

**International Centre for Political Violence and Terrorism  
Research**

**ABS Fellow - Counter Financing of Terrorism Project**

**COUNTER FINANCING OF TERRORISM BEST  
PRACTICES ADOPTED BY BANKS IN DEVELOPED  
COUNTRIES**

## EXECUTIVE SUMMARY

One major and difficult challenge of terrorist financing is the ability for terrorists to exploit financial institutions. 9/11 demonstrated how 19 attackers were able to open bank accounts, deposit funds, transmit and withdraw funds in legitimate banks.

The financial community should self-regulate before the authorities and mass media take drastic action. On 27<sup>th</sup> September 2006, the Australian Financial Review alleged that an Australian bank was involved in terrorism funding at its Jakarta branch.<sup>1</sup> On 20<sup>th</sup> September 2006, Israeli troops raided a Jordanian-owned bank and 14 money-changers on terrorism funding charges.<sup>2</sup>

We need to protect the integrity of the financial industry and financial institutions need to play their part in fighting terrorism. Although an enormous amount of money, expertise and new technologies have been introduced to bolster the due diligence systems, it is still insufficient.

Presently, there is limited information on how terrorism is funded and there is no one outstanding method of funding. Terrorists are opportunistic and adapt their modus operandi to the region they are based in. Hence financial response has to vary accordingly.

Fighting terrorist financing requires a multidisciplinary approach and the financial sector is a key actor. Countering terrorist financing relies extensively on intelligence sources and requires close cooperation between intelligence, law

---

<sup>1</sup> <http://www.smh.com.au/news/National/CommBank-denies-terrorism-funding-claims/2006/09/27/1159036569487.html>

<sup>2</sup>

[http://www.khaleejtimes.com/DisplayArticleNew.asp?xfile=data/middleeast/2006/September/middleeast\\_September449.xml&section=middleeast&col=](http://www.khaleejtimes.com/DisplayArticleNew.asp?xfile=data/middleeast/2006/September/middleeast_September449.xml&section=middleeast&col=)

enforcement agencies and stakeholders, such as financial institutions and market supervisors.

Based on an assessment of the requirements and challenges surrounding financial institutions, a package approach in the form of best practices will assist financial institutions in strengthening their internal AML/CTF systems, in line with worldwide AML/CTF recommendations and guidelines.

The International Centre for Political Violence and Terrorism Research at the Nanyang Technological University has decided to release this recommendation paper suggesting 8 best practices for banks.

The implementation of the best practices will constrict the financial operational environment of terrorist groups, cells and supporters.

## BACKGROUND

Terrorist financing can be defined as using proceeds from the sale of property to finance terrorist activity. Terrorist financing uses similar techniques as money laundering, therefore there are similar countermeasures. Terrorist organizations are also known to finance terrorist activities from criminal proceeds.

Terrorist financing is more difficult to detect than money laundering as it is directed at future activity. It is possible that the only offense that has been committed when terrorism financing takes place is conspiracy to commit a terrorist act.

Compared to fraudulent commercial transactions or volumes of money laundered by crime syndicates which may total several hundred billion dollars annually, terrorism fund transfers are smaller in comparison as terrorist operations are lower in cost. The September 11 attacks on the World Trade Center and the Pentagon is believed to cost US\$300,000. The Madrid train bombings on March 11 2004 cost an estimated US\$10,000 which was funded from drug sales of hashish and ecstasy.

Traditional methods used to fight money laundering will not work against terrorist financing. Banks should ensure they are free of money laundering and terrorist financing. Within the regulated financial system there is evidence of significant costs increases related to AML/CFT regimes. Supervisors have taken decisive action against financial institutions, mostly banks, for violation of AML/CFT requirements (*Please see Diagram 1 below*). In addition to direct costs associated with fines and litigation, adverse publicity associated with supervisory enforcement has damaged their reputation, customer base, and market capitalization. For example, the shares of a major international bank fell nearly 3

percent the day after a prominent Wall Street analyst downgraded the bank, citing ethics problems.

