EGMONT/FATF COLLECTION OF SANITISED CASES
Related to Terrorist Financing

Following the events of September 11th the Egmont Group FIUs were invited by the Training Working Group to contribute to a new initiative to collect cases relating to the use of the financial system by criminals for the purposes of terrorism. Several cases were subsequently received by the Egmont Permanent Administrative Support and then sanitised by several members of the Training Working Group. We have been liaising closely with the Financial Action Task Force and some of the cases have been given to them for their use.

Cases 1-16 have been received from Egmont FIUs while Cases 17-20 emanate from the FATF Typologies. The cases with titles will appear in the FATF "Guidelines for financial institutions".

It is hoped that this collection of cases will enable your FIU and financial institutions to identify instances where the financial circuits are being manipulated to launder terrorist funds.
This document should be disseminated within your FIU and to the financial institutions in your country.

CASE 1

A terrorist organisation collects money in Country A to finance its activities in another country. The collecting period is between November and January each year. The organisation collects the funds by visiting businesses within its own community. It is widely known that during this period the business owners are "required" to donate funds to the cause. The use or threat of violence is a means of reinforcing their demands. The majority of businesses have a large cash volume. All the money is handed over to the collectors in cash. There is no record kept by either the giver or the receiver. Intimidation prevents anyone in the community from assisting police, and the lack of documentation precludes any form of audit trail. It is estimated that the organisation collects between USD 650,000 and USD 870,000 per year. The money is moved out of the country by the use of human couriers.

CASE 2

Within a particular community, a terrorist organisation requires a payment in order for a company to erect a new building. This payment is a known cost of doing business, and the construction company factors the payment into the cost of the project. If the company does not wish to pay the terrorist organisation, then the project cannot be completed.

CASE 3

A terrorist organisation is involved in smuggling cigarettes, alcohol and petrol for the benefit of the organisation and the individuals associated with it. The contraband is purchased legally in the Europe, Africa, or the Far East and then transported into the Country B. The cost of the contraband is significantly lower in these areas than it is in the Country B due to different tax and excise duties. This difference in tax duties provides the profit margin. The contraband is then smuggled into the Country B via numerous methods. The distribution of the contraband is a key element of the successful importation. The terrorist organisation uses trusted persons and limits the number of persons involved in the operation. There is also evidence that there is a substantial co-operation between the terrorist organisation and traditional organised crime.

The methods that are currently being used to launder these proceeds involve the transport of the funds by couriers to another jurisdiction. The money enters the banking system by the use of front companies or short-term shell companies that disappear after three months. The group has also created specialised bureaux de change that exist solely to facilitate the laundering of smuggled proceeds.

A newer and more difficult method of integrating the proceeds into the banking system has recently been detected. The smuggler gives the funds to legitimate businesses that are not associated with the smuggling operation. The funds then enter the banking system as part of company's normal receipts. Monies are then passed through various financial institutions and jurisdiction, including locations identified by the FATF as non-co-operative countries or territories (NCCTs).

CASE 4

An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also procures a medical insurance policy that will cover the loan payments if he were to acquire a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organisation running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of USD 2 million from similar fraud schemes carried out by terrorist groups.

CASE 5 : Credit card fraud supports terrorist network

One operation discovered that a single individual fraudulently obtained at least twenty-one Visa and MasterCards using two different versions of his name. Seven of those cards came from the same banking group. Debts attributed to those cards totalled just over USD 85,000. Also involved in this scheme were other manipulations of credit cards, including the skimming of funds from innocent cardholders. This method entails copying the details from the magnetic strip of legitimate cards onto duplicate cards, which are used to make purchases or cash withdrawals until the real cardholder discovers the fraud. The production of fraudulent credit cards has been assisted by the availability of programmes through the Internet.

CASE 6 : 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.

CASE 7 : 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.

CASE 8 : 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.

CASE 9 : 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 was 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.

CASE 10 : 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.

CASE 11 : 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.

CASE 12

A suspicious transaction report identified activity involving multiple payments by cheque from a business account of approximately USD 420,000 to a securities brokerage in Country H. The account was also used to transfer a total of USD 2.1 million into and out of commercial and personal accounts in another country. In addition, a cash transaction report was made concerning the withdrawal of USD 11,000 from the account by an individual with a foreign passport. Two individuals with signature authority on the account were also involved in two other businesses, both of which were the subject of cash transaction reports for withdrawals totalling USD 43,000.

