

Insights into Counter Financing for Terrorism and its implications from banking perspective

ABS-IDSS Project on Counter Financing for Terrorism

**Prepared by: Gunawan Husin / ABS Fellow
May 2006**

Table of contents

1. Preface	3
2. Financial Crime: Money Laundering and Terrorist Financing.....	4
3. Terrorism is cheap?	5
4. Implications on Banking Sector	6
5. Counter measures – banking perspective	7
5.1 Sound AML / CFT Program	7
5.2 Promoting Risk-Based culture	8
5.3 Continued cooperation within financial sector and other relevant agencies ...	9
6. Implementation Issues	10
7. Conclusion	12
Appendix 1.....	13

1. Preface

Counter Financing for Terrorism was criminalised under United Nations International Convention for the Suppression of the Financing of Terrorism in 1999¹. The 1999 convention was reinforced by United Nation Security Council Resolution 1373 in 2001. Soon after the 9/11 attacks, America introduced US Patriot Act, an important tool in the war on terrorist financing, which allows US Treasury department to ask any of around 7,000 US financial institutions for immediate information on any account

United Nations and Financial Action Task Force (FATF)² also established new measures for members to adopt in order to help track and freeze terrorist assets.

Singapore, as one major financial hub in Asia and globally, sees its important role in combating financial crime such as Money Laundering and Terrorist Financing. Today, It has strict legislations that criminalise acts such as terrorism. The legislations are as follows:

- (a) The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A);
- (b) The Terrorism (Suppression of Financing) Act (Cap. 325); and
- (c) The Monetary Authority of Singapore (Anti-terrorism Measures) Regulations 2002

In 2005, Monetary Authority of Singapore issued a Consultation Paper on proposed revisions to MAS 626 Notice on Prevention of AML/CFT.

Today more governments continue to commit to fight financial crime. Canada has shown its commitment to provide international financial assistance to Asia and Caribbean countries³. In March 2006, China has also ratified United Nations conventions to fight Terrorist Financing.

The potential damage to business and society is huge hence clear and effective strategy is crucial. However due to the wide differences in jurisdictions, legislations of different economies in the global financial system, the struggle against terrorism continues to be a huge challenge.

This paper provides insights into the key importance of understanding Terrorism Financing, the important roles played by financial sector in Counter Financing for Terrorism, discussion on counter measures and implementation issues.

¹UN 1999 International Convention for the Suppression of the Financing of Terrorism (UN Security Council Resolution 1373) – “Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out”

(a) An act, which constitutes an offence within the scope of and as defined in one of the UN treaties on terrorism
(b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.”

² The FATF is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing.

³ <http://www.fin.gc.ca/news06/06-007e.html>

2. Financial Crime: Money Laundering and Terrorist Financing

In both money laundering (AML) and terrorist financing (CFT), criminals and terrorists exploit the loopholes or other weaknesses in the legitimate financial system to launder criminal proceeds, to support terrorism and ultimately hide the actual purpose of their activity. Criminals and Terrorists use many different techniques to "launder" their illicit profits. These might involve anything from buying a simple cashier's cheque to extremely complex schemes involving the high volume purchase and sale of real estate or bonds.

Money laundering and Terrorism Financing works in a permissive environment where there is lax of supervision from the relevant banking authority, poor risk-based customer due diligence process, non-understanding of the financial and non-financial indicators generated by a suspicious transaction and the exploitation of banking system loopholes.

Despite a similarity in methodology, it is important to note some key differences in the context of AML and CFT. Money laundering is the process of filtering money obtained through illegal activities, such as drug trafficking, through the financial system. The purpose is to conceal illegal sources of income and allow criminals to spend their profits without revealing the crimes that produced them. Terrorist Financing is often referred to as 'reversed money laundering', where it focuses on using legal assets for carry out terrorist activities. Key sources of funds in terrorist financing are generally clean sources such as charity organizations and revenues made from legal business.

The other key difference is the motivation. The key motivation in terrorist financing is ideological, as opposed to the profit motive behind most criminal financial activities.

Today, we see increasing nexus between terrorism and criminal activities. With the disrupted flow of funds from Middle East, terrorists in Southeast Asia for instance, are engaging more in criminal activities for funding, and making use of money laundering techniques to distribute their funds, in conjunction with cash couriers, use of alternative remittance system or most commonly known as Hawala system.

