

FINANCIAL INTELLIGENCE UNIT ANNUAL REPORT 2014



FINANCIAL INTELLIGENCE UNIT OF SRI LANKA



FINANCIAL INTELLIGENCE UNIT
ANNUAL REPORT 2014

ISBN 978-955-575-312-8

CONTENTS

LIST OF ACRONYMS	3
YEAR 2014 AT A GLANCE	5
GOVERNOR'S MESSAGE	7
DIRECTOR'S MESSAGE	8
FUNCTIONAL ORGANIZATIONAL CHART	10
FIU-SRI LANKA STAFF.....	11
CHAPTER 1: VISION, MISSION, AND STRATEGIC GOALS	
Vision	12
Mission	12
Strategic Goals	12
CHAPTER 2: MANAGEMENT OF INFORMATION	
2.1 Collection of Information	13
Cash Transactions and Electronic Fund Transfers	13
Suspicious Transaction Reports (STRs)	14
2.2 Analysis of Information	16
2.3 Dissemination of Information	17
2.4 Suspension, Confiscation and Prosecution Relating to ML/TF	18
CHAPTER 3: DOMESTIC AND INTERNATIONAL CO-OPERATION	
3.1 Domestic Co-operation	19
Law Enforcement Agencies (LEAs)	19
Supervisory Authorities	19
Co-operation on National Risk Assessment (NRA)	19
3.2 International Co-operation	22
Memorandums of Understanding (MOUs)	22
Asia/Pacific Group on Money Laundering	23
Egmont Group	24
CHAPTER 4: INSTITUTIONAL COMPLIANCE	
4.1 Ensuring Compliance of Reporting Institutions	29
4.2 Off-site Surveillance	29
One-on-One Meetings	29
Database Surveillance	29

4.3	On-site Examinations	30
CHAPTER 5: CAPACITY BUILDING		
5.1	Training	35
5.2	Outside Assistance	36
5.3	The Advisory Board	36
CHAPTER 6: AWARENESS PROGRAMMES		
6.1	Reporting Institutions	37
6.2	Supervisory Authorities	38
6.3	Law Enforcement Agencies	38
CHAPTER 7: TYPOLOGY ANALYSIS AND CASE STUDIES		
7.1	Laundering Proceeds from Transshipment	40
7.2	Money Laundering through Legal Arrangements	42
7.3	Money Laundering through Shell Companies	43
CHAPTER 8: STRENGTHENING IT INFRASTRUCTURE		
8.1	LankaFIN	45
8.2	FIU-Sri Lanka Website	46
PHOTO GALLERY.....		50
APPENDIX A: LIST OF DIRECTIONS/GUIDELINES/RULES/CIRCULARS ISSUED FROM 2006 TO 2014		54
APPENDIX B: LIST OF REPORTING INSTITUTIONS AS AT 31 ST DECEMBER 2014		56
BOX ARTICLES		
BOX 1: VIRTUAL CURRENCIES AND RISK OF MONEY LAUNDERING		25
BOX 2: MOBILE MONEY SERVICES IN THE CONTEXT OF ML/TF		31
BOX 3: RECENT COMPLIANCE CHANGES IN ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM		47

LIST OF ACRONYMS

AGD	Attorney General's Department
AMCs	Authorized Money Changers
AML	Anti-Money Laundering
APGML	Asia Pacific Group on Money Laundering
AUSTRAC	Australian Transaction Reports and Analysis Centre (Australian FIU)
BSD	Bank Supervision Department
CBS	The Centre for Banking Studies
CBSL	Central Bank of Sri Lanka
CDD	Customer Due Diligence
CEOs	Chief Executive Officers
CFT	Countering the Financing of Terrorism
CID	Criminal Investigation Department
CSTFA	Convention on the Suppression of Terrorist Financing Act No. 25 of 2005
CTRs	Cash Transaction Reports
DNFBPs	Designated Non-Financial Businesses and Professions
DSNBFI	Department of Supervision of Non-Bank Financial Institutions
ECD	Exchange Control Department
ECDD	Enhanced Customer Due Diligence
EFTs	Electronic Fund Transfers
FATF	Financial Action Task Force
FD	Fixed Deposit
FDA	Financial Data Analysis
FIs	Financial Institutions
FIU	Financial Intelligence Unit
FTRA	The Financial Transactions Reporting Act No. 06 of 2006
IBSL	Insurance Board of Sri Lanka
ICs	Insurance Companies
ICT	Information and Communications Technology
IM	Intelligence Management
IMF-STI	The IMF - Singapore Regional Training Institute
ITD	Information Technology Department
JAFIC	Japan Financial Intelligence Centre
KYC	Know Your Customer
LankaFIN	FIU-Sri Lanka's Online Database Management System
LBs	Licensed Banks
LCBs	Licensed Commercial Banks
LCS	Legal and Corporate Service
LEAs	Law Enforcement Agencies



LFCs	Licensed Finance Companies
LKR	Sri Lanka Rupees
LSBs	Licensed Specialized Banks
LSIC	Lebanon Special Investigations Commission
MER	Mutual Evaluation Report
ML/TF	Money Laundering and Terrorist Financing
MNO	Mobile Network Operation
MOUs	Memorandums of Understanding
NDB	National Development Bank
NGOs	Non-Governmental Organizations
NPOs	Non-Profit Organizations
NRA	National Risk Assessment
OOS	On-site and Off-site Supervision
PDG	Policy Development Group
PEPs	Politically Exposed Persons
PMLA	Prevention of Money Laundering Act No. 05 of 2006
PNB	Police Narcotic Bureau
RBA	Risk-Based Approach
SAs	Supervisory Authorities
SBs	Stock Brokers
SCDD	Simplified Customer Due Diligence
SEC	Securities and Exchange Commission
SIS	State Intelligence Service
SPDIR	Strategic Policy Development & International Relations
SSL	Secure Sockets Layer
STF	Special Task Force
STRs	Suspicious Transaction Reports
TOR	The Onion Router
UNSC	United Nations Security Council

YEAR 2014 AT A GLANCE

Total No. of Reporting Institutions - 2014

Licensed Commercial Banks	25
Licensed Specialized Banks	9
Licensed Finance Companies	48
Insurance Companies	21
Stock Brokers	30
Authorized Money Changers	70
Total	203

Main Activities - 2014

	(In Numbers)
Cash Transaction Reports	2,960,957
Electronic Fund Transfers	2,635,021
Suspicious Transaction Reports (STRs)	904
STRs Reported	718
STRs Generated	186
STRs Referred	189
STRs Referred to Law Enforcement Agencies	183
STRs Referred to Regulatory Authorities	6
On-Site Examinations	4
Fines Imposed	-
MOUs Signed with Foreign FIUs	3
Training / Awareness Programmes	19



GOVERNOR'S MESSAGE



The Financial Intelligence Unit of Sri Lanka (FIU-Sri Lanka) was established in 2006 to act as a central authority to receive, process, analyze, and disseminate financial intelligence with a view of mitigating crimes related to Money Laundering (ML) and Terrorist Financing (TF).

The necessary legislative framework was established to combat ML and TF in the country with the enactment of the Convention on the Suppression of Terrorist Financing Act No. 25 of 2005 (CSTFA), the Prevention of Money Laundering Act No. 5 of 2006 (PMLA) and the Financial Transactions Reporting Act No. 6 of 2006 (FTRA). The FIU-Sri Lanka has been playing a vital role in the fulfillment of Sri Lanka's commitments to International Standards of Anti Money Laundering and Combating the Financing of Terrorism (AML/CFT) set out by the Financial Action Task Force (FATF).

The prevention of ML and combating of TF are challenging tasks which need constant coordination among all stakeholders. The FIU-Sri Lanka has developed a data management system to receive data and Suspicious Transaction Reports (STRs) electronically from reporting institutions. It is staffed with officers who have specialised in relevant fields such as law, accountancy, banking, finance and ICT. Their proficiency in the field of AML/CFT has been upgraded continuously through regular participation in local and international training programmes. Awareness programmes have been conducted for officers of reporting institutions and law enforcement agencies to enhance their expertise in detecting suspicious transactions linked to ML/TF.

During 2014, the FIU-Sri Lanka was involved in a mutual evaluation exercise by peer countries to ensure that Sri Lanka is in line with international best practices set out by the FATF, under the surveillance of the Asia Pacific Group on Money Laundering (APG). The financial sector is especially monitored and screened to maintain stability and to mitigate any involvement on criminal activities with the assistance of relevant regulatory authorities.

I am pleased to note the progress made by the FIU-Sri Lanka during 2014 and glad to say the Annual Report of the FIU-Sri Lanka is very informative and useful for all stakeholders.

I congratulate the Director and his staff of the FIU-Sri Lanka for their successful achievements in 2014.

Arjuna Mahendran
Governor
Central Bank of Sri Lanka

DIRECTOR'S MESSAGE



The FIU-Sri Lanka continued its operations amidst many challenges during the year 2014 in terms of the statutory provisions of the Financial Transactions Reporting Act No. 6 of 2006 (FTRA). The Annual Report 2014 of the FIU-Sri Lanka is presented highlighting achievements vis-a-vis challenges during the year including developments in Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) legislative and policy framework and operational aspects of the FIU-Sri Lanka, stakeholder co-operation and international arrangements.

Licensed Commercial Banks (LCBs), Licensed Specialized Banks (LSBs), Licensed Finance Companies (LFCs), Stock Brokers (SBs) and Insurance Companies (ICs) continued to report to the FIU-Sri Lanka on cash transactions and electronic funds transfers (both local and foreign) of LKR 1.0 Mn and above or its equivalent in foreign currencies through the FIU-Sri Lanka's on-line database management system, "LankaFIN". Over 5.5 Mn of cash/fund transfers and 718 Suspicious Transactions were reported by the above reporting institutions while, LankaFIN system also generated 186 Suspicious Transactions Report (STRs) during the year 2014. A total of 189 STRs was referred to the law enforcement and regulatory authorities for further investigations during the year.

As a mechanism to facilitate sharing of information and intelligence for the purpose of investigation and prosecution of suspicious transactions, the FIU-Sri Lanka has signed three Memorandums of Understanding (MOUs) with General Directorate of Prevention of Money Laundering of the Republic of Albania, Financial Intelligence Unit of the Republic of Peru and the Financial Intelligence Unit of the Republic of Union of Myanmar. Accordingly, the total number of MOUs signed as at the end of 2014 stood at 27 covering different parts of the globe.

In continuing efforts to enhance awareness on detecting, analyzing and reporting of transactions relating to Money Laundering and Terrorist Financing (ML/TF), 19 awareness/training programmes were conducted during the year, accommodating more than 1,100 participants from various sectors/stakeholders of the economy. Further, the FIU-Sri Lanka also conducted special awareness programmes for judges of the Court of Appeal and High Court.

The FIU-Sri Lanka has obtained assistance from members of the Egmont Group (Association of the FIUs) to carry out investigations and collaborated with the member countries to gather intelligence on their investigations. During the year, The FIU-Sri Lanka conducted 4 on-site examinations covering the banking and finance companies sectors to assess compliance with the provisions of FTRA and rules and directions issued by the FIU-Sri Lanka.

Further, the year 2014 was an important year for the FIU-Sri Lanka due to two main reasons, i.e. completion of the country's first ever National Risk Assessment (NRA) on ML/TF and the conduct of the country's Second Mutual Evaluation by Asia Pacific Group (APG) on Money Laundering.

Sri Lanka's NRA was a nationwide activity carried out aiming at better understanding the ML/TF risks faced by the country. The FIU-Sri Lanka, as the AML/CFT regulator in the country took the lead role in the conduct of the NRA with technical assistance from the World Bank. More than eighty officers

representing key government and private sector institutions participated in the NRA Process. The final report with key recommendations was distributed among all AML/CFT stakeholders with the approval of the Advisory Board for the FIU-Sri Lanka in order to create a universal understanding on the country's level of ML/TF risk. As the primary agency involved in the NRA process, the FIU-Sri Lanka is expected to follow-up closely the effective implementation of the recommended actions.

