The Role of Information Risk Management in Combating Global Money Laundering and Terrorism Financing

Wipul Jayawickrama

Infoshield Consulting

Introduction

Money laundering and terrorism financing are financial crimes that are becoming an increasing global problem since the 1980s. As a result, the Financial Action Task Force (FATF), a 33-member organisation whose main responsibility is to develop an international standard for anti-money laundering and combating of terrorism financing, was established, and the first internationally-recognised Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) programme was established.

Today, anti-money laundering and counter terrorism financing compliance is a regulatory requirement promoted by several conventions and international treaties. Compliance is required to:

i. Meet international obligations and needs to combat money laundering and financing of terrorism,

ii. Maintain good relations with foreign and international organisations,

iii. Avoid financial penalties, and

iv. Maintain reputation.

In its simplest form, an anti-money laundering and counter terrorism financing compliance requires an entity to:

i. Implement an organisational anti-money laundering and counter terrorism financing program,

ii. Verify the identity of customers before providing them with designated services, and

iii. Report suspicious as well as certain specifically defined transactions.

Anti-money laundering and counter terrorism financing compliance is an information intensive activity. The accuracy, completeness and timeliness of the information used in the program are essential for the success of the program. Information risks, such as, breach of confidentiality and integrity, lack of availability, uncertainty of authenticity and the ability to repudiate information-related activity can affect the success of the program. Therefore, risk management of information and related technology becomes an essential part of the anti-money laundering and countering terrorism financing programs.

What is Money Laundering and Terrorist Financing?

Money laundering is the process of hiding the origin of illegally-obtained money. As per the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) and United Nations Convention against Transnational Organised Crime (2001), this includes:

i. Knowingly transferring or converting property that is proceeds of crime,

ii. Concealing the source, location, movement, and ownership and rights of property that is the proceeds of crime, and

iii. Acquiring, owning or using property, knowing that such property is the proceeds of crime.

Terrorist financing is the solicitation, collection and provision of funds to support terrorist acts or groups. The financing of terrorism can be done by both legally- and illegally-obtained funds. The International Convention for the Suppression of the Financing of Terrorism (1999) states that a person commits the crime of financing terrorism "if that person by any means, directly or indirectly unlawfully and wilfully, provides or collects funds with the intention that they are to be used, in full or in part, in order to carry out" acts of terrorism.

While similar methods are used for both money laundering and terrorist financing, and proceeds of money laundering may be used in the terrorist financing, the two processes do not share the same goal. The goal of money laundering is to conceal the source of illegally-obtained funds. The goal of terrorist financing is to collect and provide funds for terrorist activities.

How Big is the Problem?

Money laundering and terrorism financing are crimes that have far reaching negative economic and social impacts on the society, resulting in destabilised economies and wide-spread social impacts such as crime, substance misuse and loss of life. Unfortunately, both money laundering and terrorist financing are pervasive.

It is difficult to measure the actual amounts of money laundered or used to fund acts of terrorism. FATF has admitted that it is 'absolutely impossible to produce a reliable estimate of the amount of money laundered'. There is very little published statistics, but it is

common agreement that billions of dollars of illegally obtained money is laundered each year.

The available statistics are staggering. In a recent report released by the Colombian Ministry of Finance, the estimated amount of money laundered internally was 8.667 Billion Dollars. This is 3 per cent of the Gross National Product (GNP) of Columbia. The report also states that there were 42,950 suspicious transactions reported over the past 5 years. It is surmised that a major proportion of this money comprises of cash smuggled out of US and Canada, and that it is used to finance the Columbian narcotics industry.

A report by the Australian Institute of Criminology in 2007, estimated that AUD 2.8 to 6.3 billion was laundered 'in and through' Australia.

Regardless of the actual figures, money laundering and terrorist financing pose a significant problem to governments and society as a whole.

Combating Money Laundering and Terrorist Financing

Due to the transnational nature of both money laundering and terrorist financing, international cooperation is required to combat these global threats. It also requires internationally-accepted policy and standards to ensure a unified and coordinated approach. Since 1989, FATF has been the body that develops and promotes international policy. FATF has published 40 recommendations and 9 special recommendations, commonly known as the 40+9 recommendations and a 'Methodology for Assessing Compliance with the FATF 40+9 Recommendations'.

Other influential internationally-accepted conventions and directives include:

i. United Nations Convention against Corruption,

ii. Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism,

iii. European Parliament Directives on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing,

iv. United Nations Conventions against Terrorism.

Many governments have implemented legislative frameworks to combat money laundering and terrorist financing activity that are compliant with the above-mentioned conventions and directives. Legislation acts as a deterrent to money laundering and terrorist financing activities, and provides a framework for taking action against identified perpetrators of these activities.

Impact on Financial Institutes

Financial institutions and banking systems constitute a large proportion of the platform that is used to convert and transfer illegal funds. Instruments such as, bank credits, travellers' cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, are used in both money laundering and terrorist financing activities. There is a serious concern about the use of financial institutions and the banking system in these illegal activities. As a result, compliance with anti-money laundering and counter terrorism financing regulation is mandatory to financial institutions.

The penalties for non-compliance can vary in different jurisdictions. Non-compliance can result in legal and financial penalties, and depending on the jurisdiction, local law can also hold individuals within an organisation liable to penalty. For example, in Australia, a breach of anti-money laundering legislation can result in civil and criminal penalties to organisational leadership.