### **Supervisory Response to AML/CFT Violations**

The evidence shows supervisors from advanced countries have taken the lead in enforcing AML/CFT compliance in the financial sector. The most prominent cases involve large/multinational banks from the United States and Europe (e.g., Riggs Bank, Citigroup, Abbey National, ABN Amro, Union Bank of California).

*Riggs Bank* was fined US\$25 million in 2004 by the U.S. Office of the **Comptroller** of the Currency. The bank was scrutinized for connection with money laundering and terrorist financing, involving accounts of foreign governments and politically exposed persons.

*Citigroup* was ordered in 2004 by the Japan Financial Services Agency to close its private unit in Japan. Regulators cited a long list of infractions, including improper client screening and failing to prevent suspected money laundering.

*Abbey National* was fined £2.3 million in 2003 by the UK Financial Services Authority for AML/CFT compliance failure. Regulators found that the bank failed to ensure suspicious activity reports were promptly considered and reported to the National Criminal Intelligence Service.

*ABN Amro* and *Union Bank of California* were recently required to terminate banking relationships with about 550 banks in Russia, Eastern Europe, and the Caribbean mainly because of AML/CFT risk concerns in their banking businesses.

### **Diagram 1: Supervisory Response to AML/CFT Violations**

**Source: Johnston, R. B. & Nedelescu, O. M., “The Impact of Terrorism on Financial Markets”, IMF Working Paper, March 2005, PG 19.<sup>3</sup>**

---

<sup>3</sup> <http://www.imf.org/external/pubs/ft/wp/2005/wp0560.pdf>

## **BEST PRACTICE 1: MANAGEMENT COMMITMENT**

Terrorists and their supporters are opportunists who exploit any business unit in a financial institution. A strong organization-wide corporate culture against terrorism financing is essential. Top management and members of the compliance team will not deal directly with students sending frequent or large money transfers, nor will they get to meet shady businessmen with inadequate personal identification and large amounts of cash from unknown sources. Bank tellers and sales staff are the ones who are at the front lines and interact with potential launderers and terrorists.

In 2002, the United States' Department of Defense attempted to improve its financial management and conducted a survey on the best practices of world-class financial management organizations—Boeing; Chase Manhattan Bank; General Electric; Pfizer; Hewlett-Packard; Owens Corning; and the states of Massachusetts, Texas, and Virginia. It was clear strong executive leadership is essential to ensuring effective and sustained changes, and building a team of people that delivers results.<sup>4</sup>

To successfully implement a counter terrorism finance program, the financial institution needs commitment from the top management because the financial institution's corporate culture must focus on terrorism finance. If real change is to occur in organizations, it must happen at the cultural level.

Through top management's actions and the AML/CTF compliance team, the senior managers, middle managers and front line operational staff will change accordingly. A strong corporate culture against terrorism financing can be reinforced in the following ways:

---

<sup>4</sup> <http://www.gao.gov/new.items/d02784t.pdf>

- Establish a senior management position and dedicate a team to oversee the financial institution's CTF policies, regulatory compliance, practices and procedures.
- A clear message of "no tolerance" to terrorism financing. No customer relationship is worth compromising the fight against money laundering and terrorist financing.
- Effective and timely communication to get the message across:
  - o documentation of new policies
  - o policies and procedures
  - o emails from top management
  - o posters
  - o training
- Re-organization of the financial institution if necessary.
- Recognize that the fight against terrorist financing is a continuous process because terrorist financiers are constantly using new typologies.
- Provide opportunity for all staff to report suspected terrorism finance cases and a clear channel for open feedback without repercussions.
- Reinforce the highest levels of integrity in the financial institution.
- Appropriate compensation, reward and disincentive programs.

## **BEST PRACTICE 2: AWARENESS AND TRAINING OF EMPLOYEES**

Banks in the forefront of CFT have continuous programmes to increase awareness and training of all employees in relation to their roles in the Bank.