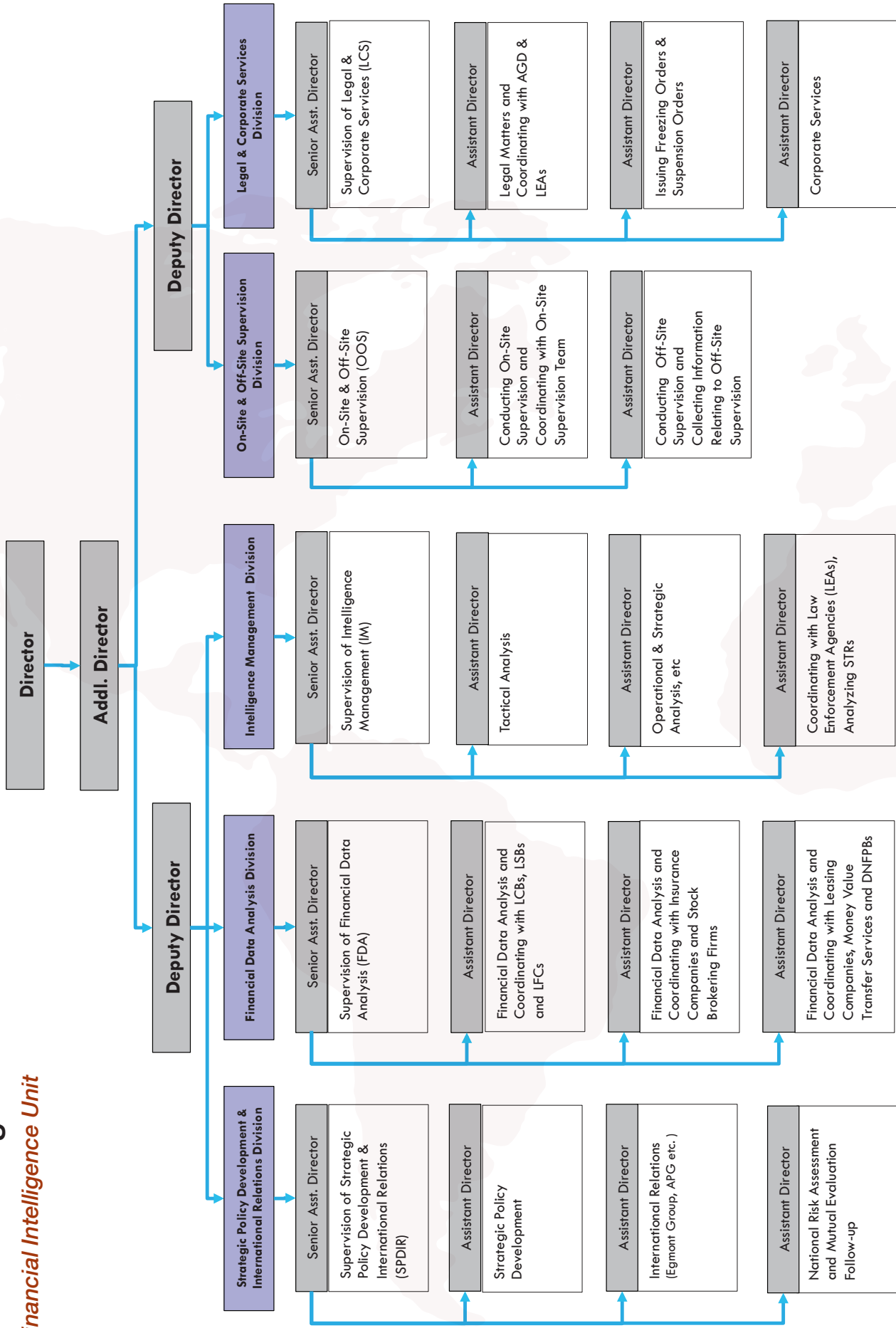
As a founding member of the APG, Sri Lanka was subjected to its first Mutual Evaluation by the APG in 2006. The second Mutual Evaluation on Sri Lanka had been continued throughout the year by an evaluation team consisting of members from Australia, Singapore, India, Malaysia, Hong Kong, Bhutan and APG Secretariat. The Mutual Evaluation focuses on Sri Lanka's level of technical compliance with FATF 40 Recommendations and the level of effectiveness in AML/CFT system and provides recommendations to strengthen the AML/CFT system. The evaluation team visited Sri Lanka during December 1-12, 2014 and May 18-22, 2015 and held discussions with various public and private sector stakeholders. The final report is expected to be adopted at the APG Plenary to be held in Auckland, New Zealand in July 2015.

With the conclusion of NRA and Mutual Evaluation, the year 2015 onwards would be more challenging for the FIU-Sri Lanka as it is necessary to ensure that the actions recommended in the NRA and Mutual Evaluation Report are implemented in order to achieve compliance status for the country on AML/CFT.

H Amarathunga
Director
Financial Intelligence Unit of Sri Lanka

Functional Organizational Chart

Financial Intelligence Unit





FIU - Sri Lanka Staff

VISION

To be the trusted and respected single agency with commitment to excellence in establishing the framework for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) in Sri Lanka.

MISSION

To administer effectively, the provisions of the Financial Transactions Reporting Act (FTRA), No.6 of 2006 by facilitating the prevention, detection, investigation and prosecution of the offences related to Money Laundering and Terrorist Financing (ML/TF).

STRATEGIC GOALS

Implement the provisions of the FTRA, No. 6 of 2006 relating to prevention, detection, investigation and prosecution of ML/TF activities.

Strengthen the AML/CFT regime in line with the revised Financial Actions Task Force (FATF) recommendations.

Complete the Second Mutual Evaluation on Sri Lanka.

Promote international co-operation on AML/CFT in line with international standards/conventions.

The FIU-Sri Lanka is the national centre for receipt and analysis of Suspicious Transaction Reports (STRs) and other threshold based disclosures/declarations relevant to Money Laundering (ML), associated predicate offences and Terrorist Financing (TF) from the relevant institutions, and the timely dissemination of the results of analysis of STRs to relevant law enforcement and supervisory authorities for effective actions.

2.1 Collection of Information

Licensed Banks (LBs), Licensed Finance Companies (LFCs), Stock Brokers (SBs), Insurance Companies (ICs) and Authorized Money Changers (AMCs) engaged in finance businesses are mandated to report to the FIU-Sri Lanka. In addition, the FIU-Sri Lanka also receives information relating to ML/TF from Law Enforcement Agencies (LEAs), Supervisory Authorities (SAs) and the general public.

As prescribed by the The Financial Transactions Reporting Act (FTRA) No. 6 of 2006, the following mandatory reports are required to be sent to the FIU-Sri Lanka by the relevant institutions.

1. Cash Transaction Reports (CTRs)
2. Electronic Fund Transfers (EFTs)
3. Suspicious Transaction Reports (STRs)

Cash Transactions and Electronic Fund Transfers

In terms of Section 6 of the FTRA, every Institution is required to report any cash transaction and any electronic fund transfer exceeding such sum as prescribed by the Minister of Finance by Order published in the Gazette or its equivalent in any foreign currency. Accordingly, the present applicable reporting threshold of LKR 1.0 Mn has been prescribed by the Minister of Finance in the Extraordinary Gazette No 1555/9 dated 25th June 2008.

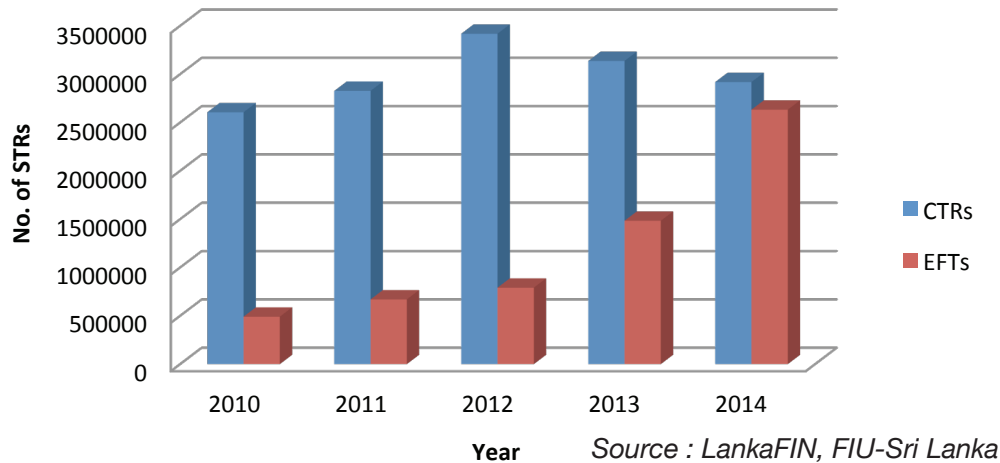
At present LBs, LFCs, SBs, ICs and AMCs submit CTRs and EFTs electronically through the LankaFIN secured network introduced by the FIU-Sri Lanka.

Table 2.1 :- Receipt of CTRs & EFTs through LankaFIN

	2010	2011	2012	2013	2014
CTRs	2,668,920	3,182,254	3,420,819	3,139,919	2,960,957
EFTs	491,512	698,659	796,836	1,483,445	2,635,021
Total	3,160,432	3,880,913	4,217,655	4,623,364	5,595,978

Source : LankaFIN, FIU-Sri Lanka

Figure 2.1
Receipt of CTRs & EFTs through LankaFIN



The total number of transactions reported on CTRs and EFTs has increased to 5,595,978 in 2014 from 4,623,364 in 2013. The EFTs have shown a considerable increase in 2014 compared to EFTs in 2013. The increase of CTRs and EFTs may have resulted from the increase in economic activities in the country.

Suspicious Transaction Reports (STRs)

If an Institution has reasonable grounds to suspect that any transaction or attempted transaction may be related to a commission of any unlawful activity or any other criminal offence, it should file an STR with the FIU-Sri Lanka. In terms of Section 7 of the FTRA, LBs, LFCs, SBs, and ICs submit STRs electronically through LankaFIN.

In terms of the Section 5 of the Prevention of Money Laundering Act (PMLA) No. 05 of 2006, any person who knows or has reason to believe from information or other matter obtained by him in the course of any trade, profession, business or employment carried on by such person, that any property has been derived or realized from any unlawful activity, shall disclose his knowledge or belief as soon as is practicable to the FIU-Sri Lanka.

At present LEAs, supervisory authorities as well as the general public submit STRs under the above provisions.

Table 2.2: STRs Reported by Stakeholders

	2010	2011	2012	2013	2014
Reporting Institutions	87	91	144	272	452
Law Enforcement Agencies & Regulators	156	91	56	88	247
Public Complaints	3	3	3	6	19
Total	246	185	203	366	718

Source : LankaFIN, FIU-Sri Lanka

According to table 2.2, total STRs reported to the FIU-Sri Lanka has also shown a significant increase of 96 percent to 718 in 2014 compared to 366 STRs reported in 2013. The STRs reported by reporting institutions show an increase of 66 percent and STRs reported by law enforcement & regulators show an increase of 180 percent compared to corresponding figures in 2013. Public complaints received by the FIU-Sri Lanka has increased to 19 in 2014 from 6 in 2013.

Figure 2.2
No. of STRs by Customer Type

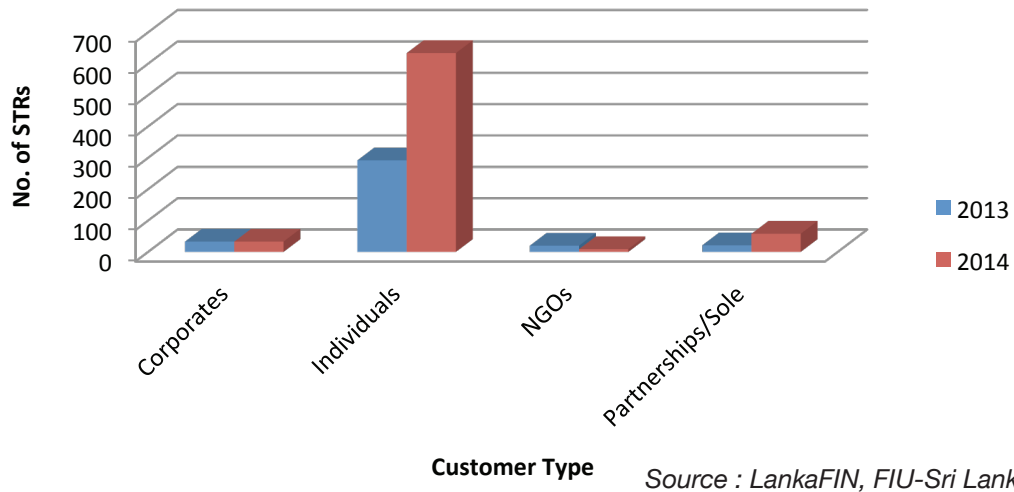
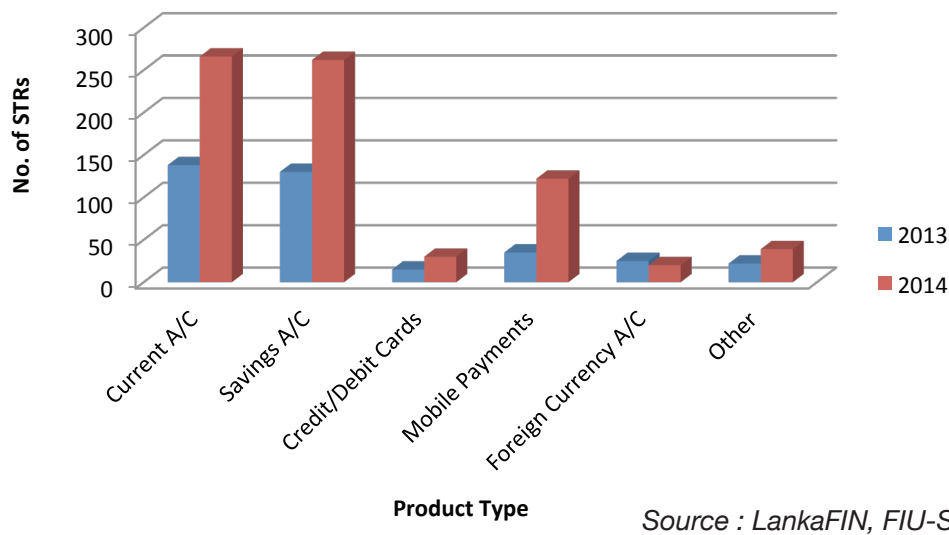


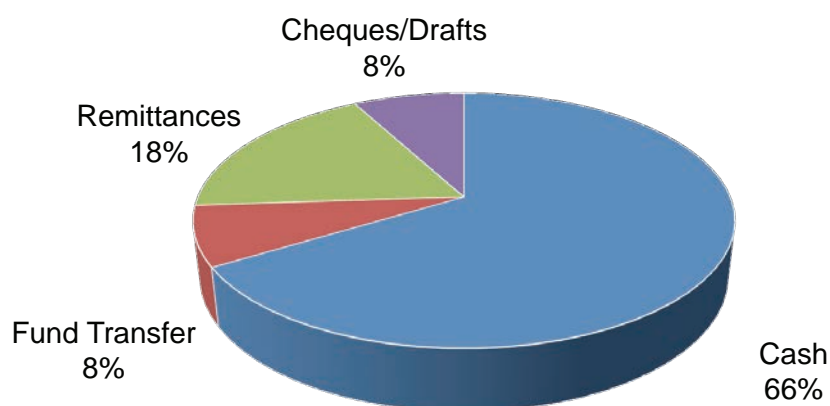
Figure 2.2 shows that the STRs on financial transactions carried out by individuals continued to be the major component of STRs reported during 2014 as well. The STRs reported on corporates, NGOs/societies and partnerships/sole proprietorships remain low.

