of the Al-Qaeda terrorist network.

Example 3: Diamond trading company possibly linked to terrorist funding operation

The financial intelligence unit (FIU) in Country C received several suspicious transaction reports from different banks concerning two persons and a diamond trading company. The individuals and the company in question were account holders at the various banks. In the space of a few months, a large number of fund transfers to and from overseas were made from the accounts of the two individuals. Moreover, soon after the account was opened, one of the individuals received several USD cheques for large amounts.

According to information obtained by the FIU, one of the accounts held by the company appeared to have received large US dollar deposit originating from companies active in the diamond industry. One of the directors of the company, a citizen of Country C but residing in Africa, maintained an account at another bank in Country C. Several transfers had been carried out to and from overseas using this account. The transfers from foreign countries were mainly in US dollars. They were converted into the local currency and were then transferred to foreign countries and to accounts in the Country C belonging to one of the two subjects of the suspicious transaction report.

Police information obtained by the FIU revealed that an investigation had already been initiated relating to these individuals and the trafficking of diamonds originating from Africa. The large funds transfers by the diamond trading company were mainly sent to the same person residing in another region. Police sources revealed that this person and the individual that had cashed the cheques were suspected of buying diamonds from the rebel army of an African country and then smuggling them into Country C on behalf of a terrorist organisation. Further research by the FIU also revealed links between the subjects of the suspicious transaction report and individuals and companies already tied to the laundering of funds for organised crime. This case is currently under investigation.

12. The second major source of funds for terrorist organisations is income derived directly from various "revenue-generating" activities. As with criminal organisations, a terrorist group's income may be derived from crime or other unlawful activities. A terrorist group in a particular region may support itself through kidnapping and extortion. In this scenario, ransoms paid to retrieve hostages, along with a special "revolutionary tax" (in reality a euphemism for protection money) demanded of businesses, provide needed financial resources but also play a secondary role as one other means of intimidating the target population. Besides kidnapping and extortion, terrorist groups may engage in large-scale smuggling, various types of fraud (for example, through credit cards or charities), thefts and robbery, and narcotics trafficking.

13. Funding for terrorist groups, unlike for criminal organisations however, may also include income derived from legitimate sources or from a combination of lawful and unlawful sources. Indeed, this funding from legal sources is a key difference between terrorist groups and traditional criminal organisations. How much of a role that legal money plays in the support of terrorism varies according to the terrorist group and whether the source of funds is in the same geographic location as the terrorist acts the group commits.

14. Community solicitation and fundraising appeals are one very effective means of raising funds to support terrorism. Often such fundraising is carried out in the name of organisations having the status of a charitable or relief organisation, and it may be targeted at a particular community. Some members of the community are led to believe that they are giving for a good cause. In many cases, the charities to which donations are given are in fact legitimate in that they do engage in some of the

work they purport to carry out. Most of the members of the organisation, however, have no knowledge that a portion of the funds raised by the charity is being diverted to terrorist causes. For example, the supporters of a terrorist movement from one country may carry out ostensibly legal activities in another country to obtain financial resources. The movement's supporters raise these funds by infiltrating and taking control of institutions within the immigrant community of the second country. Some of the specific fundraising methods might include: collection of membership dues and / or subscriptions; sale of publications; speaking tours, cultural and social events; door-to-door solicitation within the community; appeals to wealthy members of the community; and donations of a portion of their personal earnings.

Laundering of terrorist related funds

15. From a technical perspective, the methods used by terrorists and their associates to generate funds from illegal sources differ little from those used by traditional criminal organisations. Although it would seem logical that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for the terrorist group to obscure or disguise links between it and its legitimate funding sources. It follows then that terrorist groups must similarly find ways to launder these funds in order to be able to use them without drawing the attention of authorities. In examining terrorist related financial activity, FATF experts have concluded that terrorists and their support organisations generally use the same methods as criminal groups to launder funds. Some of the particular methods detected with respect to various terrorist groups include: cash smuggling (both by couriers or bulk cash shipments), structured deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments (travellers' cheques, bank cheques, money orders), use of credit or debit cards, and wire transfers. There have also been indications that some forms of underground banking (particularly the *hawala* system[2]) have had a role in moving terrorist related funds.

Example 4: Cash deposits to accounts of non-profit organisation allegedly finance terrorist group

The financial intelligence unit (FIU) in Country L received a suspicious transaction report from a bank regarding an account held by an offshore investment company. The bank's suspicions arose after the company's manager made several large cash deposits in different foreign currencies. According to the customer, these funds were intended to finance companies in the media sector. The FIU requested information from several financial institutions. Through these enquiries, it learned that the managers of the offshore investment company were residing in Country L and a bordering country. They had opened accounts at various banks in Country L under the names of media companies and a non-profit organisation involved in the promotion of cultural activities.