In a statement of principles issued by 6 major United Kingdom banks, they affirmed to devote considerable resources to establish and maintain employee awareness on risks of money laundering and terrorism financing, and their competence to identify and report relevant suspicions. The banks are listed as follows:

- Abbey National Bank
- Barclays Bank
- HBOS (Halifax Bank of Scotland)
- HSBC (Hongkong and Shanghai Banking Corporation)
- Lloyds TSB Group
- The Royal Bank of Scotland

An element of the employee awareness and training program must reflect information and feedback received from regulators and law enforcement authorities on CTF practices and effectiveness of financial institutional efforts.

According to FINTRAC, continuous training is required to make sure employees who have contact with customers, process customer transaction activity, or handle cash in any way, understand the reporting, client identification and record-keeping requirements. This includes front line and senior management employees.<sup>5</sup> When assessing training needs, financial institutions should consider the following 3 areas:

- Requirements and related liabilities

---

<sup>5</sup> [http://www.fintrac.gc.ca/publications/guide/Guide4/4\\_e.asp](http://www.fintrac.gc.ca/publications/guide/Guide4/4_e.asp)

The training should provide an understanding of reporting, client identification and record-keeping requirements and penalties for non-compliance.

- Policies and procedures

Employees, agents, or others who act on your behalf should be aware of the internal policies and procedures for deterring and detecting money laundering and terrorist financing. Each employee should have a clear understanding of his or her responsibilities under these policies and procedures. They need to understand how their institution, organization or profession is vulnerable to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities. Training should include examples of how your organization could be used to launder illicit funds or fund terrorist activity. This should help them to identify suspicious transactions and provide assurance that your services are not abused. For example, employees should be aware that Suspicious Transaction Reports are confidential, and revealing the contents will prejudice a criminal investigation. They should also understand no criminal or civil proceedings will be brought against them for making a report in good faith.

- Background information on money laundering and terrorist financing

The training program should include background information on money laundering and terrorist financing so everyone will understand their mechanics.<sup>6</sup>

---

<sup>6</sup> ibid

**BEST PRACTICE 3: TERRORISM FINANCE AUDITS**

AML/CFT compliance audits were once viewed as a checklist to comply with rules and regulations. As the AML/CFT compliance environment has changed [Please see Diagram 2], financial institutions should now use risk based self-assessments of AML/CFT in financial institutions.

<b>PAST</b>	<b>PRESENT</b>
<b>“Strict Compliance”</b>	<b>“Institutional Risk Management”</b>
“Minimum standards“	Minimum standards plus
Mandated compliance approach	Integrated risk management approach
Enhanced due diligence	Systemic —know your customer“
Point solutions	Enterprise-wide solution
Bank-internal transaction activity	Forensic analysis, including third-party content
Cost/benefit analysis: Expenditure vs. possible exposure	Bottom line business impact

**Diagram 2: AML/CFT Compliance, PAST vs PRESENT**

**Source: ACI and Towergroup<sup>7</sup>**

<sup>7</sup> [http://www.aciworldwide.com/pdfs/aci\\_trends\\_frauddetect2.pdf](http://www.aciworldwide.com/pdfs/aci_trends_frauddetect2.pdf)

All financial institutions are liable for compliance audits by regulators with regards to AML/CFT. The team responsible for AML/CFT compliance function at the financial institution should conduct internal, independent audits within the financial institution at all levels at least once annually. Factors which trigger the need for audits include new products, changes in legislation, non-compliance issues and regulatory requirements.

According to OFAC, for large firms, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas.<sup>8</sup> Larger firms may be able to use an existing internal audit function to conduct the testing or opt for external testing to eliminate doubts of internal personnel ability to stay neutral. However, this approach may not be suitable or cost-effective for smaller firms who lack qualified personnel to conduct such testing. For smaller financial institutions, the audit should be consistent with the firm's risk profile and include an independent self-review.