Figure 2.3
STRs by Product Type



As shown in figure 2.3, the majority of suspicious transactions reported relate to transactions carried out through current and savings accounts. Use of mobile payment systems to carry out suspicious transactions has increased considerably during 2014. The other types of products included, suspicious transactions related to fixed deposits, pay orders, life insurance and share transactions.

Figure 2.4
STRs by Mode of Transaction



Source : LankaFIN, FIU-Sri Lanka

Figure 2.4 shows that the majority of STRs were related to transactions carried out through cash deposits and withdrawals.

Further, STRs have been reported based on various suspicions regarding drug dealing, frauds, exchange control violations, TF, tax evasion, forgery, payment device frauds and pyramid schemes. The STRs reported by mobile service providers also continue to grow and these STRs are mostly related to collection of funds from public promising various gifts, and forged lotteries and also to drug peddling to a certain extent.

2.2 Analysis of Information

Analysis of information collected/received from the reporting institutions has been a major activity of the FIU-Sri Lanka.

The analysis on CTRs and EFTs reported is carried out through an alert generating process to identify suspicious transactions. These alerts are generated by the system automatically subject to the fulfillment of certain parameters which have been designed on the basis of ML/TF typologies identified in Sri Lanka as well as other intelligence agencies over a period of time. A periodical review and updating of the parameters is carried out to ensure the accuracy and relevancy of alerts generated. A customer or an account in the database would be subjected to an extra scrutiny on the basis of the number of alerts generated relevant to a particular customer or account. Table 2.3 shows the number of alerts and STRs generated through the LankaFIN system.

Table 2.3: STRs Generated through LankaFIN

	2010	2011	2012	2013	2014
Alerts Generated	825,845	879,859	1,046,134	1,230,351	2,744,693
STRs Generated	394	354	356	132	186

Source : LankaFIN, FIU-Sri Lanka

Preliminary analysis on the STRs received is carried out with use of the information available at LankaFIN database initially and further information from other sources such as reporting institutions, regulatory/supervisory agencies and other relevant government agencies would be called for, in order to conduct an in-depth analysis of each STR. Assistance from counterpart FIUs is also sought in analyzing STRs depending on the situation. Based on the results of the preliminary analysis, STRs are disseminated to relevant law enforcement or regulatory authorities.

According to table 2.4, the number of STRs relating to TF increased from 23 to 58, and STRs relating to ML increased from 475 to 846 from 2013 to 2014. Since 2009, with the conclusion of the internal conflict of the country, STRs relating to TF has not been significant. The STRs relating to ML are mostly connected specifically to drug dealing, frauds, cheating etc.

Table 2.4: Composition of STRs

	2010	2011	2012	2013	2014
STRs on TF	90	72	89	23	58
STRs on ML	534	467	470	475	846
Total	624	539	559	498	904

Source : LankaFIN, FIU-Sri Lanka

2.3 Dissemination of Information

After the preliminary investigations, STRs and related information are disseminated to relevant LEAs and supervisory agencies for further investigations or regulatory actions. The decision to disseminate is taken by a special committee (STR Review Committee) headed by the Director, FIU-Sri Lanka and represented by two senior officials from the Attorney General's Department (AGD) and relevant officers of the FIU-Sri Lanka based on the findings of the preliminary investigations.

Table 2.5: Dissemination of Information

	2010	2011	2012	2013	2014
Law Enforcement Agencies	21	60	48	55	183
Regulatory Agencies	13	5	8	18	6

Source : FIU-Sri Lanka

The majority of STRs referred to LEAs were on frauds and drug dealings. Further, STRs relating to suspected scams have also been referred for investigations. The STRs referred to regulatory agencies were on suspected pyramid schemes/ other illegal activities carried out violating Section 83 C of the Banking Act No. 30 of 1988 and the Exchange Control regulations.

The FIU-Sri Lanka shares information with foreign counterparts by entering into Memorandums of Understanding (MOUs) or through Egmont membership. The information shared in this manner is used only for intelligence purposes.

Table 2.6: Exchange of Information with Foreign FIUs

	2010	2011	2012	2013	2014
Information Requests Received	21	25	11	18	10
Information Requests Made	13	4	12	2	8

Source: FIU-Sri Lanka

During 2014, the FIU-Sri Lanka received requests from the FIUs of India, Belgium, Jersey and United Kingdom to share information on suspected ML/TF cases. The FIU-Sri Lanka responded to such requests without any delay. These requests were mostly related to transactions conducted by Sri Lankan citizens living abroad.

2.4 Suspension, Confiscation and Prosecution Relating to ML/TF

As prescribed in the Section 15(2) of the FTRA, the FIU-Sri Lanka is authorized to suspend the funds relating to unlawful activities to facilitate further investigations. Accordingly, the FIU-Sri Lanka has suspended funds amounting to LKR 63.00 Mn during the year. Funds suspended were mainly related to the drug trafficking offences.

Table 2.7: Suspension, Confiscation & Prosecution

	2010	2011	2012	2013	2014
Funds Suspended (LKR Mn)	181.70	107.50	1,800.00	-	63.00
Funds Confiscated (LKR Mn)	-	-	13.80	7.00	-
Prosecutions (No. of cases)	4	1	4	-	-

Source : FIU-Sri Lanka

During 2014, financial assets with a total value of LKR 914,189.27 were frozen under the United Nations Regulation No. 1 of 2012, which has been promulgated to implement United Nations Security Council Resolution (UNSCR) 1373 on TF.

Sharing of information on financial intelligence among competent authorities both domestically and internationally continued during the year 2014, facilitating the investigation and prosecution of persons suspected of committing and participating in ML/TF. The FIUs, government agencies and other stakeholders would be mutually benefitted through this process, in combating ML/TF.

3.1 Domestic Co-operation

Law Enforcement Agencies (LEAs)

The FIU-Sri Lanka maintained a close relationship with LEAs in Sri Lanka such as Criminal Investigation Department (CID), State Intelligence Service (SIS), Police Narcotic Bureau (PNB), Special Task Force (STF), and Commission to Investigate Allegations of Bribery or Corruption. Timely dissemination of financial intelligence is an important legal requirement of the FIU-Sri Lanka with a view to combat ML/TF of the country in a proactive manner.

Table 3.1: STRs Referred to LEAs by ML and TF

Year	2008	2009	2010	2011	2012	2013	2014
On ML	13	7	14	47	44	55	153
On TF	12	8	17	13	4	0	30
Total	25	15	31	60	48	55	183

Source : FIU - Sri Lanka

Supervisory Authorities

The supervisory authorities for financial institutions are the Bank Supervision Department (BSD), the Department of Supervision of Non-Bank Financial Institutions (DSNBFIs), the Exchange Control Department (ECD), the National Secretariat for Non Governmental Organisation, the Insurance Board of Sri Lanka (IBSL), and the Securities and Exchange Commission (SEC). During the year 2014, the FIU-Sri Lanka referred 6 STRs to supervisory authorities for further investigation.

Co-operation on National Risk Assessment (NRA)

NRA on ML/TF is a comprehensive process of identifying and analyzing the main sources and drivers of the ML/TF risk of the country. The purpose of NRA is to develop risk-based AML/CFT actions and to facilitate the allocation of available resources in the most effective way to control, mitigate and eliminate the identified risks.



The First Workshop of NRA on February 10, 2014

Recommendation 1 of the Financial Action Task Force (FATF) requires countries to identify, assess and understand the ML/TF risk and to apply a Risk-Based Approach (RBA) to ensure that the measures to prevent/ mitigate ML/TF risks are commensurate with the risks identified.

Sri Lanka's NRA is a government wide activity carried out with the aim of better understanding the ML/TF risks faced by the country. It is a self-assessment conducted by Sri Lankan authorities, using the National ML and TF Risk Assessment Tools developed and provided by the World Bank. The NRA process was carried out over a period of nine months from February to October 2014.

The FIU-Sri Lanka, as the AML/CFT Regulator in the country took the lead role in coordinating the NRA. Around 80 representatives from key government and private sector stakeholders participated in the process. The NRA was conducted under the ambit of the Advisory Board for the FIU-Sri Lanka which comprises of senior government officials chaired by the Governor, Central Bank of Sri Lanka (CBSL).

The specific objectives of the NRA were to:

- a) Understand the level of proceeds of crime generated in or coming into the country and the threat posed by TF;
- b) Determine how vulnerable the financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) are to ML/TF;
- c) Determine and understand the weakness in the legal framework, by considering the criminal and administrative justice system, and existing preventive systems; and
- d) Observe the most efficient way in which to allocate resources for the prevention, investigation and prosecution of ML/TF.

The World Bank model defines the ML risk as a combination of national ML threat and national vulnerability which consist of 8 modules.

The national threat module focuses on understanding the proceeds of crimes in the country. The national vulnerability consists of two parts; overall sectoral vulnerability and national combating ability. In the sectoral vulnerability, the financial sector as well as the DNFBPs in Sri Lanka were assessed. A number of input variables relating to these sectors are evaluated as main drivers of national combating ability. In addition to the ML risk assessment modules, the tool contains a separate TF risk assessment module.

Sri Lanka's NRA also included a module on Financial Inclusion Product Risk Assessment. This module aims to assist authorities in evaluating ML/TF risks arising from both existing and emerging/new financial inclusion products. It can also be used by regulators to design financial products with low or lower ML/TF risk. This module is different from other modules and benefits from the output of NRA rather than feeding into it.

All the AML/CFT stakeholders involved with the assessment process were grouped according to their area of expertise in 8 working groups as required by the WB Assessment Methodology to undertake the NRA.

The NRA process involved three stages; the first stage included a three day workshop, conducted during February 10-12, 2014 to discuss the NRA concepts to introduce NRA tools, the assessment methodology and the use of the NRA tools. The groups used information collected before-hand to populate the NRA tool, and to identify information gaps.



Inaugural Session of Final Workshop of NRA

including conduct of a discussion on the recommendations of the NRA, and a possible way forward.

After the conclusion of the NRA process, a sanitized version of the NRA report that included the recommendations made by the NRA Working Groups were disseminated to relevant stakeholders.

The overall threat and vulnerability of Sri Lanka has been assessed as medium in the NRA. Accordingly, the ML risk level of the country has been rated as medium.

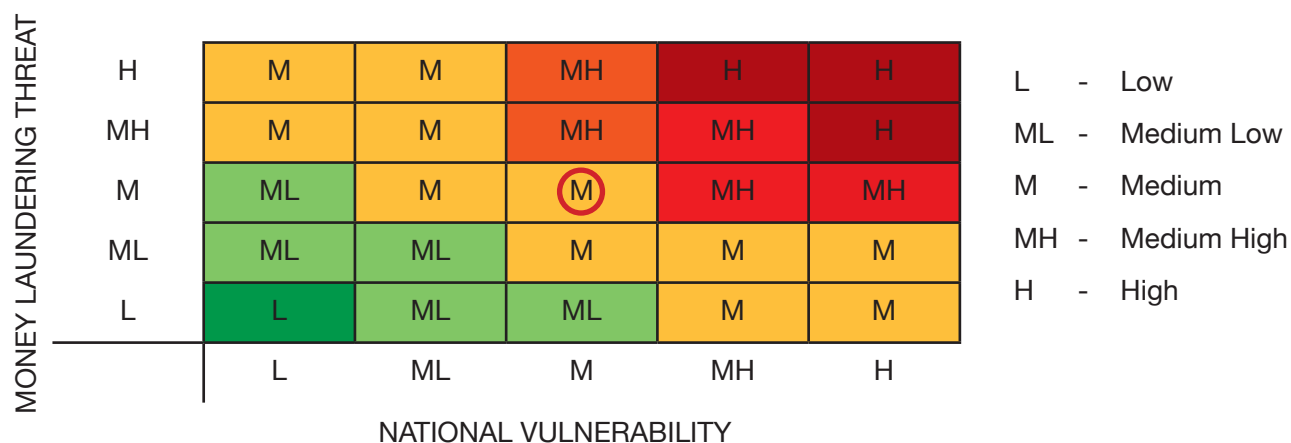
The second stage required the working group members to collect any missing data from relevant institutions and re-evaluate the inputs made during the initial workshop and populate missing data as identified at the initial workshop, and draft respective initial group reports. All groups were given time until May 15, 2014 to submit their group reports to the FIU-Sri Lanka.

The final stage of the NRA process included a two-day workshop which was held in October 2014. This workshop provided a venue for a final review of the NRA report,



Working Groups of Final Workshop of NRA

OVERALL MONEY LAUNDERING RISK OF THE COUNTRY



3.2 International Co-operation

Memorandums of Understanding (MOUs)

In terms of the provisions made under Section 17 of the FTRA, the FIU-Sri Lanka is empowered to enter into MOUs with counterpart FIUs on the approval of the Minister of Finance, to exchange information relating to ML/TF issues. Accordingly, the FIU-Sri Lanka signed 3 MOUs with the following FIUs during the year 2014.

1. General Directorate of Prevention of ML of the Republic of Albania
2. Financial Intelligence Unit of the Republic of Peru
3. Financial Intelligence Unit of the Republic of Union of Myanmar

The total number of MOUs signed by the FIU-Sri Lanka with other counterparts increased to 27 as at the end of 2014.

