Anti -Money Laundering and Combating the Financing of Terrorism (AML/CFT) Policy and Procedures Manual

Version Control

Date	Version	Author	Description
22-Feb -2017	1.1	Summaiya Macan Marker	Anti -Money Laundering and Combating the Financing of Terrorism Policy and Procedures Manual - Approved
10th May 2018	1.2	Summaiya Macan Marker	Anti -Money Laundering and Combating the Financing of Terrorism Policy and Procedures Manual - Annual Review

Approval History

Date	Version	Approved by:	Comments
31-Jan-2017	1.1	MD/ CEO and ERMC	
22-Feb- 2017	1.1	BIRMC	
1st –Mar- 2017	1.1	BOD	
15-May-2018	1.2	MD/ CEO and ERMC	Recommended
22-May-2018	1.2	BIRMC	Recommended
	1.2	BOD	

Document Owner

Business Unit/ Department
Compliance Department

Contents

1. Introduction

Cargills Bank attaches the highest importance to prevent the Bank from being a utilized as a conduit and/or to be directly or indirectly be used for financial crime purpose/s by it's customers.

This Policy and Procedure manual is a high level guide and sets out the relevant areas that employees of the Bank need to be aware of at all times. This Policy and Procedure Manual is issued to enable employees to obtain a general understanding on Anti Money Laundering/Terrorist Financing and should be read and understood in Conjunction with the other relevant and applicable circulars, instructions and guidance notes issued by the Compliance Unit from time to time.

Banks are facing a heightened level of Anti Money Laundering and Prevention of Terrorist Financing Laws and Regulations due to the ever increasing threat of financial crime world wide. During the past several years, regulatory bodies have been aggressively stepping up their enforcement actions, and hence the Banking industry is facing challenges in monitoring the adequacy of control methods utilized to prevent their Financial Institutions been used for such activities

The Cost of Non Compliance in very high and the resulted risk, such as the loss of reputation, penalties and monetary loss can be potentially fatal to any Bank

In this Context, we at Cargills Bank need to adopt strategies to deploy robust systems and adopt the highest level of Compliance. This is required not just to build a high level of trust amongst customers but also to maintain the confidence of customers, the Regulator, Correspondent Banks and all other stakeholders .

Banks and Financial Institutions play a key role to combat the risks of money laundering and assist regulators in the fight against terrorist financing. It is the paramount duty and responsibility of the Bank to know and understand its customers fully in terms of identity and activity to the extent of establishing the accuracy of its credentials in extending Banking Facilities of any forms.

This exercise enables the Bank to identify adverse risks if any, associated with the applicant/customer (at the time of establishing a Banking relationship) and help guard against criminals/fraudsters making use of banking channels/services for their unlawful activities.

With the present day multi dimension delivery of Banking services, channels and products, the need for a structured methodology for understanding customers at the time of establishing Banking relationships and ongoing due diligence has assumed a greater importance.

We at Cargills understand the Risks the Bank is exposed to, and will periodically assess the risk through Compliance Risk Assessment (CRA) and include adequate controls and mitigations to our processes and systems from time to time.

1.1 Some steps taken at Cargills Bank

- Establishment of a Compliance Department under the Compliance Officer appointed at a senior management level who is dedicated to the task of overseeing Cargills Bank's Compliance function and policies, practices and procedures with regard to Anti Money Laundering and Prevention of Terrorist Financing.
- Establishment of a Compliance Culture that values and rewards the implementation of appropriate Controls and Compliance procedures.
- Use of independent Compliance, Audit and Risk management Functions to help evaluate the Bank's Compliance with applicable Anti Money Laundering laws, rules and regulations.
- The Bank relies on those closest to our customers - The Relationship Mangers, Branch Managers ,the Front line Staff ,Tab Account opening Staff , Sales staff etc. to fully understand with whom we are doing business and provide feedback whenever required.
- Conduct "Know Your Customer" (KYC) and ensure that the business we conduct on behalf of our customers is proper and in Compliance with applicable laws and Regulations.
- Development of internal procedures and technology that assists the Bank in monitoring transactions for the purpose of identifying possible suspicious activities, screening against blacklists and regulatory reporting.
- Continuous updating of policies and procedures to ensure that same meets or exceeds applicable norms in the Banking Industry both locally and globally.

