

Terrorist Financing

The article below gives a summary of the existing status on the expectations of regulators and enforcement from banks and discusses what is possible for CFT purposes. This is a field that is developing and updates will be needed. Rohan Bedi a leading expert in the AML/CFT field explains.

Terrorist Financing is a topic that shot into the limelight after the tragic events of September 11 2001. The US passed the USA PATRIOT Act to ensure that both combating the financing of terrorism (CFT) and anti-money laundering (AML) was given adequate focus by US financial institutions. The act also had extra-territorial impact and non-US banks having correspondent banking accounts or doing business with US banks had to upgrade their AML/CFT processes.

Initially the focus of enforcement efforts for CFT purposes was on charities, unregistered money services businesses (MSBs) (so called underground banking or 'Hawalas'), and registered MSBs that were unregulated for CFT. The FATF (working with the US) brought in 9 special recommendations for CFT which were recommended standards applicable to all FATF members who were expected to upgrade their laws, regulations and enforcement efforts including through Financial Intelligence Units (FIUs) and cross-border sharing of information for CFT purposes. The FATF black-list (the NCCT list) mechanism was used to coerce countries to bring about change.

US efforts have brought about a huge change to global CFT regulations and have ushered in a new era of information sharing. US reports suggest that Saudi Arabian charities, which were prime sponsors of terrorist groups around the world, are now under much tighter controls albeit there is still a lot to do in the Middle East and South Asia. Terrorist groups like Al Qaeda are on the run albeit they are also innovating – in making/moving monies and in hiring of their key operatives - the new terrorist is a western educated middle class technology savvy

person and the source for getting information on a do-it-yourself bomb is the internet.

Money Laundering

While the monies required for a terrorist act may be small (e.g. USD 5,000) the process of advocacy, training and sustaining sleeper operations (over years) is an expensive one that requires huge amounts of money.

Since it is becoming more difficult for terrorists to raise monies from charities, terrorists are evolving and have moved into the money laundering space.

- US reports highlight that organised terrorist outfits are now working with drug traffickers and criminals to make and launder the proceeds of crime like fraud, prostitution, intellectual property theft (e.g. CD piracy), kidnap & extortion, smuggling (e.g. by Colombian guerrilla groups) - this is now routine for them.
- The UK Serious Fraud Office (SFO) highlights that terrorists are using low value but high volume frauds (e.g. credit cards, cheque fraud, VAT, internet and insurance fraud) to fund their operations.
- Paramilitary groups in Northern Ireland are using legitimate businesses such as hotels, pubs and taxi operators to launder money and fund political activities.
- Even beyond Ireland, terrorists are buying out/controlling front-end businesses especially cash-intensive businesses including in some cases money services businesses to move monies.
- There are schemes where terrorists launder their money through front property businesses before moving the money on to a registered charity for onward payments to a terrorist outfit.

International Centre for Political Violence and Terrorism Research

Strategic Counter Terrorism: Terrorist Financing

Response Series

- Bulk cash smuggling and placement through cash-intensive businesses is one typology. Terrorists are now also moving monies through the new online payment systems and using stored-value cards. They are also using trade linked schemes to launder monies. The monies from the drug trade in Afghanistan are reported to be laundered through trade (“narco-barter”) and not through banks.

Nonetheless, the older systems have not given way. Terrorists also continue to move monies through MSBs/ Hawalas, and through international ATM transactions. Correspondent banking continues to be vulnerable. Charities also continue to be used in countries where controls are not so stringent and also in many cases in Europe and North America.

Offshore shell companies (including bearer share companies) also continue to be used in terrorist financing schemes. The FATF underscores the use of false identities, “straw men” or front companies. Dubai was described by some as “the centre of terrorist finance in the Middle East” - it probably still is.

Classification is Difficult

The US Federal Bureau of Investigations (FBI) states “Terrorist financing methods range from the highly sophisticated to the most basic.” *Annexure 1* has a list of Suspicious Activity.

It is difficult to determine by the activity alone whether it is related to terrorism or to organised crime. Hence, the activity must be examined in context with other factors in order to determine a terrorist financing connection.

- Simple transactions can be found to be suspect and money laundering derived from terrorism will typically involve instances in which simple operations had been performed (*retail foreign exchange operations, international transfer of funds*) revealing links with other countries including FATF blacklisted/ formerly blacklisted countries. The funds may have moved through a state sponsor of terrorism or a country where there is a terrorism problem.
- Other links, for example, with a Politically Exposed Person (PEP); a charity; the gold,

diamond or jewellery trade, could highlight risks.

- Some customers/ counter-parties may have police records, particularly for trafficking in narcotics and weapons and may be linked with foreign terrorist groups.
- Searchspace (now “Fortent”) says terrorists have “few if any standing orders or direct debits paying utility bills or other on-going and regular costs” (this is a ‘red flag’ but other sleeper operations can have a more normal account profile).
- Accounts (especially student) that only receive periodic deposits withdrawn via ATM over two months and are dormant at other periods could indicate that they are becoming active to prepare for an attack.

CFT Tools & Controls

Given the costs of compliance, banks have questioned the value of CFT controls and linked SAR filing. However, September 2006 data by the FBI highlights that in a review of all SARs that were coded as suspected terrorist financing, the agency was able to match 20 percent of those SARs with known subjects of open FBI terrorism investigations.

There is now a much better understanding of CFT issues based on many new terrorist financing cases and the working knowledge generated by banks and software vendors collectively. Based on this, banks must introduce new CFT controls in addition to their normal AML controls and name matching (using name recognition technology (*fuzzy matching*)) against sanctions and high-risk lists provided by third-party database vendors.