Table 3.2: MOUs Signed with Counterpart FIUs from 2008 to 2014

Name of Counterpart FIU	Date of Signing
Financial Intelligence Unit of Bank Negara Malaysia	18 January 2008
Financial Intelligence Unit of the Da Afghanistan Bank	29 February 2008
Korean Financial Intelligence Unit	18 December 2008
Indonesian Financial Transaction Reports and Analysis Centre	27 May 2009
Financial Information Unit of Nepal Rastra Bank	09 July 2009
The Anti-Money Laundering Council of Philippines	09 July 2009
Cambodian Financial Intelligence Unit of National Bank of Cambodia	26 October 2009
Financial Intelligence Unit of India	30 March 2010

Australian Financial Transactions and Analysis Centre	07 May 2010
Financial Intelligence Unit of Belgium	18 June 2010
Financial Intelligence Unit of Solomon Islands	15 July 2010
Financial Intelligence Unit of Bangladesh	28 October 2010
Financial Intelligence Centre of South Africa	02 December 2010
Fiji Financial Intelligence Unit	21 July 2011
Financial Intelligence Unit of Slovenia	09 August 2011
Transaction Reports and Reports Analysis Centre of Canada	02 August 2011
Financial Crime Enforcement Network (FinCEN)-USA	10 July 2012
The Financial Information Unit of the Bank of Mongolia	11 July 2012
Federal Financial Monitoring Service (Russian Federation)	11 July 2012
Saudi Arabian Financial Investigation Unit (SAFIU)	11 July 2012
Japan Financial Intelligence Centre (JAFIC)	11 March 2013
Lebanon Special Investigations Commission (LSIC)	03 July 2013
Financial Intelligence Unit of Costa Rica	08 July 2013
Financial Intelligence Unit of Denmark	30 September 2013
General Directorate of Prevention of Money Laundering of the Republic of Albania	05 June 2014
Financial Intelligence Unit of the Republic of Peru	05 June 2014
Financial Intelligence Unit of the Republic of Union of Myanmar	17 July 2014

Source : FIU - Sri Lanka

Asia/Pacific Group on Money Laundering

As a founder member of APG, the FIU-Sri Lanka officials represented Sri Lanka at the 17th Annual Meeting of APG held in Macao SAR, China in July 2014 and the 17th Annual Typologies and Technical Seminar held in Thailand in November 2014.



Opening Session of On-site Mutual Evaluation

As part of Sri Lanka's MER process, the assessment team consisting of eight members visited Sri Lanka during 01-12 December 2014 to conduct an on-site evaluation of the AML/CFT measures of the country. This evaluation focuses on the level of compliance of Sri Lanka's AML/CFT system with the FATF 40 Recommendations and 11 Immediate Outcomes. Final report on Mutual Evaluation will be adopted at the APG plenary to be held in New Zealand in July 13-17, 2015.



17th Annual Meeting of APG Held in Macao SAR, China

Egmont Group

The FIU-Sri Lanka obtained assistance from members of the Egmont Group, the association of the FIUs consisting of 139 member FIUs (as at December 31, 2014) globally to carry out investigations and collaborated with the member countries to gather evidence on their investigations. The total number of exchange of information shared by the FIU-Sri Lanka with other Egmont members during 2014 stood at 18.



At Mutual Evaluation Exit Meeting

BOX 1: VIRTUAL CURRENCIES AND RISK OF MONEY LAUNDERING

'What is currency?', the question is simply answered as something of value. In early days, currency took various material forms from cattle to cowrie shells and has changed considerably to today's electronic currency. In recent years, there has been an increasing focus on virtual currencies in view of their rapid development. Therefore, it is vital to have an understanding of the nature of virtual currencies.

A virtual currency is a digital representation of value that can be traded on the internet and functions as;

- (1) A medium of exchange;
- (2) A unit of account; and/or
- (3) A store of value, but does not have legal tender status in any jurisdiction.

It is crucial to understand the difference between the fiat currency (also referred to as "real" currency) versus virtual currency. Fiat currency is the coin and paper money of a country that is designated as legal tender by the country, circulated and is customarily used and accepted as a medium of exchange in the country of issuance. Virtual currency is a medium of exchange that operates like a currency in some environments (i.e., it functions as a medium of exchange; a unit of account to measure value and costs of goods, services, assets and liabilities; and/or a store of value) but usually, does not have a legal tender status.

Not all virtual currencies are of same characteristics. There are three basic categories of them as closed flow, open flow and hybrid flow virtual currencies.

Closed flow virtual currencies cannot be directly purchased with real currency and can only be used to purchase virtual goods and services. This means that, it can only be obtained through actions in a video game or virtual world, and can only be redeemed within that video game or virtual world. Closed flow virtual currencies are isolated from the real economy and therefore, it does not pose ML or TF risks.

Open flow virtual currencies can be directly purchased with, or sold for, real currency as well as to buy or sell real and/or virtual goods and services. This is the most common and versatile type of virtual currency mostly at risk for ML/TF because they can be bought and sold for real currency. Open-flow virtual currencies can be bought or sold for real currency, and can be exchanged for real and/or virtual goods and services.

Eg: Bitcoin: This is the most prominent example of an open-flow virtual currency. Bitcoins are mathematical tokens composed of unique strings of numbers and letters that constitute units of the currency and have value only because the Bitcoin community collectively decides the value of Bitcoin. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into any fiat or virtual currencies.

Open flow virtual currencies can also be divided into two types based on the controlling authority. In **centralized virtual currencies**, a single administrative authority (trusted third party) controls the system. It would issue currency, establish rules and maintain a central payments ledger. The exchange rate of the virtual currency with the fiat currency is determined either through the demand and supply of the virtual currency or a fixed rate.

Eg: Liberty Reserve: was a Costa Rica-based centralized digital currency service. The site had over one million users when it was shut down by the United States government, due to lack of security and increased criminal activities.

Decentralized virtual currencies do not have a central administrative authority to issue or control the behavior of the currency. The money supply of the currency is predetermined by a mathematical algorithm. New Units are typically created through a process called “Mining”.

Eg: Bitcoin and Litecoin are decentralized virtual currencies. No single authority controls the currency. Their money supplies are determined by an algorithm and users collectively verify that transactions are legitimate.

Hybrid flow virtual currencies can be directly purchased with real currency and used to acquire real goods or services, but can't be readily sold for real currency. Further, it may be used to acquire virtual goods or services, but this is not a requirement. As this type of currency can be bought using real currency and exchanged for real or virtual goods or services, these are subjected to ML or TF risks. However, the risk is partially mitigated by the inability to convert back to real currency.

Eg: Frequent flyer miles - Frequent flyer miles could be considered hybrid virtual currencies. Miles can often be purchased with real currency, exchanged between individuals for a fee, and redeemed for real goods and services but not for real currency.

How it operates?

There are four participants in a virtual currency system namely Exchanger, Administrator, User and The Onion Router (TOR).

An Exchanger is a person/entity who is engaged in the business of exchanging virtual currency for real currency or any other virtual currency. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts. They usually accept a wide array of payments like cash; wire transfers, credit cards etc.

An Administrator is a person/entity engaged in issuing virtual currencies as a business and who has the authority to withdraw them from the circulation. Administrators usually issue rules on their virtual currencies. However, not all virtual currencies have administrators. Eg: Decentralized virtual currencies such as Bitcoin.

A User is a person/entity who obtains virtual currencies and uses it to purchase real or virtual goods and services. In general, there are two ways a user can purchase virtual currencies, i.e. through exchangers or through informal ways (such as private purchase in exchange for goods or money, through eBay or advertised in web forums).

The Onion Router (TOR) is an underground distributed network of computers on the Internet that conceals true IP addresses and therefore hides identities of the network's users, by routing transactions through multiple computers around the world. The TOR makes it very difficult to physically locate computers hosting or accessing websites on the network.

In order to understand how these virtual currencies work in reality, below is a simple briefing of how Bitcoins are performed in the virtual world.

Acquiring Bitcoins: A new user needs to choose a wallet that she/he installs in the computer or mobile phone. Wallets are available for free on bitcoin.org (normal internet) or applications for mobiles. Once this wallet is installed, it will generate his/her Bitcoin address.

Placement: Cash is to be deposited by the user to Bitcoin exchange's bank account. Within four hours of deposit, the exchange emails Bitcoins to the Bitcoin wallet.

Transferring Bitcoins to another Person: These Bitcoins can then be sent to any other user in the world who has a Bitcoin wallet. Transfer is by a simple email from one Bitcoin wallet to the other person's Bitcoin wallet. Transfer is instantaneous, with no fees and is anonymous.

To encash Bitcoins: A person who wants to encash bitcoins may visit any Bitcoin exchange website and has to enter the number of Bitcoins he wishes to sell. The exchange will have the Bitcoin purchase price advertised. Then, he has to confirm the order with the email address and bank account details. Once the order is confirmed, the exchange will provide their unique Bitcoin wallet address. Bitcoins to be sold need to be transferred to the unique wallet address which was provided in the order confirmation. Then funds will be transferred to the nominated bank account.

Advantages and downsides of using virtual currencies

Virtual currencies have relatively lower transaction fees. Therefore, they are cheaper to use as a payment mode than other online payment methods such as credit cards. It is a more cost effective method for cross border transactions because using virtual currency is cheaper compared to the traditional methods. Most importantly, it is a vehicle for innovation with rapid developments.

However, the downsides of using virtual currencies are also noteworthy. Virtual currencies can be easily used for illicit transactions such as drug related transactions. Further, it may also be difficult for consumers to understand the virtual currency phenomenon. On the contrary, payment methods such as credit cards and debit cards are easier to understand and use.

Similar to all other payment methods, virtual currencies also possess ML risk. The foremost motive for this is its anonymity. Decentralized systems such as Bitcoins afford anonymous transactions. Even centralized systems may not be adequately regulated and therefore may be complicit in ML. Further, they can be used globally to conduct domestic and cross-border transfers in various denominations and therefore perform as an alternative to formal banking system/fiat currency to circumvent AML/CFT requirements.

In mitigating the ML risk arising from virtual currencies, countries should first identify its level of using virtual currencies, the potential growth and ways to regulate the industry. In this attempt, FATF which was established to set standards and promote effective implementation of legal, regulatory and operational measures for combating ML and TF, revised its recommendations in 2012. Among the forty recommendations, Recommendation 15 emphasizes a RBA with regard to new developments such as virtual currencies:

Accordingly, countries and financial institutions must identify and assess ML/TF risks relating to the development of new products and business practices (including new delivery mechanisms) and the use of new or developing technologies for both new and existing products. The FIs should take appropriate measure to manage and mitigate risk before launching new products, business practices, or use of new technologies for new or existing products.

Furthermore in the current context, the FATF Policy Development Group (PDG) has issued draft guidance for a RBA to virtual currencies which is to be approved in June 2015. The overall aim of the guidance is to strive for a consistent global approach by setting some common principles (i.e. entities which should fall within the scope of the FATF Recommendations), but providing some flexibility in the way in which countries apply AML/CFT requirements to these entities based on what makes sense for each jurisdiction's existing legal framework (i.e. by designating virtual currency exchangers as financial institutions or DNFBPs).

References

APG/EAG Capacity Building Seminar (2013) *Understanding the nature of virtual currencies and how they work*. Blue Sky Hotel and Tower, Mongolia. 26 September 2013. Joint APG/EAG Capacity Building Workshop 2013

Bitcoin Project 2009-2015 Released under the MIT license (2014) Bitcoin [online]. Available from: <https://bitcoin.org/en>. [Accessed: 07 January 2014]

David Carp (2013) *What is Virtual Currency and how it works*. Blue Sky Hotel and Tower, Mongolia. 26 September 2013. Joint APG/EAG Capacity Building Workshop 2013

Financial Action Task force. (2013) *The FATF Recommendations February 2012*. France: FATF Secretariat

Financial Action Task force. (2014) *Discussion Paper on Virtual Currencies*. OECD Conference Centre. France: FATF Secretariat

Financial Action Task force. (2015) *Guidance for a Risk-Based Approach; Virtual Currencies*. France. FATF Secretariat

United States of America. Government Accountability Office (2013) *Guidance on Taxation of Virtual Economies and Currencies*. United States of America: Government accountability Office

Wallwork A.S (2013) *Taxonomy of Virtual Currencies*. Blue Sky Hotel and Tower, Mongolia. 26 September 2013. Joint APG/EAG Capacity Building Workshop 2013

Wikipedia (2014) *Bitcoin* [online] Available from: <https://en.wikipedia.org/wiki/bitcoin>. [Accessed: 07 January 2014]

Wikipedia (2014) *Liberty reserve* [online]. Available from: https://en.wikipedia.org/wiki/liberty_reserve. [Accessed: 07 January 2014]

4.1 Ensuring Compliance of Reporting Institutions

As key stakeholders, reporting institutions play a major role in effective implementation of AML/CFT measures in the country. In terms of the FTRA, the legal requirement of a reporting institution is to ensure that the preventive and detective measures are in place to protect the financial system from money launderers and terrorist financiers. The FTRA provisions enable the FIU-Sri Lanka to ensure compliance of reporting institutions through on-site and off-site surveillance. Further, the FIU-Sri Lanka has also been empowered by the FTRA to impose penalties for any reporting institution for breach of laws and regulations issued in this regard.

4.2 Off-site Surveillance

Under off-site surveillance, one-on-one meetings with stakeholders are conducted. In addition, surveillance is conducted to ensure compliance through online reporting of data and information.

One-on-One Meetings

One-on-one meetings are held periodically with compliance officers of the reporting institutions to review and discuss the progress achieved and problems encountered by them in ensuring respective institution's compliance with AML/CFT measures. Table 4.1 shows the one-on-one meetings held with reporting institutions during 2012 - 2014.