For financial institutions, FINTRAC provides the following guidelines when conducting AML/CFT audits:

- Interviews with individuals handling transactions and supervisors to determine knowledge of legislative requirements, policies and procedures.
- A review of criteria and process for identifying and reporting suspicious transactions.
- A review of the ability of business units to highlight transactions exhibiting red flag characteristics.
- A sampling of large cash transactions and international electronic funds transfers followed by a review of reporting such transactions.
- A test of validity and reasonableness of exceptions to large cash transaction reports.

---

<sup>8</sup> [http://www.nyscpa.org/committees/sec/ofac\\_sec\\_frb.pdf](http://www.nyscpa.org/committees/sec/ofac_sec_frb.pdf)

- A test of the record-keeping system for compliance with legislation.
- A test of the client identification procedures for compliance with legislation and procedures.<sup>9</sup>

#### **BEST PRACTICE 4. CLOSE WORKING RELATIONSHIP WITH AUTHORITIES**

Intelligence and law enforcement agencies are at the fore front of information gathering but usually bankers do not receive the information. The incorporation services and the corporate registers probably do not have the relevant information to counter terrorism financing. There is a discrepancy between information available to financial institutions and the authorities, hence the gap must be bridged to optimize sharing of information.

Previously mentioned in Best Practice 1, an Indonesian-based Islamic charity, Medical Emergency Rescue Committee (MERC) raised funds by asking donors to send donations to an Australian bank's Jakarta branch. The report said the charity MERC was not listed as a terrorist group by the United Nations but terrorism experts believed some of their funds could end up in the hands of militants. Hence, the bank was accused of terrorism financing.<sup>10</sup>

Actions taken in the UK provide positive examples in achieving such a close working relationship, and bridging information gaps.

In the statement mentioned in Best Practice 2, to combat money laundering and terrorism financing, 6 major UK Banks support the increasing need for a “partnership approach” between government, regulators, law enforcement, banks

---

<sup>9</sup> [http://www.fintrac.gc.ca/publications/guide/Guide4/4\\_e.asp](http://www.fintrac.gc.ca/publications/guide/Guide4/4_e.asp)

<sup>10</sup> <http://www.smh.com.au/news/National/CommBank-denies-terrorism-funding-claims/2006/09/27/1159036569487.html>

and the public. The UK Banks provide appropriate skilled resources to the authorities, access to customer and transaction records at quick notice and regular communication with the authorities. Post 9/11, UK Banks have been providing 24/7 incident support to the authorities and this includes:

1. Account monitoring;
2. Transaction monitoring;
3. Intelligence exchange;
4. Academic collaborations;
5. False/stolen document liaison; and
6. Non-Governmental Organization project. (NGO Project)

### **BEST PRACTICE 5: USE A RISK BASED APPROACH**

A risk-based approach instead of a rule-based approach should be adopted to combat terrorist financing as it is difficult to monitor all transactions that exceed a set threshold. In 2005, Citigroup employed 300,000 people; had a presence in more than 100 countries; maintained more than 200 million customer accounts; and processed more than \$1 trillion of transactions every day.<sup>11</sup> It was impossible for Citigroup to neither scrutinize nor investigate every transaction above a threshold. Instead, a subset of transactions with higher risk elements that triggered more red flags was investigated.

According to the Australian Bankers' Association (ABA), a risk based approach entails notions of judgement and flexibility rather than a mandatory prescriptive

---

<sup>11</sup> <http://www.citigroup.com/citigroup/citizen/antimoneylaundering/index.htm>

regime based on strict liability or zero tolerance. Flexibility involves an element of judgement on the part of the regulated as well as the regulator.<sup>12</sup>

The Wolfsberg Group<sup>13</sup> provides guidance to financial institutions with regards to the risk based approach. Financial institutions should be committed to applying enhanced and appropriate due diligence with customers engaged in sectors and activities that are identified by authorities as being used for financing terrorism. These include underground banking businesses or alternative remittance systems. It is necessary for customers engaged in such sectors or activities to adopt and adhere to specific acceptance policies and procedures and for banks to increase monitoring activity of customers who meet the acceptance criteria.