Terrorist Financing has become very important in recent years. It is widely acknowledged to be an essential component of terrorist activity, as terrorists are able to facilitate their activities only if they have the financial resources to do so. After 9/11 attacks, combating the financing of terrorism has reserved its own specialization. FATF developed special recommendations that have since been considered to be the standards in the fight against terrorist financing.⁴

Subsequently, European Union, the United States and others have published lists of persons and entities suspected of terrorism and are calling for the blocking of all related assets and the facilitation of international investigative cooperation.

⁴ <http://www.fatf-gafi.org> , Special Recommendation on Terrorist Financing, October 2001

3. Terrorism is cheap?

In August 2004, the United Nations (UN) Monitoring Team report on Taliban and Al Qaeda described the following costs involved in various terrorist attacks.

- (a) Madrid train bombings, March 11, 2004: \$10,000
- (b) Istanbul truck bomb attacks, November 15 and 20, 2003: \$40,000
- (c) Jakarta JW Marriot Hotel bombing, August 5, 2003: \$30,000
- (d) Bali bombings, October 12, 2002: \$50,000
- (e) USS Cole attack, October 12, 2000: \$10,000
- (f) East Africa embassy bombings, August 7, 1998: \$50,000

These figures create a belief on cheap terrorism, causing a perception that it does not require a lot of money to make simple explosive devices. This is particularly true when we are dealing with simple structured organisations such as Palestinian in the 70's and Algerians in the 80's.⁵

However, when this is applied to the entire Al Qaeda's network, not only it is irrelevant but also will drive to an end on war against terrorism financing. The general argument is that there is only small and insignificant amount incurred during the operational stage of a terrorist attack, hence it is extremely difficult to trace and also money may never have entered the financial system in the first place.

There is an obvious huge disconnect between a multi billion terrorism economy as against the cost of thousands of dollar to blow up a train. To do this, we need to understand the terrorist group's objective, from organizational and operational level.

The 9/11 attacks on America clearly shows that banks were mainly used by the terrorists in their funds distribution. Many have argued that should there be more cooperation and information sharing between relevant institutions, then perhaps this could have been avoided. The appendix section of this paper shows the money trail of the 9/11 attacks.

As an organisation, a terrorist group needs to maintain its array of activities that allow itself to achieve its main mission, such as the establishment of Islamic caliphate. To do this, they need money to recruit, to indoctrinate, to communicate, to create infrastructure such as safe house, sleeper cells and bomb making facility, to travel, to train, to bribe local officials and to purchase other equipments. Most of these are not cheap and are beyond the financial means of individual terrorist, therefore require a proper organisation structure that facilitates collection and distribution of funds.

The operational objective of a terrorist group aims for success in carrying out an attack. At this operational level, the activities include procurement, preparation and delivery of material, weapons and vehicles, reconnaissance of target and assault on targets.

⁵ Brisard, J.C, Terrorism Financing – Roots and Trends of Saudi terrorism financing, JCB Consulting, 2002

Terrorist relies on international financial system to carry out their operations. The later section will discuss further the role financial institutions in war on terror, by safeguarding its financial system from terrorist infiltration, therefore preventing future acts of terror directly and by providing information to law enforcement authorities, intelligence agencies, and military personnel.

Loretta Napoleoni, a global terrorist financing expert, defines the financial network as terror's Balance of Payments. The cash inflow includes revenues from main categories such as legitimate business, illegal revenues and criminal activities. The cash outflow refers to those expenses discussed earlier as organizational and operational expenses. This Balance of payment is related to war economies that sustain terror, criminal activities and legitimate activities. The big question here is how big is this economic system and how much it overlaps with the world economy.⁶

4. Implications on Banking Sector

Post 9/11 attacks on America, we see financial sector under increasing pressure from governments, especially in US Federal government, to furnish information about their consumers suspected wrongdoing. Hundreds of thousands of transactions involving banks' customers, other financial sectors, and even casinos are reported to US Treasury department.

According to FinCen, the US Financial Intelligence Unit, in its February 2006 report, American institutions filed 689,414 Suspicious Activity Report (SAR) forms in 2004, and through the first six months of 2005, 435,167 SAR forms were filed. Fintrac, the Canadian Financial Intelligence unit, said in November 2005 that it had unearthed more than \$2 billion in suspicious financial transactions, including \$180 million linked to the financing of terrorism, over the previous year.

Main reason behind the massive increase in the filing is the expanded coverage on other financial services provider such as money-order issuers, currency exchanges, broker dealers, futures commission merchants, insurance companies and mutual funds. The other reason is to safeguard the reporting institution on tougher examination process, resulting in hefty fines and regulatory compliance problems.

In December 2005, ABN AMRO New York branch was fined for USD 80 Million for failing to set up adequate compliance program within its Correspondence Banking business, and most recently in April 2006, Bank Atlantic was fined for USD 10 Million for similar violations.