Financial penalties can be heavy. There are several instances where financial organisations that are in breach of compliance requirements have been heavily fined. Some examples of fines imposed on financial institutes in the past few years include:

(i) Bank of Ireland - £375,000 in 2004 for issuing 40 unidentifiable bank drafts,

(ii) Royal Bank of Scotland - £ 750,000 in 2002 for not having adequate controls to verify the identity of their clients £5.6 million in 2010 for lending to people on government ban lists,

(iii) Abbey National Banking Group - £2.3 million in 2003 for breaches of the anti-money laundering regulations and breakdowns in systems and control procedures,

(iv) Riggs Bank - US$25 million in 2004 for failing to design and implement a suitable anti-money laundering program. A further US$ 16 million criminal fine,

(v) ANZ Banking Corporation - US$5.75 million in 2009 for violations of US sanctions against Sudan and Cuba,

(vi) Pacific National – US$ 7 million in 2011 violation to the Bank Secrecy and US Patriot acts.

The impact on financial institutes is not limited to financial loss. Reputational damage can be significant, and may result in restrictions and sanctions imposed on the institution depending on the extent of the breach, both resulting in loss of revenue and their competitive edge.

Therefore, the establishment of anti-money laundering and counter terrorism financing programs is a non-negotiable requirement for the financial industry.

The Organisational Anti-Money Laundering and Counter Terrorism Financing Program

Many countries have imposed mandatory reporting requirements for large transactions to respective reporting authorities. For example, in the United States of America,

there is a requirement to report all transactions over USD 10,000 to the Internal Revenue Service. Similarly, in Sri Lanka transactions over LKR 1,000,000 have to be reported to the Central Bank's Financial Intelligence Unit (FIU). Most banking and financial systems possess the capability to identify and generate automated reports of these transaction.

However, experienced money launderers do not conduct large transactions that result in drawing attention to them. It is the responsibility of the financial institution to implement suitable procedures and systems to:

(i) Identify sanctioned and suspicious customers and transactions, and

(ii) Report sanctioned and suspicious transactions to appropriate authorities.

To be able to identify and report sanctioned and suspicious transactions, the organisation needs to have a robust anti-money laundering and counter terrorism financing program. Aspects of this programme include:

i. Maintaining an anti-money laundering and countering terrorist financing policy,

ii. Maintaining organisational awareness of the policy and its implications,

iii. Maintaining a list of global sanctions obligations,

iv. Providing training to relevant staff on identifying and reporting sanctioned and suspicious transactions,

v. Designing business rules to ensure that no individual transaction can knowingly breach anti-money laundering and countering terrorist financing,

vi. Defining clear processes to enable identification and reporting sanctioned and suspicious transactions,

vii. Implementing controls to prevent deliberate subversion of the compliance requirement,

viii. Ensuring that business partners do not engage in business activities that can lead the organisation breaching applicable compliance requirements, and

ix. Screening new and existing customers and staff to ensure that they are not on a sanctioned list.

The Role of Information Technology in the Compliance Process

There is an on-going attempt to subvert the anti-money laundering and countering terrorist financing programs. These attempts are becoming increasingly sophisticated. Therefore, access to timely, accurate and relevant information is critical to a successful anti-money laundering and countering terrorist financing program. This requires efficient use of information-related technologies to filter customer data and inspect this data for anomalies.

Typically, technology used in the anti-money laundering and countering terrorism financing uses rule-based analytics capable of name analysis and profiling of transactions. For example, the frequency and size of transactions and flags to indicate that a certain person is on a watch list were used to identify transactions that potentially could be related to money laundering and terrorism financing activity. However, detection based on such rules and analytics can be subverted using smaller and distributed transactions and using associates to conduct transactions. To ensure that such subversive activity is detected, intelligence capabilities such as link analysis, peer group analysis and time sequence matching should be integral to a good anti-money laundering and countering terrorism financing technology implementation.

The Role of Information Risk Management

Anti-money laundering and countering terrorist financing programmes are information intensive. The use of inaccurate information, for example something as simple as a mis-spelt name or a name with alternate spelling can result in a severe compliance breach. A premature release of information may result in the inability to prevent a suspicious transaction. Many other information risks can affect the integrity of an otherwise successful anti-money laundering programme. Therefore, is it important to ensure that information risk is managed throughout the anti-money laundering and counter terrorist financing program.

Information risk management is the application of the generic process of risk management to information assets and the information environment. All aspects of information risk, i.e., the risk of breaches of confidentiality; integrity and availability on information as well as non-repudiation of information-related activity are applicable in the anti-money laundering and countering terrorist financing information management environment. Other information-related risks can include breach of privacy and data protection legislation.

Due to the sensitive nature of the anti-money laundering and countering terrorist financing information environment, an active approach to information risk management should be adopted. Information is subject to various vulnerabilities and threats. These could be inherent to the information systems as well as deliberate attempts of subversion. Internal risk management frameworks, information governance frameworks and information security management programmes should be used to create a secure environment for storing, processing transmitting and archieving of information used in the anti-money laundering program.

In Summary

There are global obligations and compliance requirements imposed on governments and various commercial and non-commercial entities to identify and report suspicious transactions that may support money laundering and terrorism financing activities. Anti-money laundering and counter terrorism financing reporting programs are highly information intensive. Breach of information attributes, such as, confidentiality, integrity, availability authenticity and non-repudiation can impact the outcomes of these programs resulting in penalties, reputational loss and negative impacts on international relationships. Therefore, it is important to ensure that an effective information risk management program is in place to support the objectives and integrity of these programs. ■