According to the analysis by the FIU, the managers of the offshore investment company and several other clients had made cash deposits to the accounts. These funds were ostensibly intended for the financing of media based projects. The analysis further revealed that the account held by the non-profit organisation was receiving almost daily deposits in small amounts by third parties. The manager of this organisation stated that the money deposited in this account was coming from its members for the funding of cultural activities.

Police information obtained by the FIU revealed that the managers of offshore investment company were known to have been involved in money laundering and that an investigation was already underway into their activities. The managers appeared to be members of a terrorist group, which was financed by extortion and narcotics trafficking. Funds were collected through the non-profit organisation from the different suspects involved in this case. This case is currently under investigation.

16. The difference between legally and illegally obtained proceeds raises an important legal problem as far as applying anti-money laundering measures to terrorist financing. Money laundering has generally been defined as a process whereby funds obtained through or generated by criminal activity are moved or concealed in order to obscure the link between the crime and generated funds. The terrorist's ultimate aim on the other hand is not to generate profit from his fundraising

[2] For more information on the *hawala* system of alternate remittance / underground banking, see the 1999-2000 *FATF Report on Money Laundering Typologies*, 3 February 2001 (pp. 4-8).

mechanisms but to obtain resources to support his operations. In a number of countries, terrorist financing thus may not yet be included as a predicate offence for money laundering, and it may be impossible therefore to apply preventive and repressive measures specifically targeting this terrorist activity.

17. When terrorists or terrorist organisations obtain their financial support from legal sources (donations, sales of publications, etc.), there are certain factors that make detecting and tracing these funds more difficult. For example, charities or non-profit organisations and other legal entities have been cited as playing an important role in the financing of some terrorist groups. The apparent legal source of this funding may mean that there are few, if any, indicators that would make an individual financial transaction or series of transactions stand out as linked to terrorist activities.

Example 5: High account turnover indicates fraud allegedly used to finance terrorist organisation

An investigation in Country B arose as a consequence of a suspicious transaction report. A financial institution reported that an individual who allegedly earned a salary of just over USD 17,000 per annum had a turnover in his account of nearly USD 356,000. Investigators subsequently learned that this individual did not exist and that the account had been fraudulently obtained. Further investigation revealed that the account was linked to a foreign charity and was used to facilitate funds collection for a terrorist organisation through a fraud scheme. In Country B, the government provides matching funds to charities in an amount equivalent to 42 percent of donations received. Donations to this charity were being paid into to the account under investigation, and the government matching funds were being claimed by the charity. The original donations were then returned to the donors so that effectively no donation had been given to the charity. The charity retained the matching funds. This fraud resulted in over USD 1.14 million being fraudulently obtained. This case is currently under investigation.

18. Other important aspects of terrorist financing that make its detection more difficult are the size and nature of the transactions involved. Several FATF experts have mentioned that the funding needed to mount a terrorist attack does not always call for large sums of money, and the associated transactions are usually not complex. For example, an examination of the financial connections among the September 11th hijackers showed that most of the individual transactions were small sums, that is, below the usual cash transaction reporting thresholds, and in most cases the operations consisted of only wire transfers. The individuals were ostensibly foreign students who appeared to be receiving money from their parents or in the form of grants for their studies, thus the transactions would not have been identified as needing additional scrutiny by the financial institutions involved.

Example 6: Lack of clear business relationship appears to point terrorist connection

The manager of a chocolate factory (CHOCCo) introduced the manager of his bank accounts to two individuals, both company managers, who were interested in opening commercial bank accounts. The two companies were established within a few days of each other, however in different countries. The first company (TEXTCo) was involved in the textile trade while the second one was a real estate (REALCo) non-trading company. The companies had different managers and their activities were not connected.

The bank manager opened the accounts for the two companies, which thereafter remained dormant. After several years, the manager of the chocolate factory announced the arrival of a credit transfer issued by the REALCo to the account of the TEXTCo. This transfer was ostensibly an advance on an order of tablecloths. No invoice was shown. However, once the account of TEXTCo received the funds, its manager asked for them to be made available in cash at a bank branch near the border. There, accompanied by the manager of CHOCCo, the TEXTCo manager withdrew the cash.

The bank reported this information to the financial intelligence unit (FIU). The FIU's research showed that the two men crossed the border with the money after making the cash withdrawal. The border region is one in which terrorist activity occurs, and further information from the intelligence services indicated links between the managers of TEXTCo and REALCo and terrorist organisations active in that region.