In Asia, we have yet to see prosecution of financial institution on such violation, like those in USA. In September 2005, US Department of Treasury designated Banco Delta Asia in Macau as a primary money laundering concern. It had allegedly provided financial services to multiple North Korean government agencies and front companies that have engaged in Money Laundering and the proliferation of weapons of mass destructions (WMD).

⁶ Napoleoni, L, Modern Jihad – Tracing the Dollars behind the Terror Networks, Pluto Press, 2003

5. Counter measures – banking perspective

Some key observations from recent Banking Secrecy Act (BSA) violations under US contexts, can be summarized in three key areas, as follows:

- (a) Lack of sound AML / CFT program
- (b) Having AML / CFT program that does not cover your risk
- (c) Lack of understanding on regulatory requirements

The following counter measures provide some recommendations on banking perspective, in response to several key observations learnt from several US BSA violations.

5.1 Sound AML / CFT Program

It is extremely important that Banks and/or other financial institutions understand that their key vulnerability point is the point of entry into their systems. Sound AML/CFT program must include comprehensive KYC (know your customer) and CDD (customer due diligence) process in place, supplemented by record keeping. The key deadly sins of ABN AMRO New York, along with other institutions were, not being able to identify and monitor obvious high-risk customers, willful blindness in the face of suspicious activity and to let dangerous wire transfers going through foreign institution's correspondent account⁷

Point of entry represents key vulnerability of Banks, as well as the terrorist/criminal groups, because this is the point where they are more prone to detection. FATF provides in depth recommendation on KYC and CDD process, as they acknowledged the increasingly sophisticated techniques used by terrorist / criminal groups to enter banking system. For example, using legal persons to disguise true ownership and control over illegal funds.⁸

AML/CFT Program should also consist the following elements, as follows:

- (a) Designation of AML/CFT officer
- (b) Documentation of policies, procedures and internal control
- (c) Training program
- (d) Periodic transaction testing
- (e) Independent program review

Implementation of appropriate CFT technology could also help. Today, the anti money laundering technology focuses on identifying suspicious transactions that have little resemblance to those typically used by terrorists. The current technology could be reconfigured to include indicators that better fit the profile of terrorist financing, for example, liquidating accounts or purchases of high risk materials.

⁷ The Seven Deadly sins of ABN AMRO, AmSouth, Arab Bank, Bank of New York, Lehman Brothers and Oppenheimer, and their lessons, International Money Laundering Conference, 15 March 2006, Florida

⁸ The Forty Recommendation, Financial Action Task Force on Money Laundering, 20 June 2003

5.2 Promoting Risk-Based culture

Often, question such as how much do we need to do and spend on AML/CFT program are asked. The answer really depends on factors such as, location, business and products or services offered to the customers.

Good understanding of these key factors will enable a financial institution to create an approach with the corresponding risk mitigation measures, and its action plan for residual risks.

Risk based approach should include the following elements, such as:

- (a) Type of customers
- (b) Geographical area
- (c) Type of business, such as on line business, non-face to face business?
- (d) Business activities / services / products
- (e) Reasonable mitigating factors
- (f) Plan of action for residual risk
- (g) Management approval

Promoting a risk-based culture within an organisation also allows greater cooperation between different departments. Typically, banks need to face the classic arguments between profit maximization and risk management. Who else would be in a better position to understand the business profile of a customer, other than its relationship manager?

It is also important for Banks to understand the risks behind their products and services offering. Under today's environment, it is not only the 'Know your Customers' process, but also to know your customers' customers, your employees and your outsourcing parties. In United States for example, the definition of Politically Exposed Persons (PEPs) extends to the PEPs' family circle.

Some of the high risks banking products include:

- (a) Correspondent Banking
- (b) Cash Management

Correspondent Banking is often referred to as a banker's bank, and it covers domestic and foreign correspondent banking accounts. A bank maintains correspondent relationships with other banks to provide certain services that can be performed more economically or efficiently due to the other bank's size, expertise or geographic location. The services include deposit accounts, funds transfer, cheque clearing, letter of credits, loans and others such as data processing and payroll services.

The risk factor is higher for foreign correspondent banking accounts, as some foreign financial institutions are not subject to the same jurisdiction, hence this poses higher risk. The normally large amount of funds, multiple transactions and lack of familiarity of foreign FI's customers, criminal and terrorists can easily conceal the source and the use of illicit funds. The risk mitigation process in this case relates back to the key point of entry, and they are the Know Your Customer and Customer Due Diligence process.