Table 4.1: One-on-one Meetings with Reporting Institutions

Sector	2012	2013	2014
Banks	11	13	4
Financial Companies	5	2	-
Insurance Companies	1	1	-
Stock Brokers	3	-	1
Total	20	16	5

Source: FIU-Sri Lanka

Database Surveillance

All reporting institutions are required to submit fortnightly/monthly reports to the FIU-Sri Lanka electronically using the online data submission system, 'LankaFIN'. The Financial Data Analysis Division of the FIU-Sri Lanka continuously monitors the reporting institutions' compliance on the submission of accurate and complete data.

Meanwhile, senior officials of the FIU-Sri Lanka participate in monthly meetings of Chief Executive Officers (CEOs) of LBs and LFCs organized by the supervisory departments of the CBSL such as BSD and DSNBFI for the purpose of facilitating discussion on any issues of LBs and LFCs related to AML/CFT.

4.3 On-site Examinations

In terms of Section 18 of the FTRA, the FIU-Sri Lanka or any other person authorized by the FIU-Sri Lanka is empowered to carry out on-site examinations on the operations of reporting institutions to ensure the effective implementation of the requirements imposed under the FTRA or any other directions, rules or regulations issued by the FIU-Sri Lanka.

Table 4.2: No. of On-site Examinations Conducted and Fines Imposed by the FIU-Sri Lanka

Year	2008	2009	2010	2011	2012	2013	2014
No. of on-site examinations	8	5	5	4	16	26	4
Imposition of penalties (LKR Mn)	1.8	4.1	1.0	-	-	2.9	-

Source : FIU-Sri Lanka

In addition, the supervisory authorities also monitor the AML/CFT compliance of the reporting institutions as a part of their regular examinations. Findings of the examinations carried out by the supervisory authorities relating to AML/CFT are reported to the FIU-Sri Lanka.

BOX 2: MOBILE MONEY SERVICES IN THE CONTEXT OF ML/TF

What are Mobile Money Services?

Mobile money is a broad term that describes the use of the mobile phone to access financial services. The term does not assume any specific deployment model, or any particular transaction type. It merely describes a service where a customer uses mobile technology to trigger a financial event. As such, it encompasses information-only services (eg. a balance inquiry) and transactional services (eg. the use of mobile technology to send money to another person or to pay for goods and services, as well as government payments of salaries and benefits).

Characteristics of Mobile Money Services

Payment services that are commonly referred to as mobile money services include a range of services: some are simply new means of access to bank accounts, some enable payment from a credit card or other financial services products and some offer payment from existing accounts held by mobile network operators.

The payment services that are considered in this discussion involve the creation of a prepaid account, usually held by the mobile network operator (and in some cases a stand-alone account with a partner bank), and operated as an independent means of payment.

Mobile money services offer their customers to transfer money, pay utility bills, and make recurring payments such as insurance premiums, charitable donations or subscriptions and membership payments to clubs and professional bodies.

Sri Lankan Context

The regulatory framework for mobile money was enabled in year 2012, opening the market to both bank and non-bank providers and extending services to Sri Lanka's unbanked population. Revision to the Payments & Settlements Systems Act, No. 28 of 2005 facilitated the granting of a license to Dialog Axiata PLC, a Mobile Network Operator (MNO) to operate as a payment services provider. Accordingly, Dialog Axiata has implemented eZ cash in June 2012 and had been able to sign up over one million customers in just one year from June 2012 to June 2013. Another mobile network operator, Mobitel (Pvt) Ltd., entered into the market in December 2013 through a scheme known as mCash.

Two sets of guidelines were issued by the CBSL in year 2011, regulating two distinct mobile money products which are as follows:

1. An e-wallet linked to a bank account (regulated by the Mobile Payments Guidelines No.1 of 2011 for the Bank-led Mobile Payment Services); and
2. An e-wallet provided by a non-bank (including an MNO) that must have equivalent funds held in a custodian account in one (or more) Licensed Commercial Bank (regulated by the Mobile Payments Guidelines No.2 of 2011 for Custodian Account based Mobile Payment Services)

A license to provide mobile money products under the custodian account model can be granted to any "Licensed Service Provider", which can be any mobile payment service provider licensed under

the Service Providers of Payment Cards Regulations No.1 of 2009. Four types of entities qualified for this purpose are as follows;

1. Any Licensed Commercial Bank
2. Any Licensed Specialized Bank
3. Any Licensed Finance Company
4. Any public company with unimpaired capital of at least LKR 75 Mn.

Dialog, Mobitel and other MNOs that fit the criteria have qualified to provide mobile money services based on the above mentioned Mobile Payments Guidelines No.2 of 2011 for Custodian Account based Mobile Payment Services.

Mobile money payments for custodian account based mobile payment services operate primarily in three stages. That is,

1. Loading (cash-in)
2. Transferring
3. Withdrawal (cash-out)

A registered e-money subscriber can load money into his e-wallet from any registered merchant across the country. The MNO should perform due diligence on merchant. As per the CBSL guidelines, the MNO has to define the duties, responsibilities and procedures to be followed by merchants acting as agents for cash-in and cash-out transactions.

How a Mobile Money Services Vulnerable to ML/TF Risks?

Every payment system has some vulnerability that can facilitate ML/TF.

There are a few general risk categories that can be examined when assessing the vulnerability of any product. Hence, these risk factors are discussed in terms of mobile money services as follows.

- 1. Anonymity** - Anonymity means the ability for someone to disguise their identity in opening and operating an account. When a mobile customer is registered, transactions are less anonymous than with cash, since mobile transactions can be linked to a unique mobile number and since transactions (sender's mobile number, amount, receiver's mobile number and date) are recorded and traceable. This differs from cash where there is neither a unique identifier for the user nor a recorded trace of the payment. But at the same time the risk of anonymity is prevalent in mobile services when the actual user of the mobile service differs from the initial registered owner. Since a customer can obtain many mobile money accounts, mobile services can be obtained for all these registrations and the user of the account will not necessarily be the registered owner himself. Hence the product is vulnerable to the risk of anonymity at the time of operating the account.
- 2. Elusiveness** - Elusiveness means that the ownership of a transaction is disguised to either confuse or mislead authorities. While cash transactions are elusive, mobile money transactions are clearly traceable in the system of mobile operators as part of usual business practice. Telephone number (sending and receiving), time and the amount of the transaction are known to the mobile operator. However, when the same registered account is used by different individuals, elusiveness of transactions might occur since the transactions cannot be distinguished separately.

3. **Rapidity** - Rapidity means how fast can money move from one financial product to another or from a financial product in one country to overseas. Over a distance, the electronic character of mobile technology can make transactions more rapid and easier than cash. Rapidity is therefore a bigger risk factor for mobile money services than for cash.
4. **Lack of Oversight** - A mobile operator offering mobile money services is usually regulated, either indirectly through a partnership with a bank or directly through becoming a license holder of payments or e-money even though the cash economy lacks oversight.

Measures in Place to Mitigate Identified Risks

Three stages in the mobile money services operation will pose vulnerabilities to ML/TF risks. The measures that are available in the existing system to mitigate the risks arising from these vulnerabilities are discussed below.

1. **Loading with proceeds of crime** - At the loading stage, illicit monies are loaded into the system. This relates to the “placement” phase of ML. This can be for several reasons, one of which is to continue the process of smurfing, whereby criminals hide the true value of what is being loaded by dividing it into small batches that are more likely to go undetected.

The existing systems in the country can very easily look for any anomalies. Transacted values in mobile payments are very small and frequent use would facilitate the detection of such use. Further, it makes more difficult to the criminal as illicit funds will have to be split among a large number of mobile money accounts.

2. **Transferring of proceeds of crime** - Payment services can be abused to “layer” the funds. Layering is the strategy criminals employ to complicate the money trail, making it harder to trace.

This activity is also difficult in the existing practice, since the amounts involved are very small and the funds flow is easily traceable unlike cash.

3. **Withdrawal of proceeds of crime** - Criminals could find the withdrawal stage useful as a continuation of the layering process or as a way to integrate funds of illicit origins. The rapid movement of funds, coupled with anonymity, from their initial loading to ultimate withdrawal could be used to facilitate either ML or TF.

In the existing mobile money service operation, the account balance limits are very small. Hence, this becomes more difficult to be exploited. If this is to occur, these funds would need to be split among a large number of mobile money accounts meaning a criminal would need to withdraw many times from an agent. This would likely to be flagged, hence minimizing the risk involved.

With the availability of good systems of mobile network operators, sound monitoring and surveillance systems, all the above risks can be mitigated to a large extent. Guidelines have been issued by the regulator to the MNOs emphasizing their responsibilities in operating mobile money services. These are as follows:

- 1) Strictly adhering to the Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures in registering customers and maintaining customer accounts.

- 2) Monitoring and supervising the activities of e-money holders and merchants to ensure that they only engage in permitted services.
- 3) Submitting periodic reports and providing access to the e-money system, as and when requested by the custodian bank, in order to monitor the balances and activities of e-money holders.
- 4) Reporting to the custodian bank any suspicious transactions as per the regulations issued by the FIU-Sri Lanka established in terms of the FTRA.
- 5) Complying with any direction issued by the CBSL and adhering to reporting requirements imposed by the CBSL with regard to the custodian account based system.

References:

GSM Association (2013) *Mobile Money: Enabling Regulatory Solutions*. United Kingdom: GSM Association

Central Bank of Sri Lanka 2011, *Mobile Payments Guidelines No. 1 of 2011 for Bank-led Mobile Payment Services*.

Central Bank of Sri Lanka 2011, *Mobile Payments Guidelines No. 2 of 2011 for Custodian Account Based Mobile Payment*.

Service providers of Payment Cards Regulation No. 1 of 2009

Simone Di Castri (2013) *Enabling Mobile Money Policies in Sri Lanka (July 2013)*. United Kingdom. GSM Association

In the rapidly developing business environment, financial institutions tend to develop new products and business practices with the use of the modern technology available in the field. Consequently, financial institutions are required to deal with unanticipated vulnerabilities in ML/TF. Stakeholders need to pay more attention in upgrading the capacity of human resources in order to address emerging ML/TF threats and vulnerabilities. In this connection, the FIU-Sri Lanka has identified the necessity to increase the number of staff and enhance the knowledge of emerging trends of ML/TF typologies of the staff to carry out its growing responsibilities efficiently and effectively.

5.1 Training

The FIU-Sri Lanka currently consists of a multi-disciplinary team skilled in areas of Accountancy, Law, Banking and Finance, Economics and Information and Communication Technology (ICT). The staff of the FIU-Sri Lanka was provided with both local and international training opportunities related to different aspects of ML/TF during the year 2014. Details of the international and local training programmes attended by the staff during the year 2014 are given in Table 5.1 and Table 5.2, respectively.

Table 5.1: International Trainings/Workshops Attended by the FIU-Sri Lanka Officers during the Year 2014

Month	Training/Workshop	Country
February	6th BIMSTEC Sub Group Meeting on Combating the Financing of Terrorism (CFT)	India
February	Egmont Committee and Working Group Meeting	Hungary
March	FIUs Regional Co-operation Seminar	UAE
May	Workshop on Wire Transfers Relating to the Terrorist Financing	Thailand
June	Australian Transaction Reports and Analysis Centre (AUSTRAC) Regional Workshop-Money Laundering in the Insurance Market: A Risk and Vulnerability Assessment	Nepal
June	22nd Egmont Group Annual Plenary / Heads of FIUs Meeting	Peru
July	17th APG Annual Meeting and Technical Assistance Forum	China
September	Workshop on Enhancing AML/CFT Frameworks	Singapore
October	Joint FATF/EAG Evaluators' Training Programme	India
November	2014 FATF/APG Joint Experts' Meeting on Typologies and APG Technical Seminars	Thailand
December	Workshop on Money Laundering & Related Laws for the FIU and Judges of Court of Appeal	Australia

Source: FIU-Sri Lanka

Table 5.2: Local Trainings/Workshops Attended by the FIU-Sri Lanka Officers during the Year 2014

Month	Training/Workshop	Venue
April	Financial Intelligence for Banking and Financial Institutions	Centre for Banking Studies, Rajagiriya
May	Statistical Programming and Modelling Using SPSS Software	Centre for Banking Studies, Rajagiriya
July	ICA-International Diploma in Compliance	Centre for Banking Studies, Rajagiriya
August	Introduction to Statistics and Econometrics	Centre for Banking Studies, Rajagiriya
November	Portfolio at Risk and Bank Failures	Centre for Banking Studies, Rajagiriya

5.2 Outside Assistance

The FIU-Sri Lanka continues to obtain the services of two senior officers from the Attorney General's Department in executing with statutory functions and taking counter measures on ML/TF. The said consultants also participate as resource persons in awareness programmes conducted by the FIU-Sri Lanka.

The Information Technology Department of the CBSL (ITD) continued its co-operation for the development of IT infrastructure and maintenance of LankaFIN, a web based system to receive all electronic reports related to CTRs, EFTs and STRs without any interruption.

5.3 The Advisory Board

The Advisory Board of the FIU-Sri Lanka, which is chaired by the Governor of the CBSL, consists of 15 other senior officials represented from relevant key ministries and institutions of the country. The Advisory Board provides guidance on policy matters and other strategic issues relating to the FIU-Sri Lanka. The Advisory Board was convened in March and October during the year 2014.

Important policy decisions taken by the Advisory Board are given below.

- Granting approval to conduct the NRA with the technical guidance of the World Bank
- Granting approval to conduct mutual evaluation by the APG on the level of compliance with the FATF recommendations and the effectiveness of the AML/CFT system of the country
- Accepting to hold the 20th Asia Pacific Group on Money Laundering (APGML) plenary in Colombo in July 2017

Further, the FIU-Sri Lanka is in the process of amending the laws relating to ML and TF, with the approval of the Advisory Board.