CASE 13 : Purchase of cheques and wire transfers by alleged terrorists

Suspicious transaction reports outlined unusual activity involving three grocery markets, two of which shared a common location. The activity was conducted by individuals of the same origin using a single address, which corresponded to one of the business locations. Two individuals employed by a grocery store and a third whose occupation was unknown each deposited funds just under applicable reporting thresholds and immediately drew cheques payable to a fourth individual. The cheques cleared through two different banks in a foreign country. All three bank customers supplied the same address. In addition, two individuals associated with a second grocery store located at the common address above each purchased bank cheques just under the applicable reporting threshold at the same bank branch, at the same time but from different tellers. One of the cheques was purchased on behalf of the second grocery store, the other on behalf of third party. The cheques were payable to two different individuals, one of whom shared the same last name as one of the purchasers. In related activity, a third business used the common address discussed above when opening a business account which immediately received a USD 20,000 wire transfer from a wholesale grocery located in another region of the country. Filings of cash transaction reports indicated that a total of about USD 72,000 was withdrawn in cash from other accounts associated with this business.

CASE 14 : Suspect money order purchases at money remittance company

In Country D, both a money remittance company and a financial institution filed suspicious transaction reports outlining the movement of approximately USD 7 million in money orders through the account of a foreign business. The money remittance company reported various individuals purchasing money orders at the maximum face value of USD 500 - 1,000 and in sequential order. Purchases were made at multiple locations, primarily in the north east part of Country D, with several instances also reported in the south-east. The money orders were made payable to various individuals, negotiated through banks in an NCCT jurisdiction and later cleared through three Country D financial institutions. The foreign business endorsed the money orders. In some instances, the funds were then credited to accounts at other Country D banks or foreign financial institutions (one in an NCCT country, the second location not identified). Suspicious transaction reports filed by the institution indicated similar purchases of money orders in the north east of the country and negotiated at the foreign business. Various beneficiaries were identified, and the amounts ranged from USD 5,000 to USD 11,000. The foreign business identified by the money remittance company was also identified as a second beneficiary. The money orders cleared through a foreign bank's correspondent account at the Country D financial institution.

CASE 15

Suspicious transaction reports identified an import/export business, acting as an unlicensed money transmitter/remittance company, generating USD 1.8 million in outgoing wire transfer activity during a five-month period. Wire transfers were sent to beneficiaries (individuals and businesses) in North America, South Asia, Asia and the Middle East. Cash, cheques, and money orders were also deposited to the suspect account totalling approximately USD 1 million. Approximately 60 percent of the wire transfers were sent to individuals and businesses in foreign countries, which were then responsible for disseminating the funds to the ultimate beneficiaries. A significant portion of the funds was ultimately disseminated to nationals of Afghanistan residing in various countries. Individuals conducting these transactions described the business as involved in refugee relief or money transfer. The individual with sole signatory authority on the suspect account had made significant deposits (totalling USD 17.4 million) and withdrawals (totalling USD 56,900) over an extended period of time through what appeared to be 15 personal accounts at 5 different banks.

CASE 16

A pattern of cash deposits below the reporting threshold caused a bank to file a suspicious transaction report. Deposits were made to the account of a bureau de change on a daily basis totalling over USD 341,000 during an approximately two and one-half month period. During the same period, the business sent ten wire transfers totalling USD 2.7 million to a bank in another country. When questioned, the business owner reportedly indicated he was in the business of buying and selling foreign currencies in various foreign locations, and his business never generated in excess of USD 10,000 per day. Records for a three-year period reflected cash deposits totalling over USD 137,000 and withdrawals totalling nearly USD 30,000. The business owner and other individuals conducting transactions through the accounts were nationals of countries associated with terrorist activity. Another bank made a suspicious transaction report on the same individual indicating an USD 80,000 cash deposit, which was deemed unusual for his profession. He also cashed two negotiable instruments at the same financial institution for USD 68,000 and USD 16,387.

CASE 17 : Terrorists acquire funds through criminal activity

In late 1999, a network of religious extremists was broken up in an FATF member jurisdiction (Country A) as its members were preparing violent acts on its soil for the end-of-year festivities. The inquiry launched by law enforcement authorities revealed the existence of links between this network and a number of individuals living in another FATF country (Country B) and known to the specialised services for their religious extremism.

Investigations were undertaken in Country B as part of the judicial inquiry initiated on the basis of the information provided by the authorities of Country A. The investigation established that this group of ten individuals, most of whom had fought in a European regional conflict, was implicated in a number of armed attacks against several shops in early 1996 and in an attack on an armoured truck in a shopping centre car park of the same year, during which automatic weapons, rocket launchers and grenades had been used.