Annex 1: Characteristics of financial transactions that may be a cause for increased scrutiny

As a normal part of carrying out their work, financial institutions should be aware of elements of individual transactions that could indicate funds involved in terrorist financing. The following list of potentially suspicious or unusual activities is meant to show types of transactions that could be a cause for additional scrutiny. This list is not exhaustive, nor does it take the place of any legal obligations related to the reporting suspicious or unusual transactions that may be imposed by individual national authorities.

This list of characteristics should be taken into account by financial institutions along with other available information (including any lists of suspected terrorists, terrorist groups, and associated individuals and entities issued by the United Nations[3] or appropriate national authorities – see Annex 2 : Sources of Information), the nature of the transaction itself, and the parties involved in the transaction, as well as any other guidance that may be provided by national anti-money laundering authorities. The existence of one or more of the factors described in this list may warrant some form of increased scrutiny of the transaction. However, the existence of one of these factors by itself does not necessarily mean that a transaction is suspicious or unusual. For examples of terrorist financing cases developed from the enhanced scrutiny/reporting by financial institutions, please also see the various case examples provided in the body of the main document.

Financial institutions should pay particular attention to:

A. Accounts

(1) Accounts that receive relevant periodical deposits and are dormant at other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out.

(2) A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

(3) When opening an account, the customer refuses to provide information required by the financial institution, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.

(4) An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

(5) An account opened by a legal entity or an organisation that has the same address as other legal entities or organisations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

(6) An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits are made in comparison with the income of the founders of the entity.

[3] This guidance does not supersede or modify requirements imposed by national or regional authorities, which call for the freezing of assets of individuals and entities suspected of being terrorists or terrorist related, as part of implementing relevant United Nations Security Council Resolutions.

(7) The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

(8) An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation.

(9) An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organisation and that shows movements of funds above the expected level of income.

B. Deposits and withdrawals

(1) Deposits for a business entity in combinations of monetary instruments that are atypical of the activity normally associated with such a business (for example, deposits that include a mix of business, payroll and social security cheques).

(2) Large cash withdrawals made from a business account not normally associated with cash transactions.

(3) Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in cheques or other payment instruments.

(4) Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

(5) Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

(6) The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.

(7) The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

(8) The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.

(9) The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

C. Wire transfers

(1) Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

(2) Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected.

(3) Use of multiple personal and business accounts or the accounts of non-profit organisations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

(4) Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.

D. Characteristics of the customer or his/her business activity

(1) Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.

(2) Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.).

(3) Stated occupation of the transactor is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

(4) Regarding non-profit or charitable organisations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

(5) A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

(6) Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

E. Transactions linked to locations of concern

(1) Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).

(2) Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).

(3) A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern.

(4) The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern.

(5) A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.

(6) The opening of accounts of financial institutions from locations of specific concern.

(7) Sending or receiving funds by international transfers from and/or to locations of specific concern.

Annex 2: Sources of Information

Several sources of information exist that may help financial institutions in determining whether a potentially suspicious or unusual transaction could indicate funds involved in the financing of terrorism and thus be subject to reporting obligations under national anti-money laundering or anti-terrorism laws and regulations.

A. United Nations lists

Committee on S/RES/1267 (1999) website: http://www.un.org/Docs/sc/committees/AfghanTemplate.htm

B. Other lists

(1) Financial Action Task Force

FATF Identification of Non-Cooperative Countries and Territories

FATF website: http://www.fatf-gafi.org/NCCT_en.htm

(2) United States

Executive Order 13224, 23 September 2001 (with updates)

US Department of the Treasury website: http://www.ustreas.gov/terrorism.html

(3) Council of the European Union

Council Regulation (EC) Nº 467/2001 of 6 March 2001 [on freezing Taliban funds]

Council Decision (EC) Nº 927/2001 of 27 December 2001 [list of terrorist and terrorist organisations whose assets should be frozen in accordance with Council Regulation (EC) Nº 2580/2001]

Council Common Position of 27 December 2001 on application of specific measures to combat terrorism [list of persons, groups and entities involved in terrorist acts]

EUR-lex website: http://europa.eu.int/eur-lex/en/index.html

C. Standards

(1) Financial Action Task Force

FATF Special Recommendations on Terrorist Financing

FATF website: http://www.fatf-gafi.org/TerFinance_en.htm

FATF Forty Recommendations on Money Laundering

FATF website: http://www.fatf-gafi.org/40Recs_en.htm

(2) UN Conventions and Resolutions

International Convention on the Suppression of Terrorist Financing

Website: http://untreaty.un.org/English/Terrorism.asp

UN Security Council Resolutions on Terrorism

Website: http://www.un.org/terrorism/sc.htm

(3) Council of the European Union

Council Regulation (EC) Nº 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism

EUR-lex website: http://europa.eu.int/eur-lex/en/index.html