- The Bank recognizes and is aware that preventing money laundering and adhering to KYC principles is an ongoing process and that ongoing due diligence is required in order to keep pace with the ever more sophisticated schemes employed by criminals
- The Bank adopts a continuous Risk Based Framework methodology for assessment of Risk and Customer Due Diligence

IT Systems for Transaction Monitoring and Screening

- Cargills Bank is a subscriber to the online date file of World check which is integrated to the Compass AML system and screening of respective parties is via the same.

1.2 The Compliance Structure in the three lines of Defense Model

Compliance Risk is the Risk arising due to non-Compliance with applicable Laws, Regulations and standards including Internal polices. Compliance risks could come in the form of Regulatory, legal, financial and reputational risk.

Cargills Bank employs a three line of defense mechanism in order to facilitate the management of Compliance Risk and is positioned as the second line of defense in the three lines of defense frame work of the Bank.

The Internal Audit Departments acts as the third lines of defense whilst all Business/Operations/Services function as the first line.

2. Introduction to Risk Based Compliance

The Financial Intelligence Unit (FIU) of the Central Bank of Sri Lanka (CBSL) introduced the "Risk Based Approach" by way of CDD Gazette No 1951/13 of January 2016 and Circular No 1/18 with reference 037/05/002/0018/017 dated 11th January 2018.

The risk based approach starts with the identification and assessment of the risk to be managed with taking into consideration its customers, countries /geographical areas, products, services, transaction and delivery channels etc.

The intensity and extensiveness of risk management functions shall be in line with the "risk based approach" and be proportionate to the nature, scale and complexity of the Bank's activities, the customer profile and the money laundering and terrorist financing risk posed to the Bank by way of it's day to day operations .

The Bank has already taken appropriate steps to identify, assess and manage its money laundering and terrorist financing risks in relation to its customers, based on countries or geographical areas, products, services, transactions and delivery channels.

The Risk based compliance Circular is attached hereto marked **Annex 01**

3. Definitions

3.1 What is Money Laundering?

Definition of "Money Laundering"

"The process of converting cash or other property which is derived from criminal activity so as to give it the appearance of having been obtained from legitimate source" or "the act of concealing the transformation of profits from illegal activities and corruption into evidently "legitimate" assets"

The Process of Money Laundering

There are, theoretically four factors that are common to Money Laundering operations:

- The real source of criminal money must be concealed and not be done without public knowledge.
- The form in which money is held must be changed in order to hide its identity.
- The trail of transaction must be obscured to defeat any attempted follow-up by law enforcement agencies.
- The launderer must maintain constant control on the monies as he cannot legally declare any theft/loss of such money.

Stages of Money Laundering

Money Laundering occurs in three (03) stages

- Stage 1- Placement

This is the first movement of cash from it's source, as such placement means the consolidation and placement of different proceeds of criminal money in the financial system through different sources, or smuggling them out of the country. The objective of the launderer is to remove the proceeds of the illegal transaction to another location without detection and to transform them into transferable assets.

- Stage 2 - Layering

The Launderer by moving the money through many accounts, through different countries and through dummy companies creates complex layers of transactions to disguise the trail and provide anonymity. This process will distance his deeds from his gains and obliterate the path of movement of funds.

- Stage 3 - Integration

Once the money has been cleaned through the first two processes, "washed" or "cleaned "funds are brought back into circulation

Example of a typical flow chart of Money Laundering

3.2 What is Terrorist Financing?

In Terms of the Law, Terrorist Financing is any person who commits an offence within the meaning of the applicable laws if that person by any means, directly or indirectly, unlawfully and willfully provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature

or context, is to intimidate a population, or to compel a Government or an International Organization to do or to abstain from doing any act, is considered culpable of the offense.

4. AML /CFT Compliance Governance

4.1 Bank Responsibilities in the Terms of Governance aspect

- Screening is to be conducted on all persons prior to been recruited by the Bank and relevant document such as Police Report, Grama Sevaka Report , CRIB Reports Referral confirmation etc., as may be decided by the Banks Human Resource Department, in line with Banks Recruitment policy is to be obtained.
- The Bank shall appoint a dedicated Compliance Officer in terms of Section 14 of the FTRA, who shall be responsible for ensuring the Bank's Compliance with the requirements of the relevant laws. This Officer will be at the senior management level in the organization structure of the Bank and will be required to report to the Board Integrated Risk Management Committee.
- The Bank to have an Internal Audit function to test all procedures and Systems from an independent aspect for Compliance as a third line of defence for the Bank.