One common Cash Management product is Electronic Banking. Electronic Banking provides electronic delivery of banking products to customers, including ATMs, On-line account opening, Internet banking transactions and Phone Banking facility. Despite the greater convenience to customers, not only this facility is subject to fraud, but also it is high in volume and is subjected to use by unknown third party sometimes outside the bank's targeted geographic area.

5.3 Continued cooperation within financial sector and other relevant agencies

In Singapore, counter measures on Money Laundering and Terrorism Financing were introduced to safeguard its integrity as a world-class financial and commercial centre, through vigilant and professional enforcement of the laws.

The Commercial Affairs Department (CAD) of the Singapore Police Force is the agency tasked to investigate into Money Laundering and Terrorism Financing activities. The measures are grouped into the following categories:

- Legislation
- Strict Enforcement Action
- Partnership with business community
- International co-operation⁹

The Association of Banks in Singapore (ABS) Financial Crime Task Force is also another good example on active collaboration between key banks in Singapore, to promote sharing of best practices, technology, knowledge and information.

The current CFT project initiated by ABS and IDSS-ICPVTR¹⁰ also sees the importance of positive collaboration between financial sector, academic sector from different countries and law enforcement agencies of different countries, in the continued battle against terrorism financing.

⁹ Anti Money Laundering & Counter-Terrorism Financing, Commercial Affairs Department, Singapore, 2002

¹⁰ Joint initiative between Association of Banks in Singapore (ABS) and International centre of political violence and terrorism research – Institute of Defense and Strategic Studies (ICPVTR – IDSS) of Nanyang Technological University, Singapore, 2005-2006

6. Implementation Issues

This section will discuss some factors surrounding our financial sector, which hinder the effective implementation of the counter measures, especially in the area of cooperation between different sectors and countries.

Within a financial institution, as was earlier discussed, the common loopholes or deficiency in the banking system. Factors such as inadequate customer identification program, its implementation and reinforcement, as well as due diligence process are the key issues in the financial sector.

Some other factors are also evident in the financial regulations such as:

- (a) Inadequate rules for the licensing and creation of financial institutions.
This refers to the assessment of the managers' background and owners. In some countries, it is possible for individuals or legal entities to operate financial institutions without effective authorization or registration, and this loophole can be penetrated by terrorists or criminals to hold controlling position in those institutions.
- (b) Lack of training given to front line staff, on money laundering and terrorist financing
- (c) Procedures on record keeping on clients identity and transactions
On the other hand, it is also important to have law, that require effective identification of the beneficiary
- (d) Absence of mandatory suspicious transactions reporting system and lack of sanctions for failure to make effective reporting
- (e) Excessive secrecy provisions ¹¹

Global financial system includes main units such as banks, insurance companies, money service business, securities brokerage, and other Non Bank financial intermediaries. These units are created under well-established corporate laws and they are required to comply with local financial regulatory requirements, backed by the threat of civil or criminal penalties.

Regulatory requirements in different economies are highly unequal. Financial Institutions in US for instance, are subject to far more stringent provisions, including terrorist financing. However international cooperation is still crucial, as Al-Qaeda is also relying on other non-US based global financial system, including the Islamic banking system, through which it can still transfer, store and invest its funds.

Enforcement of financial laws and regulations has also proven difficult to sustain. According to British Bankers Association, banks in UK have spent about GBP 250 Million every year to comply with anti-terror and anti-money laundering laws.¹²

¹¹ Manual on Countering Money Laundering and the Financing of Terrorism, Asian Development Bank, March 2003

¹² The Economist, Looking in the wrong places, 20 October 2005

Other key contributing factors that represent obstacles to international cooperation include:

- (a) Restrictive laws or regulations prohibiting international exchange of information,
- (b) Prohibiting authorities from conducting investigations on behalf of foreign counterparts,
- (c) Obvious unwillingness to respond constructively to requests for assistance, and generally restrictive practices relating to the investigation of suspicious matters,
- (d) Failure to criminalize financial crime and refusal to provide judicial cooperation with investigations, particularly on the grounds that tax matters might be involved
- (e) Inadequate resources
- (f) Failure to provide the administrative and judicial authorities with the necessary financial, human, or technical resources to exercise effective oversight or conduct investigations,
- (g) Inadequate or corrupt professional staff, and
- (h) Lack of a centralized Financial Intelligence Unit for the collection, analysis, and dissemination of relevant information¹³

¹³ FATF, Report on Non-Cooperative Countries and Territories, 2000

7. Conclusion

Post 9/11 attacks on America had seen tougher financial compliance standards, especially in western countries. Opening account in a bank is no longer a simple process. More demands for identification and sources of fund are causing longer wait to access the money and ultimately higher costs of transaction.