For instance, in a terrorist profiling project conducted by banks in the UK, the findings revealed:

1. 88% of those linked to terror finance or bank fraud were male;
2. 84% were in the 25-40 age group;
3. 98% were not home-owners;
4. 71% of them held their accounts for less than 2 years with the banks; and
5. 52% of them fit into all of the abovementioned categories.

The project highlighted UK banks' initiative in customer profiling and data collection to assist in risk profiling customers. This project can be similarly replicated at financial institutions in other regions.

---

<sup>12</sup> [http://www.bankers.asn.au/ArticleDocuments/ABA-20536-v1-FS\\_AML\\_CTF\\_submission\\_13\\_April\\_2006.DOC](http://www.bankers.asn.au/ArticleDocuments/ABA-20536-v1-FS_AML_CTF_submission_13_April_2006.DOC)

<sup>13</sup> <http://www.wolfsberg-principles.com/>

## **BEST PRACTICE 6: HIGH STANDARDS OF IDENTITY ESTABLISHMENT (KNOW-YOUR-CUSTOMER)**

Related to the adoption of a risk based approach will be the requirement by banks to know their customers. Proper and appropriate identification of customers must take place to prevent terrorism abuses.

In 2004, the Reserve Bank of India (RBI) released guidelines in the implementation of KYC and they are listed as follows:

1. Customer Acceptance Policy: All banks shall develop criteria for accepting any person as their customer and to restrict any anonymous accounts and ensure documentation of KYC. This is also a regulatory requirement in paragraph 4.1 of MAS 626.
2. Customer Identification Procedures: Customer to be identified not only while opening the account, but also at the time when the bank has doubts about his transactions. This is also a regulatory requirement in paragraph 4.3 of MAS 626.
3. Monitoring of Transactions: KYC can be effective by regular monitoring of transactions. Identifying an abnormal or unusual transaction and keeping watch on higher risk group is essential. This is also covered by paragraph 4.21 to 4.24 of MAS 626.
4. Risk management: Manage internal work to reduce risk of unwanted activity. Managing responsibilities, duties and various audits plus regular employee training for KYC procedures.<sup>14</sup>

---

<sup>14</sup> <http://www.rediff.com/money/2006/sep/12guest.htm>

# KNOW YOUR CUSTOMER!

---






- Do they fit the usual profile of your customers?
- Is the order unusual?
- Are they familiar with chemicals and their use?
- Have you checked their documents carefully?
- Are they being evasive?
- Are they trying to pay in cash?

---




If you notice anything that you suspect may be connected  
with terrorist activity ... **DON'T HESITATE...**  
Call the Anti-Terrorist Hotline on **0800 789321**



Produced by the National Counter Terrorism Security Office

**Diagram 3: Know Your Customer Poster**

**Source: National Counter Terrorism Security Office<sup>15</sup>**

<sup>15</sup> [www.ukhsa.com/documents/ACPO%20Poster%20A4.pdf](http://www.ukhsa.com/documents/ACPO%20Poster%20A4.pdf)

## **BEST PRACTICE 7: TRANSACTION MONITORING**

Financial institutions will need to detect abnormal or suspicious patterns of customer behaviour which indicate criminal or terrorist use. There are 3 main steps by which a financial institution can implement an effective transaction monitoring system. The system can be set up by utilizing technology, filtering transactions using red flag indicators and updating constantly the red flag indicators based on latest terrorism finance typologies.

Upon purchase of a suitable transaction monitoring system for AML/CFT, the system should be populated with black listed names from lists obtained from the United Nations and lists from countries which the firm is operating in. The financial institution should include red flag indicators from open sources, regulators and their own business units.