4.2 Board of Directors

Shall be Responsible for following

- Developing and maintaining an AML policy in line with evolving statutory and regulatory obligations.
- Ensure that the Bank develops AML Compliance procedures on applicable regulations on combating Money Laundering/Terrorist Financing and ensuring that the staff keep up to date with new money laundering requirements and developments.
- Ensuring that staff are aware of their obligations in complying with the Bank's policies and procedures.
- Ensure that staff are adequately trained in combating money laundering and Terrorist financing and a mechanism be established to communicate all relevant changes of related laws.

- Seeking from the Compliance Division, at least annually, a report relating to the Bank's Compliance with its Anti-Money Laundering obligations and a Compliance Risk Assessment.
- Ensuring that the Screening process is in place and carried out at the time of appointing or hiring of all employees whether permanent, contractual or outsourced.
- Appoint a senior management level Officer as the Compliance Officer who shall be responsible for ensuring the Financial Institution's Compliance with the requirements of the AML laws and rules and regulations.
- Ensure that the Compliance Officer or any other person authorized to assist him/her or act on his/her behalf, has prompt access to all customer records and other relevant information which may be required to discharge their functions.

4.3COMPLIANCE OFFICER (CO)

It is mandatory to appoint a Compliance Officer who shall be Responsible for ensuring the Institution's compliance with regulations relating to Anti Money Laundering and Prevention of Terrorist Financing and to act on his/her own authority. The Compliance Officer would further co- ordinate matters with the Financial Intelligence Unit (FIU) of Central Bank of Sri Lanka (CBSL) and any Law Enforcement Authority accordingly.

The Compliance Officer appointed by the Bank will be a Key Management Personnel (KMP) category staff member of the Bank and required to obtain fit and proper certification from the Central Bank of Sri Lanka

Compliance Officer shall be Responsible For/to

- Develop and implement a comprehensive AML and KYC policy and Customer Due Diligence Procedures.
- Frequently design and implement suitable training programs for relevant employees including the Board of Directors, in order to effectively implement the regulatory requirements and internal policies and procedures relating to money laundering and terrorist financing risk management.

- Shall develop requirements relating to CDD and ensure that methods are in place to identify any unusual transaction/s and/or transaction pattern which need to be vigilant of and eligible to be reported as suspicious transactions
- Ensuring that all departments of the Bank are complying with the policy by way of conducting monitoring, testing and reviews
- Ensure a Compliance report is submitted to the Board of Directors at least annually and to the Risk Committee at appropriate intervals
- Undertaking internal reviews of all suspicions and determining whether or not such suspicions have substance and require disclosure to the FIU at CBSL.
- Obtaining and making use of national and international findings concerning Countries with serious AML deficiencies/Sanctions and informing relevant parties of the Bank.
- Adopt the Three line of Defense Framework and carry out the Compliance responsibilities applicable to the second line of defense
- Roll out the Risk based approach for Customer Due Diligence (CDD) and KYC procedures and Implement Risk Profiling of customers of the Bank
- Ensure that AML related mandatory reporting to the FIU is Carried out in accordance with applicable Laws and Regulations

4.4 Branch Managers/ Business Unit Heads/Department Heads

- Branch Managers/BU heads are responsible for day to day Compliance with Anti Money Laundering obligations within all segments of the Bank.
- Ensuring that the Compliance Officer is provided with prompt notification of unusual suspicious transactions and other matters of significance relating to Money Laundering and/or Terrorist Financing.
- Ensuring that all staff members are aware of their obligations and the Bank's procedures, and that staff are adequately trained in the area of Anti Money Laundering
- Ensure that all AML breaches including KYC and CDD matters are brought to the notice of the Compliance Officer.