Awareness of stakeholders is essential for effective implementation of the AML/CFT framework of the country. Thus, the FIU-Sri Lanka, as the authority for the implementation of the AML/CFT framework in the country, continued to conduct awareness programmes for key stakeholders as well as the general public during the year 2014. Accordingly, 1,138 participants from reporting institutions, supervisory authorities and LEAs attended 19 awareness programmes conducted during the year 2014.

6.1 Reporting Institutions

Awareness programmes were conducted for staff of reporting institutions such as LBs, FCs and leasing companies. These programmes provided opportunities for participants to enhance their knowledge on areas such as customer identification, record keeping, reporting requirements, identification of suspicious transactions and to obtain clarifications on issues/ problems they have encountered relating to compliance. Details of training programmes conducted during 2014 are given in Table 6.1.

Table 6.1: Awareness Programmes Conducted for the Reporting Institutions during the Year 2014

Date Conducted	Participating Institution/s	Venue	Programme	No. of Participants
25 January	People's Leasing and Finance PLC	Center for Banking Studies, Rajagiriya	KYC Regulations	40
1 April	Financial Institutions	Center for Banking Studies, Rajagiriya	KYC Regulations	25
23 April	Financial Institutions	Center for Banking Studies, Rajagiriya	KYC Regulations	30
26 April	Indian Overseas Bank	Center for Banking Studies, Rajagiriya	KYC Regulations	7
24 May	Financial Institutions in Northern Province	CBSL-Regional Office	KYC Regulations	66
24 May	Financial Institutions	Center for Banking Studies, Rajagiriya	KYC Regulations	20
10 July	Financial Institutions	Center for Banking Studies, Rajagiriya	Best Practices for Tellers	50
18 July	National Development Bank PLC	Center for Banking Studies, Rajagiriya	KYC Regulations	40
25 July	Nations Trust Bank PLC	Nations Trust Bank, Colombo	KYC Regulations	50
20 August	Nations Trust Bank PLC	Nations Trust Bank, Colombo	KYC Regulations	35
25 August	National Development Bank PLC	Center for Banking Studies, Rajagiriya	KYC Regulations	45

5 September	Seylan Bank PLC	Seylan Bank, Colombo	Seminar on AML/CFT	40
18 October	Alliance Finance PLC	Postgraduate Institution of Management, Colombo	KYC Regulations	250
15 November	Commercial Leasing and Finance PLC	Center for Banking Studies, Rajagiriya	AML/CFT Framework	60

6.2 Supervisory Authorities

In terms of the FTRA, supervisory authorities have a substantial role to play in AML/CFT by submitting STRs to the FIU-Sri Lanka and taking actions on information referred to them by the FIU-Sri Lanka. Accordingly, the FIU-Sri Lanka organized two awareness programmes for supervisory authorities during the year 2014. Details of these programmes are given in Table 6.2.

Table 6.2: Awareness Programmes Conducted by the FIU for Supervisory Authorities during the Year 2014

Date Conducted	Participating Institution/s	Venue	Programme	Number of Participants
22 May	Securities and Exchange Commission of Sri Lanka	Securities and Exchange Commission, Colombo	KYC Regulations	10
20 September	Lankaclear (Pvt) Ltd.	Center for Banking Studies, Rajagiriya	Regulatory and Compliance Requirements of AML	30

6.3 Law Enforcement Agencies

The FIU-Sri Lanka organized several awareness programmes for judges and officials from the Attorney General's Department, who play a vital role in enforcing the laws relating to ML/TF. Details of the programmes are given in Table 6.3.



Workshop on Prosecution of Offences under AML/CFT Legislation, Conducted for Prosecutors from the Attorney General's Department during December 13-14, 2014

Table 6.3: Awareness Programmes Conducted by the FIU-Sri Lanka for Law Enforcement Agencies during the Year 2014

Date Conducted	Participating Institution/s	Venue	Topics Covered	Number of Participants
25-26 October	High Court Judges	Batticaloa, Sri Lanka	Role of the High Court Judges in Enforcing AML/CFT Legislation	50
13-14 December	Prosecutors from the Attorney General's Department	Kalutara, Sri Lanka	Prosecution of offences under AML/CFT Legislation	55
22-23 December	Magistrates and District Court Judges	Colombo, Sri Lanka	Introduction to Legislation on Money Laundering and Financing of Terrorism	235



Workshop on Role of the High Court Judges in Enforcing AML/CFT Legislation Conducted at Batticaloa during October 25-26, 2014

7.1 Laundering Proceeds from Transshipment

Transshipment ports are used to export goods to a particular destination in the absence of a direct link by air, land or sea to the intended destination or for other economic and logistical reasons.

Transshipment is one of the most common methods in carrying out Trade Based ML. Sri Lanka is exposed to ML through transshipment since the country is situated in a central position in the Indian Ocean connecting Eastern and Western trade routes. In this case, the purpose of transshipment is to export illegal goods hiding the identity of the jurisdictions/parties involved.

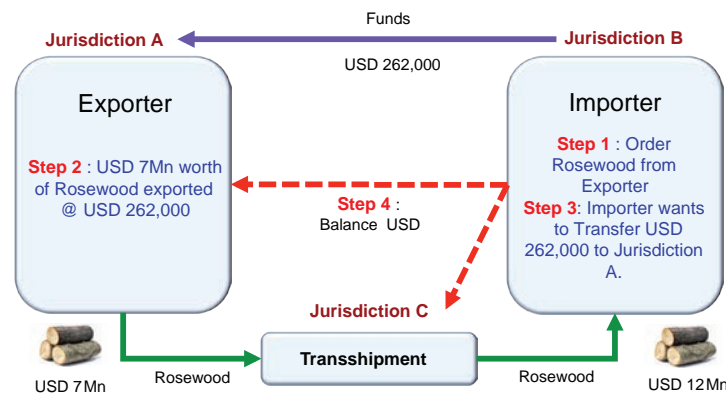
Case Study

Sri Lanka Customs submitted an STR to the FIU-Sri Lanka requesting assistance for their investigations on 28 containers of rosewood timber logs which were due to be transshipped to Jurisdiction 'B' via Sri Lanka from Jurisdiction 'A'. The Customs had intercepted the 28 rosewood containers weighing 420 metric tons.

Transshipment of said rosewood is prohibited or illegal since;

- Rosewood is one of the most valuable tropical hardwoods that are found in Madagascar, East Africa, Brazil and South East Asian countries.
- Trading of rosewood logs comes under Convention on International Trading of Endangered Species (CITES) and Sri Lanka is a signatory to this international convention.
- International trading is allowed only on permits issued by the local authority concerned.
- Cutting and trading of rosewood is banned in Madagascar

Diagram 1

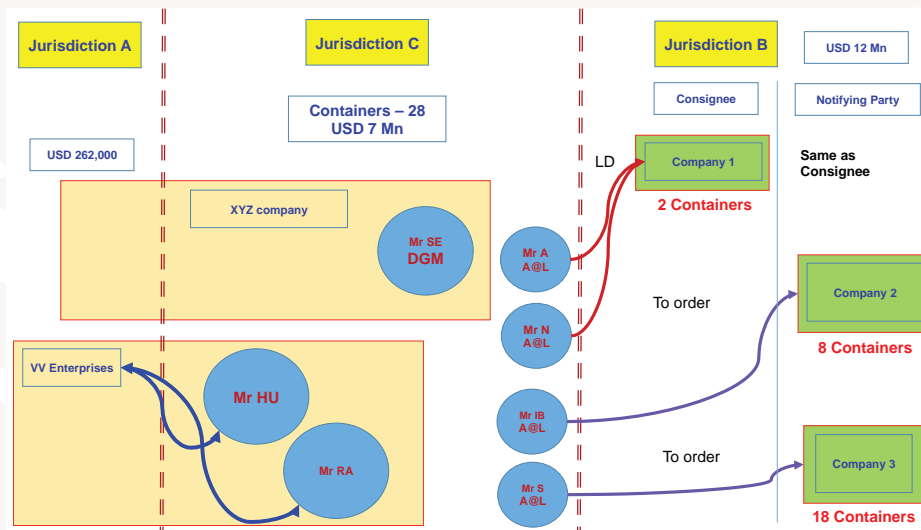


The jurisdiction B imports Rosewood worth of USD 7 Mn. from Jurisdiction A. These logs of Rosewood were undervalued at USD 262,000 in comparison with their fair market value and received by Jurisdiction C Port. According to the bill of lading, the Rosewood logs were to be delivered to an unidentified consignee of Jurisdiction B.

The officials of Sri Lanka Customs were able to identify the illegal transshipment of Rosewood to Sri Lanka. Dealing with banned goods is an offence, in terms of Prevention of Money Laundering Act (PMLA) No. 5 of 2006 and Customs Ordinance.

The “XYZ” is container transportation and shipping company and they have many subsidiary companies which are involved in the international trade. The “VV” Enterprises is an exporting company in Jurisdiction A. Agents hired by Company 1, Company 2 and Company 3 had stayed in Sri Lanka and helped the transshipment process. When the containers were ceased by the Sri Lanka Customs, agents appeared as representatives for each company although they had failed to produce appropriate documentation and therefore, the Customs had ceased 28 Nos. of containers with logs of Rosewood.

Diagram 2



Indicators relevant to this case;

- Shipping of goods from a jurisdiction designated as “High Risk” for ML activities
- Significant discrepancies between the description of the goods in the bill of lading and the actual goods shipped
- Use of shell companies to place or layer, obscure ownership and retain control
- Customers’ inability to produce appropriate documentation

7.2 Money Laundering through Legal Arrangements

Money launderers often misuse legal arrangements to disguise and convert the proceeds of their crimes into legal terms.

Case Study

The FIU-Sri Lanka received an STR as a public complaint that Mr. 'MS' has misused funds of a legal arrangement called SS Trust. It was incorporated through a trust deed attested in 1997. The trust has been established to help Tsunami affected children. A children's orphanage has been built by the trust.

The Board of trustees was Mr. 'MS', his wife, father, mother, two other Sri Lankans and three individuals from Netherland. The trust had received funds from these foreign trustees as donations.

In addition to this trust, Mr. 'MS' acts as a director of several other companies. He and two other trustees of the SS Trust act as directors of a finance company called 'D' Investment (Pvt) Ltd. It has been registered under the Companies Act, at the same address of 'SS' Trust.

Donations to the trust were received to its current account and Mr. 'MS' had withdrawn the funds to invest in his other companies. In order to cover up the discrepancy of the funds, he had issued fixed deposit certificates in the name of 'D' Investment Ltd. The name in the Fixed Deposit (FD) certificate was different from the registered name of the company which was "D Investment (Pvt) Ltd".

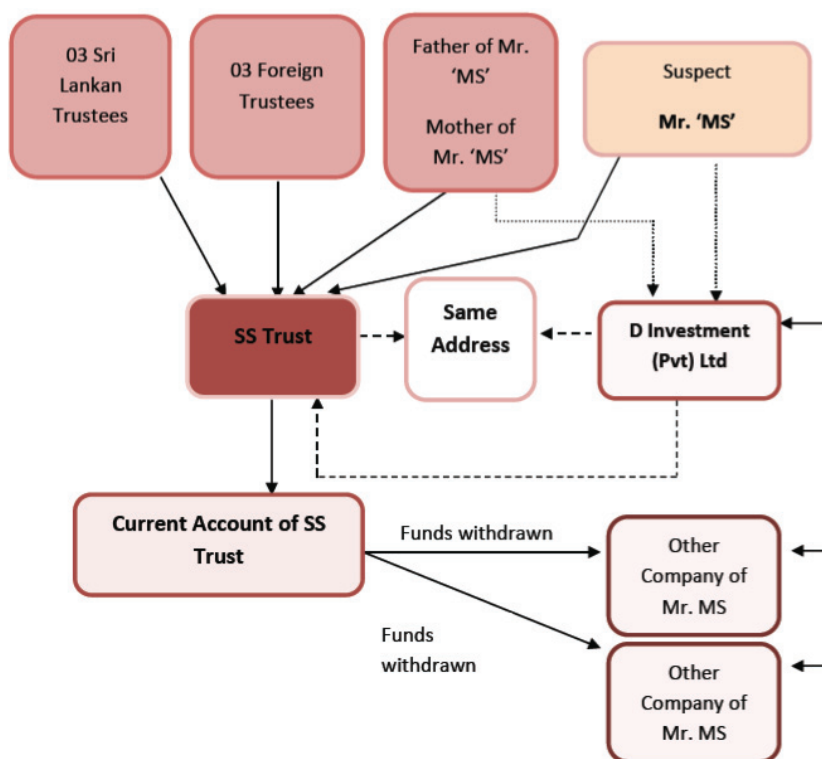
It was further observed that this finance company is an illegal deposit taking institution and had operated only for accounting purpose. The value of the fraudulent FDs amounted to LKR 15 Mn and no interest payment was ever credited to the account of the trust as the interest given to the FDs.

The accounts of the trust have been prepared in a manner that the foreign trustees were satisfied, by showing that the donations were invested in fixed deposits in a legalized FC. The funds were withdrawn through cheques from the said current account of the trust using the signature of the father of Mr. 'MS', who was an authorized signatory of the account. He had believed that the withdrawals were for bona fide purposes and had given his signature without any suspicion.

In addition to the fake FD certificates, Mr. 'MS' had issued fraudulent bill payment documents to cover up the fund withdrawals from the trust. These bills were signed by a person who was neither a trustee nor an employee of the trust. Further, the materials given to the construction of the orphanage had been used for other private properties of Mr. 'MS'.

Accordingly, the case was referred to the CID for further investigation. The facts revealed on the 'D' Investment (Pvt) Ltd was referred to the DSNBFI to take necessary action.