As an example, the Wolfsberg Group has released a list of red flag indicators for correspondent banking and they are reproduced below:

- transactions involving high risk countries vulnerable to money laundering (if and to the extent this can be identified);
- transactions with correspondents already identified as higher risk correspondents;
- large (value or volume) transaction activity involving monetary instruments;
- travelers checks, money orders, bank drafts) - especially involving instruments that are sequentially numbered;
- transactional activity that appears unusual in the context of relationship with a correspondent;
- transactions involving shell banks;
- transactions involving shell corporations;

- transaction activity frequently involving amounts that are just below local transaction reporting requirements, or transactions or enquiries that test an Institution's internal monitoring thresholds or controls.<sup>16</sup>

Details on money laundering and terrorism typologies examination conducted by FATF can be obtained from [www.fatf-gafi.org](http://www.fatf-gafi.org). For instance, red flag indicators for Alternative Remittance Services can be obtained from <http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf>.

Lastly, the financial institution should keep abreast of the latest money laundering and terrorist financing methods and update its transaction monitoring system accordingly.

### **BEST PRACTICE 8: SUSPICIOUS ACTIVITY REPORTING (SAR)**

SARs reporting is an integral part of the AML/CTF system. SARs reporting is known to be more useful against money laundering and less for terrorist financing. However the nexus between money laundering and terrorist financing exists because terrorist funding includes a criminal element. According to Dr Loretta Napoleoni, author of “Terror Inc”, the most important entry in the terror balance of payments is drug smuggling. Terror groups have successfully established commercial co-operation with criminal organizations in the narcotics trade.<sup>17</sup>

In conversations with bankers involved in compliance, they will mention making tremendous disclosures and but the after disclosure the case drops into a “black hole” and never heard of again. There have also been reports of “defensive filing”

---

<sup>16</sup> [www.wolfsberg-principles.com/pdf/faq-correspondent-banking-app1.pdf](http://www.wolfsberg-principles.com/pdf/faq-correspondent-banking-app1.pdf)

<sup>17</sup> <http://www.senliscouncil.net/modules/events/paris/napoleoni>

of SARs by financial institutions to avoid risking penalty. FinCEN expects SARs filed in the US to reach record levels in 2006.<sup>18</sup>

Suspicious Activity Report filings by year (US Banks)	
Year	Number
2001	203,538
2002	273,823
2003	288,343
2004	381,671
2005	522,655

**Diagram 4: SARs filed by US Depository Institutions, 2001-2005**

Source: FinCEN, [www.moneycentral.msn.com](http://www.moneycentral.msn.com)<sup>19</sup>

SARs are still a valuable resource in investigation and identification of terrorism funds, especially with the aid of intelligence sources. Negative attitudes with respect to the reporting of SARs mentioned above should be avoided. Guidance for proper filing of SARs against money laundering is available from national regulators and best practices documents from international bodies.

---

18

<http://articles.moneycentral.msn.com/Banking/FinancialPrivacy/WhyYourBankThinksYoureATerrorist.aspx?page=1>

19

<http://articles.moneycentral.msn.com/Banking/FinancialPrivacy/WhyYourBankThinksYoureATerrorist.aspx?page=1>

A list of best practices which includes the terrorist financing element into SARs disclosures has been released by the Business Executives for National Security (BENS) in the US. Financial institutions should file a SAR disclosure for transactions with the following characteristics:

- Financial activity to and from countries identified as state sponsors of terrorism
- Financial activity inconsistent with the stated purpose of the business
- Financial activity not commensurate with stated occupation
- Use of multiple accounts at a single bank for no apparent purpose
- Importation of high dollar currency/traveler's checks not commensurate with stated occupation
- Structuring of deposits at multiple bank branches to avoid BSA requirements
- Abrupt changes in account activity
- Use of multiple personal and business accounts to collect and then funnel funds to a small number of foreign beneficiaries.<sup>20</sup>

---

<sup>20</sup> [http://www.bens.org/images/BENS\\_SAR\\_Report.pdf](http://www.bens.org/images/BENS_SAR_Report.pdf)