4.5Staff Members

- Remaining vigilant to the possibility of ML/TF.
- Complying fully with all AML/CTF Policies and procedures in respect of customer identification, account monitoring, record keeping and reporting, Risk Profiling and CDD
- Reporting all suspicions of Money Laundering and Terrorist Financing to the Compliance Officer
- All staff are required to read, understand and then accept the AML/CFT policy on an annual basis. Compliance Department along with the Human Resources Department follows up to ensure that all staff comply to this requirement.
- Employees are aware that those who violate any of the regulations or the policies /procedures outlined on AML/CTF, will be subject to disciplinary action on per the Human Resource Policy Frame Work of the Bank.
- All staff are mandatorily required to complete both the e learning module and the respective evaluation on an annual basis. The Compliance Department together with the HR Division follows up to ensure that all staff comply to this requirment
- All staff of the Bank are required to read and understand the Compliance Manual which is available on the Bank's intranet.
- Reports on the E-learning and Acceptance of Policy to be periodically tabled to BIRMCand the Board.

Compliance is Everyone's Responsibility

5. Legal framework for Anti Money Laundering (AML) / Combating of Financing Terrorism (CFT) in Sri Lanka

For several years government authorities, the Central Bank of Sri Lanka, Financial Sector Authorities and other Legal and Law Enforcement Authorities have worked together with the national experts to formulate the necessary AML/CFT legal framework for Sri Lanka.

The first piece of legislation, the Convention on the Suppression of Terrorist Financing Act, No.25 of 2005 became law on 8th August 2005.

The other two laws, the Prevention of Money Laundering Act No.5 of 2006 and the Financial Transactions Reporting Act. No.6 of 2006 became law on 6th March 2006.

5.1 Prevention of Money Laundering Act (PMLA) NO 05 of 2006

The offence of Money Laundering is defined as receiving, possessing, concealing, investing, depositing or bringing into Sri Lanka, transferring out of Sri Lanka or engaging in any other manner in any transaction, in relation to any property derived or realized directly or indirectly from "Unlawful Activity" or proceeds of "Unlawful Activity".

Under the Prevention of Money Laundering Act (PMLA) Persons who commit or have been concerned in the commission of predicate offences, and thereby come into possession or control of property derived directly or indirectly from the commission of such predicate offences will be held accountable and responsible for Money Laundering

Predicate offences have been set out as offences under the following;

- The Poisons, Opium and Dangerous Drugs Ordinance
- Any law or regulation for the time being in force relating to the prevention and suppression of terrorism;
- The Bribery Act
- The Firearms Ordinance the Explosives Ordinance or the Offensive Weapons Act, No. 18 of 1966.
- The Exchange Control Act (now replaced by the Foreign Exchange Act)
- An offence under section 83C of the Banking Act, No. 30 of 1988
- Any law for the time being in force relating to transnational organized crime

- Any law for the time being in force relating cyber-crime;
- Any law for the time being in force relating to offences against children
- Any written law for the time being in force relating to offences connected with the trafficking or smuggling of person
- The Customs Ordinance and any Regulation
- The Excise Ordinance and any Regulation
- The Payment Devices Frauds Act,
- The National Environmental Act, No. 47 of 1980 and any Regulation,
- An offence under any other written law for the time being in force which is punishable by death or with imprisonment for a term five years or more.

5.2 Financial Transaction Reporting Act (FTRA) NO.6 Of 2006 (FTRA)

The FTRA provides for the setting up of a Financial Intelligence Unit (FIU) as a national central agency to receive, analyze and disseminate information relating to Money Laundering and Financing of Terrorism.

The FTRA obliges institutions, to report to the FIU - Cash Transactions and Electronic Fund Transfers above a value prescribed by an Order published in the Gazette. The term "Institutions" covers a wide array of persons and entities. Currently the reporting threshold has been set as amounts Rupees One Million or above (Rs. 1,000,000/-) or its equivalent in any designated foreign currrency

The Bank's Compliance Department is responsible to collate the report and submit it bi- monthly to the Financial Intelligence Unit of Sri Lanka (FIU).

All suspicious transactions need to be reported by the Bank to the FIU irrespective of their magnitude.

5.3 Convention on the Suppression of Terrorist Financing Act NO. 41 Of 2011

On 10th January 2000, Sri Lanka became a signatory to the International Convention for the Suppression of Terrorist Financing adopted by the United Nations General Assembly on 10/01/2000 and ratified same on 8/9/2000. The Convention on the Suppression of Terrorist Financing Act. No.25 of 2005 was enacted to give effect to Sri Lanka's obligations under this Convention and was further amended under Act no. 41 0f 2011.

Under the Act, the provision or collection of funds for use in terrorist activity with the knowledge or belief that such funds that could be used for financing a terrorist activity is an offence.