Diagram 3



Indicators relevant to this case;

- Appointing family members as Board of trustees
- Providing false or counterfeited documentations
- Having illegal deposits

7.3 Money Laundering through Shell Companies

Shell companies are often associated with fraud and utilized by individuals to facilitate fraudulent activities. Such activities include ML, tax evasion, fictitious service schemes etc.

Case Study

The FIU-Sri Lanka received an STR from a leading foreign commercial bank regarding the selling of lands to foreigners illegally through shell companies. The government of Sri Lanka has imposed regulations restricting foreigners to buy lands in the country, and if they wish to buy, they were required to pay 100% of the value as taxes.

Mr. 'S' is a senior partner of company 'SA' which was a legal firm and engaged in incorporating limited liability companies. In addition, he is a director of companies 'SH' and 'LR' as well. Company 'SH'

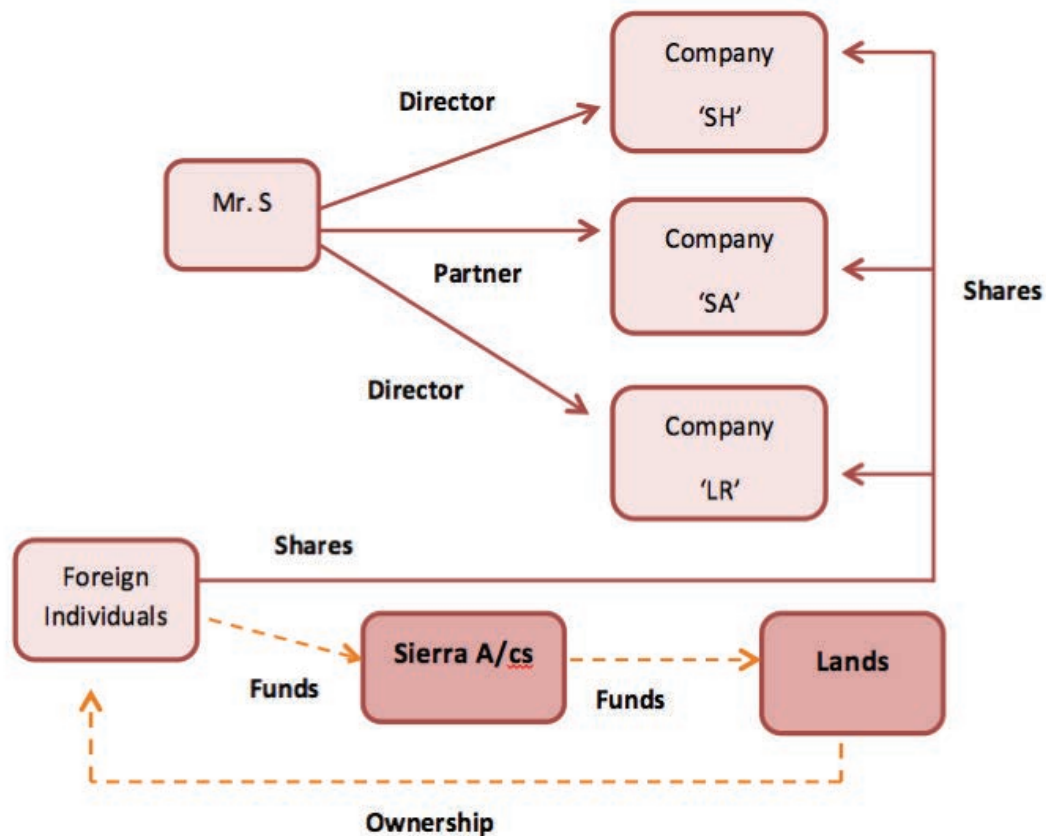
provides secretarial services to the two companies. These companies were shell companies and had opened accounts at the bank which reported the STR.

Company 'SH' and 'LR' had purchased lands around Sri Lanka as company assets through Company 'SA'. At the same time potential foreign buyers are found around the world by 'SA', and are introduced to the STR reporting bank to open SIERA accounts.

Later, funds received from foreign investors to their SIERA accounts had been used to purchase shares of these shell companies. Subsequently, 100% ownership of companies was transferred to the foreigners. With this share transfer, ownership of the company assets including the lands purchased in Sri Lanka was also automatically transferred to the foreigners.

Accordingly, Company 'SA' had deviated from the regulation imposed by the government which restricts foreigners buying lands in Sri Lanka. Foreign parties were not aware of these activities and they had faced difficulties in proceeding constructions since the element of cheating is evident. The case was referred to the relevant law enforcement authorities for further investigations.

Diagram 4



Indicators relevant to this case;

- Establishing shell companies to place or layer, obscure ownership
- Misusing Clients' Accounts
- Attempting to disguise the real owners or parties to the transactions

8.1 LankaFIN

The FIU-Sri Lanka, with the assistance of the ITD developed the LankaFIN web based system for submitting online information on suspicious transactions. Accordingly, LankaFIN received CTRs and EFTs from 25 LCBs, 9 LSBs, 48 LFCs, 21 ICs and 30 SBs in 2014.

A Compliance Officer for each reporting institution is required to be appointed for the purpose of ensuring the institution's compliance with Section 14 of the FTRA. There were 133 registered Compliance Officers and 136 registered Compliance Assistants as at end 2014, and they actively participated in compliance work including submission of data to the FIU-Sri Lanka. Sector-wise distribution of 269 registered LankaFIN users is shown in the Table 8.1.

Table 8.1: Distribution of Registered LankaFIN Users by Reporting Institutions

Sector	Compliance Officers	Compliance Assistants	Total No. of LankaFIN Users
Licensed Commercial Banks	25	50	75
Licensed Specialized Banks	9	8	17
Licensed Finance Companies	48	48	96
Insurance Companies	21	16	37
Stock Brokers	30	14	44
Total	133	136	269

Source: FIU-Sri Lanka

Because of the importance and confidentiality of the data submitted through the LankaFIN System, Secure Sockets Layer (SSL) Certification has been obtained for the system. Further, the file transmitting process uses MD5 Hash Code for increasing data security and controlling integrity.

Transaction details received through the LankaFIN system are stringently checked to fulfill the KYC/CDD rules issued by the gazette dated March 28 of 2011 "KYC/ CDD Rules for Licensed Banks and Licensed Finance Companies - Extraordinary Gazette No 1699/10". The reports which do not meet the requirements of the said KYC/CDD rules are rejected through the LankaFIN system.

8.2 FIU-Sri Lanka Website

The FIU-Sri Lanka Website, www.fiusrilanka.gov.lk, was launched on the 1st of January 2014. More than 14,000 people have viewed the Website during 2014 and it was observed that the majority of the users accessed the United Nations Security Council Resolutions (UNSCR) page in addition to the Home Page. The Website provides the amendments to the UNSCR 1267 list of designated persons in accordance with the Regulation 4(2)(b) of the United Nations No. 2 of 2012 published in the Gazette Extraordinary No. 1760/40 of May 31, 2012 for use of financial institutions. The UNSCR 1373 (2001) and its successor resolutions refer to designating individuals and entities related to terrorism and terrorist financing in Sri Lanka. Accordingly, Financial Institutions are obliged to have measures in place to identify and freeze funds, financial assets or economic resources of such designated persons and entities upon order of the Competent Authority.

BOX 3: RECENT COMPLIANCE CHANGES IN ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

The AML/CFT initiatives are becoming increasingly interconnected across operations and jurisdictions. As a result significant changes were made to the requirements issued by the FATF in February 2012. Accordingly, the earlier 40 Recommendations on ML and 9 Special Recommendations on TF were merged and Revised 40 General Recommendations were developed by the FATF. Regulators and financial institutions are obliged to make significant changes in response to the continuously evolving regulatory landscape. Key areas of changing AML/CFT compliance are as follows.

1. Risk-Based Approach (RBA)

When considering the changes in the regulatory landscape of AML compliance, strong emphasis on the RBA is a necessity requirement. Initially, the NRA has to be conducted and countries should ensure that regulated businesses apply a RBA with regard to these risk assessments. In addition, the supervisors should also apply a RBA in their supervisory framework.

At present, the legal framework of Sri Lanka does not facilitate the assessment of ML/TF on a RBA. Hence, amendments are proposed to the prevalent legislation to adopt a RBA. The NRA was conducted with the guidance and coordination of the FIU-Sri Lanka and the results have also been disseminated to the relevant stakeholders. Accordingly, preventive measures are proposed on the vulnerable areas that have been identified in the above assessment.

2. Simplified Customer Due Diligence (SCDD) and Enhanced Customer Due Diligence (ECDD)

In the RBA, financial institutions are required to identify, assess and understand their customers and categorize them based on their risk profiles. The SCDD will have to be justified on the basis of lower risk while ECDD are to be based on the high risk. Further, when assessing ML risks countries must also consider the potential high risk factors.

The FIU-Sri Lanka is in the process of issuing a comprehensive gazette notification on Customer Due Diligence (CDD) to all financial institutions which will address deficiencies in the current rule.

3. Beneficial Ownership

As per the new regulations, companies are required to hold adequate, accurate and current information on their beneficial ownership, and such information has to be assessed in a timely manner by regulators and regulated businesses. Furthermore, trustees must disclose their status to designated persons when forming business relationships/occasional transactions. As a result, governments and financial authorities will require banks and all other legal entities to further improve their KYC procedures.

Companies Act No. 07 of 2007 and Trust Ordinance in Sri Lanka are required to be amended to ensure that information on beneficial ownership of legal persons and legal arrangements is maintained in accordance with the revised standards.

4. Politically Exposed Persons (PEPs)

As per the new regulations, PEPs regime was extended to domestic PEPs and persons holding prominent positions in international organizations. New requirements facilitates a RBA with regard to the level of due diligence performed on domestic PEPs compared to foreign PEPs. ECDD will be appropriate in all instances where the business relationship is deemed high risk. This may affect financial institutions that do not currently carry out ECDD for high risk domestic PEP relationships.

Existing AML/CFT regulations in Sri Lanka specify that authorization of the senior management is required when opening of accounts for PEPs. The new gazette notification on CDD would provide further guidance for the financial institutions on PEPs.

5. New Technologies

Criminals continue to evolve their tactics to get dirty money into the legitimate financial system to produce clean funds. Well known threats are ML through shell companies and trusts. New threats come from mobile banking and virtual currencies while current threats come from e-money issuers, cybercriminals etc. All these have to be considered in developing a robust and sophisticated AML approach.

Current AML/CFT guidelines on new technologies in Sri Lanka have been revisited and more enhanced measures have been included in the proposed gazette notification on CDD.

6. Real Engagement by Senior Management

The AML policy of the respective institution will have to be approved by its Board of Directors as per the changing regulatory framework. Board of Directors in all financial institutions should actively be involved in ensuring the AML compliance. This should ensure the commitment of the senior management which has to be started from the AML policy itself.

As per the FIU-Sri Lanka's advice, all financial institutions are required to maintain an AML policy document approved by the board of directors. Furthermore, appointment of the compliance officer should be approved by the CEO of each institution.

7. Sectorial Guidance

Countries are required to adopt the RBA in assessing ML/TF risk. The NRA of a country will be based on the sectorial risk assessment prior to the national risk compilation. Hence, the ML risks and concerns of the financial and non-financial sectors will be identified, assessed and understood in this process. This will further enable a country to identify the gaps and make amendments to rectify the same and formulate and implement national policies.

When the NRA of Sri Lanka was conducted, separate risk assessments were compiled for sectors in the Financial as well as DNFBPs prior to the overall country risk compilation. After identifying the sectorial ML/TF risk, institution-wise risk assessments should be carried out to understand risks inherent to the sector.

8. Enforcement of Administrative Sanctions and Sanctions for Non-Compliance

The changing regulatory framework has higher focus on enforcement activities. There are administrative sanctions introduced for system failures and much greater focus is given to sanctions for non-compliance. This stresses the fact that, merely having regulations to assure the level of compliance is not sufficient. The legal and regulatory framework should ensure that there is sound enforcement procedures embedded in the legislature as well as the practical implementation of the same by the law enforcement.

When amendments are proposed to the existing legislation, proportionate and dissuasive sanctions have been proposed in line with the revised standards.

9. Impact on Taxation Issues

In recent years, more AML rules have focused on taxation issues. Consequently, the tax evasion and other serious fiscal offences have been included in the list of the AML predicate offences. Tax evasion of Sri Lanka is not a predicate offence according to the current AML/CFT legislation of Sri Lanka. Since tax evasion is a key issue affecting the AML/CFT framework of a country, it has been proposed to include as a predicate offence in the amendments to the legislation.