This group's violent acts in fact formed just one element in an entire logistical set-up working for a much larger Islamic terrorist organisation whose ramifications extended beyond Country A to three more FATF countries. The ordinary criminal offences were designed to obtain funds to serve "the cause", whilst another group dealt with trafficking false administrative documents, collecting information and clandestine movement of personnel. The members of the network were recently convicted of, among others, armed robbery and criminal association.

CASE 18 : Terrorists collect funds from lawful sources

In 1996, a number of individuals known to belong to the religious extremist groups established in the south-east of an FATF country (Country C) convinced wealthy foreign nationals, living for unspecified reasons in Country C, to finance the construction of a place of worship. These wealthy individuals were suspected of assisting in the concealment of part of the activities of a terrorist group. It was later established that "S", a businessman in the building sector, had bought the building intended to house the place of worship and had renovated it using funds from one of his companies. He then transferred the ownership of this building, for a large profit, to Group Y belonging to the wealthy foreigners mentioned above.

This place of worship intended for the local community in fact also served as a place to lodge clandestine "travellers" from extremist circles and collect funds. For example, soon after the work was completed, it was noticed that the place of worship was receiving large donations (millions of dollars) from other wealthy foreign businessmen. Moreover, a Group Y worker was said to have convinced his employers that a "foundation" would be more suitable for collecting and using large funds without attracting the attention of local authorities. A foundation was thus reportedly established for this purpose.

It is also believed that part of "S's" activities in heading a multipurpose international financial network (for which investments allegedly stood at USD 53 million for Country C in 1999 alone) was to provide support to a terrorist network. "S" had made a number of trips to Afghanistan and the United States. Amongst his assets were several companies registered in Country C and elsewhere. One of these companies, located in the capital of Country C, was allegedly a platform for collecting funds. "S" also purchased several buildings in the south of Country C with the potential collusion of a notary and a financial institution.

When the authorities of Country C blocked a property transaction on the basis of the foreign investment regulations, the financial institution's director stepped in to support his client's transaction

and the notary presented a purchase document for the building thus ensuring that the relevant authorisation was delivered. The funds held by the bank were then transferred to another account in a bank in an NCCT jurisdiction[1] to conceal their origin when they were used in Country C.

Even though a formal link has not as yet been established between the more or less legal activities of the parties in Country C and abroad and the financing of terrorist activities carried out under the authority a specific terrorist network, the investigators suspect that at least part of the proceeds from these activities have been used for this purpose.

CASE 19 : Suspicious money transfers and relief organisation

Suspicious transaction reports (STRs) were filed by financial institutions on transactions totalling USD 9 million involving structured cash deposits and deposits of business, payroll and social benefit cheques. Deposited funds were subsequently transferred within one or two days to a company located abroad. The deposit and wire transfer activity involved 37 individuals, four businesses and 44 accounts. Two of the businesses appear to be ethnic based money remittance companies; one is described as a relief organisation at the same location as one of the money remittance businesses; the fourth business, was the beneficiary of the money transfer activity. The majority of the wire transfers were sent to two accounts in the foreign location.

CASE 20 : Simple transactions found to be suspect

In October 2001, the financial intelligence unit (FIU) of Country E forwarded to the judicial authorities some ten files with relation to money laundering derived from terrorism. In general, the files dealt with instances in which simple operations had been performed (retail foreign exchange operations, international transfer of funds) revealing links with other countries. Some of the customers had police records, particularly for trafficking in narcotics and weapons, and were linked with foreign terrorist groups.

One of the files submitted by the FIU in relation with terrorism is of particular interest in this respect: the customer was holder of a current account and of a savings account in the reporting financial institution. Moreover, he purchased securities and a life insurance with single premium in the same institution. He performed several transfers from his current account to beneficiaries in different countries. The suspicions of the bank arose from the fact that a name similar to the customer's appeared on the consolidated list of persons and/or entities included in the UN Security Council Resolution on Afghanistan (S/RES/1333(2000)) and Regulation 1354/2001 of the European Commission. The suspicion of the bank was strengthened by the fact that the customer had been progressively withdrawing funds he held at this bank since the end of April 2001. He successively cleared out his savings account, sold the securities he had purchased before the expiry date, repurchased his life insurance premium and finally transferred his remaining funds to the European country where he resided. The last operation he performed occurred at the end of August 2001, that is, about two weeks before the attacks in the United States. The bank has had no more contact with this customer since then.

[1] Countries identified through the FATF initiative to identify non-cooperative countries or territories (NCCTs) in the fight against money laundering. For more information, see the FATF website: http://www.fatf-gafi.org.