- For implementing AML/CFT monitoring software, detection rules designed to capture the suspicious activity list given in *Annexure 1*, are possible where the value thresholds set are not low (i.e., AML type rules) *or* where the rules are not based on value thresholds (e.g. multiple receipts/ payments from/ to the same person/entity).
- However, it is not possible to create a specific detection rule for some items listed in *Annexure 1* on Suspicious Activity i.e., these are fine

International Centre for Political Violence and Terrorism Research

Strategic Counter Terrorism: Terrorist Financing

Response Series

points and become important in the course of investigating other alerts.

- Based on the experience of banks, setting up of detection rules directly at the account/ customer level with *low value thresholds* for CFT purposes, is difficult. The alerts generated could potentially be unmanageable as many CFT detection scenarios may not be unique enough. Peer group analysis technology is needed.

PEER GROUP ANALYSIS TECHNOLOGY

The following are essential:

1. A robust KYC system
2. Capability (link-up) to use the KYC data by the technology
3. Peer groups identified i.e., data quality
4. Implementation of peer group analysis technology
5. Value thresholds for monitoring against, set for the respective peer groups

In the context of the above, creating detection rules for peer group monitoring for CFT purposes, is possible.

This promises to be a long road for many banks.

- Data mining technologies such as link analysis (and visualisation tools) can be used to throw up links amongst people, accounts and transactions. This has been used by law enforcement for years.
- New tools are now available to help banks prevent identity theft including a passport check on machine readable passports.
- Additional databases can be considered for monitoring against/ verifying specific cases, where practical (e.g. police records, sanitised information on SAR filing in other locations of the bank/ other banks (the USA PATRIOT act allows this), IPR Theft perpetrators, mortgage fraud early warning databases, information from enforcement shared through secure channels).
- Since setting up of CFT detection scenario rules is not possible for all items in *Annexure 1*, front office staff must be vigilant for CFT linked transaction red flags that become apparent in the normal course of their work.
- Controls out of the transaction monitoring process, for example, account openings by

groups of individuals, are also important to watch for.

- Training front office staff on a customer's body language is an important CFT control (see www.lichaamstaal.com/english/).

The above is not exhaustive and other specialist AML technologies (e.g. sequence matching behaviour detection) can also help in detection of larger operations involving money laundering. Cheque fraud and credit card fraud are separate areas requiring proper processes and technology.

Any bank that is used for terrorist financing will suffer tremendous reputational damage and potentially also a real business impact in terms of share price, expensive fines and possible loss of license to operate in the particular market where the scam happened.

The Future

The trend is for terrorist groups to be replaced by smaller decentralized groups. Hence, the premise that terrorists need a financial support network may become outdated.

Moreover, some terrorist operations do not rely on outside sources of money and may now be self-funding, either through legitimate employment/ businesses or low-level criminal activity, for example, the 7/7 London terrorists.

Some experts argue that for anti-terrorism, a more direct approach may be more effective than the CFT approach. If terrorists for example, just carry USD 10,000 in cash and don't route it through the banking system, the CFT approach would not be effective.

Annexure 1 – Suspicious Activity

The writer (www.rohanbedi.com) is a leading AML/CFT expert.

This is his personal comment.

International Centre for Political Violence and Terrorism Research

Strategic Counter Terrorism: Terrorist Financing

Response Series

Annexure 1 - Suspicious Activity

FFIEC List

The US FFIEC BSA/AML Examination manual 2006¹ states the following examples of potentially suspicious activity that may indicate terrorist financing:

Activity Inconsistent with the Customer's Business

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from high-risk countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories (NCCT)).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding non-profit or charitable organizations, financial transactions occur 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 organization and the other parties in the transaction.
- A safe deposit box 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.

Funds Transfers

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves high-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.

Other Transactions That Appear Unusual or Suspicious

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to high-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in high-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from high-risk locations when there appear to be no logical business reasons for dealing with those locations.
- Banks from high-risk locations open accounts.
- Funds are sent or received via international transfers from or to high-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

¹ http://www.occ.treas.gov/bsa/pages_manual/manual_online.htm

International Centre for Political Violence and Terrorism Research

Strategic Counter Terrorism: Terrorist Financing

Response Series

Red Flags - NGO Terrorist Financing

An October 2006 article by World-Check² states “The red flags most often associated with NGO terrorist financing are:

- Foreign banks accounts, where the NGO's stated aims and activities have no connection with that area.
- The NGO has a high volume of wire transfers.
- Transfers are made to regions where there is a high risk of terrorist activity.
- The NGO has multiple accounts without a satisfactory explanation for their use.
- The NGO receives third party cheques for deposit into its account.
- Multiple cheques are received from the same individual.
- Donations are diverted from their intended purpose or application.
- Cash deposits are followed by immediate ATM withdrawals.
- Donation cheques are cashed rather than deposited in the NGO account.
- Transfers are received from intermediary organisations.
- There are multiple transfers to the same recipient.
- The NGO has a hoard of cash available that is not deposited into its account.
- There is evidence of layering of funds.
- The account history is inconsistent with typical NGO activity.

Many NGO officers who are involved in terrorist financing have had prior experience with other NGO's that were also fronts. All NGO staff, as well as officers and directors, should be vetted when the organisation is periodically checked.”

² <http://www.world-check.com/articles/2006/10/30/are-your-ngo-clients-involved-terrorist-financing/>