On the other hand, the banking sector itself is bearing additional burden to stop funds flow into terrorist financial network. Banks are scanning their customer accounts more carefully for signs of suspicious people and transactions. Accounts have been frozen and in America, foreign banks have been cut of from doing business, if they are not sharing information. Banks comply with the rules because of fear of sanctions and reputation risk.

Given these facts, terrorists are also getting smarter and continue to show the ability to keep their money flows alive, by also resorting to primitive means such as cash couriers across countries with loose border control.

The financial and non-financial counter measures in combating terrorism financing must work collectively to ensure effectiveness. Not only, we must look into creating indicators on financial behaviour of the terrorist groups and linking charities with terrorism, but also we need to deal with the whole question of indoctrination process, where the radical jihad philosophy is being taught. Without these, the financing of terrorism will be difficult to stop.

IDSS-ICPVTR ¹⁴ believes in multi dimensional counter terrorism strategies or responses. Along with Financial response, the centre is actively working with other relevant agencies in Singapore and overseas, on Ideological response, Educational response, Legislative response and Media response.

¹⁴ More details on counter terrorism initiatives of International Centre for Political Violence and Terrorism Research, refer to www.pvtr.org

Appendix 1.

Funds movement in September 11, 2001 attacks on America, as described by FBI.

The 19 hijackers opened 24 domestic bank accounts at four different banks. The following financial profile was developed from the hijackers' domestic accounts:

Account profile

- Accounts were opened with cash/cash equivalents in the average amount of \$3,000 to \$5,000
- Identification used to open the accounts were visas issued through Saudi Arabia or the U.A.E
- Accounts were opened within 30 days after entry into the U.S
- All accounts were normal checking accounts with debit cards
- None of the hijackers had a social security number
- They tended to open their accounts in groups of three or four individuals
- Some of the accounts were joint accounts with others
- Addresses used usually were not permanent (i.e. mail boxes, etc.) and changed frequently
- Hijackers would often use the same address/telephone numbers on the accounts
- No savings accounts or safe deposit boxes were opened
- Hijackers would open their accounts at branches of large well known banks
- The majority of hijackers (12) opened accounts at the same bank

Transaction profile

- Some accounts would directly receive/send wire transfers of small amounts to foreign countries UAE, Saudi Arabia, Germany
- Hijackers would make numerous attempts of cash withdrawals which often would exceed the limit of the debit card
- High percentage of withdrawals were from debit cards vs. low percentage of checks written
- Numerous balance inquiries were made
- Hijackers would often travel domestically
- There was a tendency to use Western Union to wire money
- One deposit would be made and then the money would trickle out a little at a time
- Account transactions did not reflect normal living expenses for rent, utilities, auto payments, insurance, etc
- There was no normal consistency with timing of deposits/disbursements
- Funding for normal day to day expenditures was not evident from transactions
- Overall transactions are below reporting requirements
- Funding of the accounts dominated by cash and overseas wire transfers
- ATM transactions occur where more than one hijacker present (uninterrupted series of transactions involving several hijackers at the same ATM)
- Use of debit cards by hijackers who did not own affected accounts

International Activity

- Three of the hijackers supplemented their financing by opening foreign checking accounts and credit card accounts at banks located in the UAE
- While in the U.S., two of the hijackers had deposits made on their behalf by unknown individuals
- Hijackers on all four flights purchased traveler's checks overseas and brought them to the U.S. These traveler's checks were partially deposited into their U.S. checking accounts
- Three of the hijackers (pilots/leaders) continued to maintain bank accounts in Germany after moving to the U.S
- Two of the hijackers (pilots/leaders) had credit cards issued by German banks and maintained those after moving to the U.S
- It is suspected that other unknown foreign accounts exist that were opened by the hijackers to further supplement the financing of the September 11, 2001, attacks
- One of the hijackers (pilot/leader) received substantial funding through wire transfers into his German bank in 1998 and 1999 from one individual
- In 1999, this same hijacker opened an account in the UAE, giving power of attorney over the account to this same individual who had been wiring money to his German account
- More than \$100, 000 was wired from the UAE account of the hijacker to the German account of the hijacker in a 15-month period.¹⁵

¹⁵ Dennis M. Lormel, Chief, Financial Crimes Section, Federal Bureau of Investigation, Statement for the Record, House Committee on Financial Services, Subcommittee on Oversight and Investigations, Washington, D.C., February 12, 2002