PHOTO GALLERY



PHOTO GALLERY



PHOTO GALLERY



PHOTO GALLERY



APPENDIX A: LIST OF RULES/ DIRECTIONS/ CIRCULARS / GUIDELINES ISSUED FROM 2006 TO 2014

YEAR 2014

1. Prevention and Suppression of Terrorism and Terrorist Financing Obligations of Reporting Institutions- Authorized Money Changers
2. Prevention and Suppression of Terrorism and Terrorist Financing Obligations of Reporting Institutions- All Licensed Banks and Licensed Finance Companies
3. Prevention and Suppression of Terrorism and Terrorist Financing - Obligations of Insurance Companies
4. Prevention and Suppression of Terrorism and Terrorist Financing - Obligations of Stock Brokers

YEAR 2013

1. KYC/ CDD Rules for Authorized Money Changers, January 31 of 2013
2. Public Statement by the Financial Action Task Force (FATF)
3. Prevention and Suppression of Terrorism and Terrorist Financing Obligation of Reporting Institutions - All Licensed Banks & Licensed Finance Companies
4. Prevention and Suppression of Terrorism and Terrorist Financing Obligation of Reporting Institutions - Insurance Companies
5. Prevention and Suppression of Terrorism and Terrorist Financing Obligation of Reporting Institutions - Stock Brokering Companies

YEAR 2012

1. Revisions to 40+9 Recommendations of the FATF
2. Notification from the FIU of the St. Vincent and the Grenadines
3. Compliance with the Reporting requirements under the Financial Transactions Reporting Act. No. 06 of 2006 for all Financial Institutions
4. Amendments to the KYC/ CDD Rules, No.1 of 2011 for the Licensed Banks and Licensed Finance Companies - Extraordinary Gazette No 1756/27, May 04 of 2012

YEAR 2011

1. KYC/ CDD Rules for Licensed Banks and Licensed Finance Companies - Extraordinary Gazette No 1699/10, March 28 of 2011
2. Auditor's Declaration on Establishment of Audit Functions
3. Compliance with the Reporting Requirement under Section 7 of the FTRA
4. Revisions to Extraordinary Gazette Notification No. 1699/10 - KYC/CDD Rules No. 01 of 2011

YEAR 2010

1. Web Based Information Reporting System to Insurance Companies
2. Web Based Information Reporting System to Stock Brokers

YEAR 2009

1. Compliance with the Section 2 of the FTRA - (LBs)
2. Compliance with the Section 2 of the FTRA - (RFCs)
3. Inclusion of the Tamil Foundation among the List of Terrorist Organizations in US
4. AML/CFT Compliance Functions of the Insurance Industry
5. Web Based Reporting System for LCBs & LSBs
6. Web Based Reporting System RFCs

YEAR 2008

1. KYC/ CDD Rules for the Insurance Industry
2. Compliance with Rules on CDD for Financial Institutions
3. Compliance with Reporting Requirement (Amended)
4. Inclusion of the World Tamil Movement among the List of Terrorist Organizations in Canada
5. Use of Banking System by Institutions and Persons not Authorised to Accept Deposits
6. Compliance with Reporting Requirement of FTRA-Securities Industry
7. Compliance with Reporting Requirement of FTRA-Insurance Industry

YEAR 2007

1. KYC/ CDD Rules for the Securities Industry
2. Compliance with KYC/CDD Rules for New Customers and Existing Customers
3. Compliance with the Reporting Requirements under the FTRA
4. Light a Million Candles Campaign-Offences Against Children
5. Mandatory Reporting Requirements-Electronic Fund Transfers

YEAR 2006

1. Compliance with the Reporting Requirement under the FTRA No 6 of 2006
2. Section 312 & Section 319 of the Patriot Act
3. The Financial Transactions Reporting Act No. 06 of 2006 Submission of Data
4. Financial Transactions Reporting Act (FTRA) No. 06 of 2006
5. CDD for Inward Remittance

APPENDIX B: REPORTING INSTITUTIONS AS AT 31ST DECEMBER 2014

Licensed Commercial Banks

- 1 Amana Bank PLC
- 2 Axis Bank Ltd
- 3 Bank of Ceylon
- 4 Cargills Bank Ltd
- 5 Citibank, N.A.
- 6 Commercial Bank of Ceylon PLC
- 7 Deutsche Bank A.G.
- 8 DFCC Vardhana Bank PLC
- 9 Habib Bank Ltd
- 10 Hatton National Bank PLC
- 11 ICICI Bank Ltd
- 12 Indian Bank
- 13 Indian Overseas Bank
- 14 MCB Bank Limited
- 15 National Development Bank PLC
- 16 Nations Trust Bank PLC
- 17 Pan Asia Banking Corporation PLC
- 18 People's Bank
- 19 Public Bank Berhad
- 20 Sampath Bank PLC
- 21 Seylan Bank PLC
- 22 Standard Chartered Bank
- 23 State Bank of India
- 24 The Hongkong & Shanghai Banking Corporation Ltd
- 25 Union Bank of Colombo PLC

Licensed Specialized Banks

- 1 DFCC Bank PLC
- 2 HDFC Bank of Sri Lanka
- 3 Lankaputhra Development Bank Ltd
- 4 MBSL Savings Bank Ltd
- 5 National Savings Bank
- 6 Pradeshiya Sanwardhana Bank
- 7 Sanasa Development Bank Ltd
- 8 Sri Lanka Savings Bank Ltd
- 9 State Mortgage and Investment Bank

Licensed Finance Companies

- 1 Abans Finance PLC
- 2 Alliance Finance Co. PLC
- 3 AMW Capital Leasing and Finance PLC
- 4 Arpico Finance Company PLC
- 5 Asia Asset Finance PLC

- 
- 6 Asian Finance Ltd
 - 7 Associated Motor Finance Co. PLC
 - 8 Bartleet Finance PLC
 - 9 Bimputh Finance PLC
 - 10 Brac Lanka Finance PLC
 - 11 Capital Alliance Finance PLC
 - 12 Central Finance Co. PLC
 - 13 Central Investments & Finance PLC
 - 14 Chilaw Finance PLC
 - 15 Citizens Development Business Finance PLC
 - 16 City Finance Corporation Ltd
 - 17 Commercial Credit and Finance PLC
 - 18 Commercial Leasing and Finance Ltd
 - 19 Deshodaya Development Finance Company Ltd
 - 20 ETI Finance Ltd
 - 21 George Steuart Finance PLC
 - 22 Ideal Finance Ltd
 - 23 Kanrich Finance Ltd
 - 24 Lanka ORIX Finance PLC
 - 25 LB Finance PLC
 - 26 MCSL Financial Services Ltd
 - 27 Melsta Regal Finance Ltd
 - 28 Mercantile Investments and Finance PLC
 - 29 Multi Finance PLC
 - 30 Nation Lanka Finance PLC
 - 31 Orient Finance PLC
 - 32 People's Leasing & Finance PLC
 - 33 People's Merchant Finance PLC
 - 34 Prime Grameen Micro Finance Ltd
 - 35 Richard Pieris Finance Ltd
 - 36 Senkadagala Finance PLC
 - 37 Indra Finance Ltd
 - 38 Singer Finance (Lanka) PLC
 - 39 Sinhaputra Finance PLC
 - 40 Siyapatha Finance PLC
 - 41 Softlogic Finance PLC
 - 42 Swarnamahal Financial Services PLC
 - 43 T K S Finance Ltd
 - 44 The Finance Co. PLC
 - 45 The Standard Credit Finance Ltd
 - 46 Trade Finance & Investments PLC
 - 47 U B Finance Co. Ltd
 - 48 Vallibel Finance PLC

Insurance Companies

- 1 AIA Insurance Lanka PLC
- 2 AIG Insurance Ltd
- 3 Allianz Insurance Lanka Ltd

- 
- 4 Allianz Life Insurance Lanka Ltd
 - 5 Amana Takaful PLC
 - 6 Arpico Insurance Ltd
 - 7 Asian Alliance Insurance PLC
 - 8 Ceylinco Insurance PLC
 - 9 Continental Insurance Lanka Ltd
 - 10 Co-operative Insurance Company Ltd
 - 11 HNB Assurance PLC
 - 12 Janashakthi Insurance PLC
 - 13 Life Insurance Corporation (Lanka) Ltd
 - 14 LOLC Insurance Company Ltd
 - 15 MBSL Insurance Company Ltd
 - 16 National Insurance Trust Fund Board
 - 17 Orient Insurance Ltd
 - 18 People's Insurance Ltd
 - 19 Sanasa Insurance Co. Ltd
 - 20 Sri Lanka Insurance Corporation Limited
 - 21 Union Assurance PLC


Stock Brokers

- 1 Acuity Securities Ltd
- 2 Acuity Stockbrokers (Pvt) Ltd
- 3 Asha Phillip Securities Ltd
- 4 Asia Securities (Pvt) Ltd
- 5 Assetline Securities (Pvt) Ltd
- 6 Bartleet Religare Securities (Pvt) Ltd
- 7 Candor Equities Ltd
- 8 Capital Alliance Limited
- 9 Capital Alliance Securities (Pvt) Ltd
- 10 Capital Trust Securities (Pvt) Ltd
- 11 Claridge Stockbrokers (Pvt) Ltd
- 12 CT CLSA Securities (Pvt) Ltd
- 13 Enterprise Ceylon Capital (Pvt) Ltd
- 14 First Capital Equities (Pvt) Limited
- 15 First Capital Markets Ltd
- 16 First Guadian Equities (Pvt) Ltd
- 17 J B Securities (Pvt) Ltd
- 18 John Keells Stockbrokers (Pvt) Ltd
- 19 Lanka Securities (Pvt) Ltd
- 20 LOLC Securities Ltd
- 21 Nation Lanka Equities (Pvt) Ltd
- 22 NatWealth Securities Ltd
- 23 Navara Securities (Pvt) Ltd
- 24 NDB Securities (Pvt) Ltd
- 25 NSB Fund Management Co Ltd
- 26 Perpetual Treasuries Ltd
- 27 Richard Peiris Securities (pvt) Ltd
- 28 S C Securities (Pvt) Ltd

- 29 Serendib Stockbrokers (Pvt) Ltd
- 30 SMB Securities (Pvt) Ltd
- 31 Softlogic Stockbrokers (Pvt) Ltd
- 32 Somerville Stock Brokers(Pvt) Ltd
- 33 Taprobane Securities (Pvt) Ltd
- 34 TKS Securites (Pvt) Ltd
- 35 Wealthtrust Securities Ltd

Authorized Money Changers

- 1 Crown Money Exchange (Pvt) Ltd-Branch
- 2 A O Lakshmi Jewels (Pvt) Ltd
- 3 Abdeen Money Changers (Pvt) Ltd
- 4 Amani International (Pvt) Ltd
- 5 Anton Money Exchange (Pvt) Ltd
- 6 Ariyawansa Enterprises (Pvt) Ltd
- 7 Ariyawansa Enterprises (Pvt) Ltd - Branch
- 8 Armex Money Changers (Pvt) Ltd
- 9 Arrujina Jewellery (Pvt) Ltd
- 10 Aruna Forexc (Pvt) Ltd
- 11 Aswin Exchange (Pvt) Ltd
- 12 Bullion Money Exchange (Pvt) Ltd
- 13 Capital Exchange (Pvt) Ltd
- 14 City Exchange (Pvt) Ltd
- 15 City Exchange (Pvt) Ltd-Branch
- 16 City Money Exchange (Pvt) Ltd
- 17 Colombo Money Exchange (Pvt) Ltd
- 18 Dadigama Group (Pvt) Ltd
- 19 Data Exchange International (Pvt) Ltd
- 20 Daya Authorized Money Changer (Pvt) Ltd
- 21 Delta Sarath Holdings (Pvt) Ltd
- 22 Devi Forex (Pvt) Ltd
- 23 George Michael Holdings (Pvt) Ltd
- 24 Global Village Exchange (Pvt) Ltd
- 25 Golden Money Changers (Pvt) Ltd
- 26 GTV Enterprises (Pvt) ltd
- 27 International Exchange (Pvt) Ltd
- 28 Jewel Lanka Money Exchange (Pvt) Ltd
- 29 Jewels City (Pvt) Ltd
- 30 Kamal Enterprises (Pvt) Ltd
- 31 Keyser Exchange (Pvt) Ltd
- 32 Kudamadu Money Exchange (Pvt) Ltd
- 33 M P Money Changer (Pvt) Ltd
- 34 Majestic Jewellery (Pvt) Ltd
- 35 Maruthi Money Exchange (Pvt) Ltd
- 36 Mayurie Money Changers (Pvt) Ltd
- 37 Metro Forex (Pvt) Ltd
- 38 Midna Mini Market (Pvt) Ltd
- 39 Milano Money Exchange (Pvt) Ltd

- 
- 40 Montecarlo Exchange (Pvt) Ltd
 - 41 Narmatha Gold Centre (Pvt) Ltd
 - 42 New Nathasha Money Changer (Pvt) Ltd
 - 43 New Regal's Money Changer (Pvt) Ltd
 - 44 Niketh Money Exchange R K (Pvt) Ltd
 - 45 Nilmi Money Exchange (Pvt) Ltd - Branch
 - 46 Nilmi Money Exchanging (Pvt) Ltd
 - 47 Pearl Exci (Pvt) Ltd
 - 48 Prasanna Money Exchange (Pvt) Ltd - Branch
 - 49 Prasanna Money Exchange (Pvt)Ltd
 - 50 Pushpa Money Changers (Pvt) Ltd
 - 51 Rafeek's Gems (Pvt) Ltd
 - 52 Ravi Forexae (Pvt) Ltd
 - 53 Red Ruby Jewellers (Pvt) Ltd
 - 54 Rimha Jewellers (Pvt) Ltd
 - 55 Rivindu Enterprises (Pvt) Ltd
 - 56 Royal Money Exchange (Pvt) Ltd
 - 57 Royal Money Exchange (Pvt) Ltd-Branch
 - 58 Royal Money Mart (Pvt) Ltd
 - 59 Salaka Trust Investment (Pvt) Ltd
 - 60 Salaka Trust Investment (Pvt) Ltd-Branch I
 - 61 Sharanga Money Exchange (Pvt) Ltd
 - 62 Shifaz Money Exchange (Pvt) Ltd
 - 63 Swiss Money Exchange (Pvt) Ltd
 - 64 Swiss Money Exchange (Pvt) Ltd-Branch
 - 65 Thomas Cook Lanka (Pvt) Ltd I
 - 66 Thomas Cook Lanka (Pvt) Ltd-Branch II
 - 67 Unic Forex (Pvt) Ltd
 - 68 Vasanthas International Money Exchange (Pvt) Ltd
 - 69 Wimal Exchange (Pvt) Ltd
 - 70 Windsor Money Exchange (Pvt) Ltd