6. Financial Intelligence Unit Guidelines

Rules are made by the Financial Intelligence Unit of Sri Lanka and the most recent rules were issued by virtue of Circular No 1/18 with Ref: 037/05/002/0018/017 dated 11th January 2018 and is referred to as "Guidelines on Money Laundering and Terrorist Financing Risk Management for Financial Institutions No 1 of 2018"

The previous set of rules issued by the FIU were by way of gazette 1951/13 issued on 27th January 2016 and referred to as the "Financial Institutions Customer Due Diligence Rules, No. 01 of 2016.These rules were issued under Section 2 of the Financial Transactions Reporting Act No.6 of 2006 and any contravention of, or non-Compliance with the same will be liable to the penalties under the relevant provisions of the Act

The Cargills Bank General Circular on Account Opening, KYC and CDD has been prepared taking cognizance of same - Please refer Annex 02

7. Customer Due Diligence – Overview

7.1 What is Customer Due Diligence?

All Banks are required to implement a Customer Due Diligence programme (CDD). The regulatory expected outcomes of a Customer Due Diligence program is each Bank, including Cargills Bank should be satisfied that its customers are who they say they are, understand whether its customers are acting on behalf of others and the identity of any beneficial owner(s), and understand its customers' circumstances to guard against the being used for fraud, money laundering or other criminal activity.

Cargills Bank, along with all other regulated Banks, carry out Due Diligence on their customers to obtain this information and reach this level of comfort. The steps in the Risk Based Due Diligence Process consists of five different aspects.

i. First Step - Identifying the Customer

The Bank needs to obtain the information to establish to their satisfaction the identity of the customer and the intended nature of the business relationship. There are no exceptions to this requirement.

Further details covering this requirement are set out in the Bank's account opening circular - Annex 02 hereto. It shall be the primary responsibility of the employee opening the account to conduct KYC/CDD, and obtain and verify the authenticity of the identification documentation in terms thereof.

ii. Second Step - Verifying the Customer's Identity

In some cases, the information must then be verified. Information on the customer is obtained directly from the customer and at times from other external sources. Irrespective of how or where the identification information is obtained, a determination must be made whether the information needs to be verified. Verification for this purpose means the information is verified from reliable, independent third-party source(s), and original document being sighted and copies retained been certified as such.

iii. Third Step - Customer KYC Information

In most cases it will be appropriate to know more about the customer than just the identity. For example, there is usually the need to be aware of the nature and scale of business the customer is engaged in and the and surrounding circumstances in addition to the source of funds and/or wealth. This will allow the Bank to assess the extent to which the customer's transactions and activity with Cargills Bank are consistent with the customer's legitimate business. For these purposes, this additional information will be the customer KYC information.o

The extent of KYC information to be obtained by the Bank will depend on the ML/TF Risk Assessment performed by the Bank to ascertain the level of ML risk posed by the customer. In addition to the Local regulators, all major international organizations set out the need to obtain sufficient KYC information , adopting a Risk based focused framework for CDD and to give the appropriate weightage to each risk factor it deems necessary.

iv. Fourth Step - Obtaining information on the purpose and intended nature of the business relationship

It is important to get information on the purpose and intended nature of the business relationship so as to be able to establish what business the customer is involved in and be able to create a risk profile of the customer. This is essential in order to be able to identify any suspicious activities that seem to be unrelated or not in line with the customer's legitimate business.

v. Fifth Step - Conducting ongoing monitoring of the business relationship

Ongoing monitoring on customers and their transactions is required by the Regulator and is important in order to detect any suspicious activity not only at the inception of a business relationship or at the occurrence of an occasional transaction but also at later stages throughout the duration of the Business relationship.

7.2 Responsibility for Conducting Customer Due Diligence

Responsibility within Cargills Bank for conducting the Customer Due Diligence rests with the respective Cargills Relationship Manager /Sales staff/Channel/Tabz and other staff members

within the Cargills Bank as ,he who opens the account and manages the relationship retains primary responsibility for the customer relationship and KYC requirements.

7.3 High Risk Situations

High Risk Jurisdictions

Responding to the threat posed by high-risk and non-cooperative jurisdictions a key objective for promoting the global implementation of AML/CFT standards worldwide-

Compliance with the standards protects the integrity of the international financial system and enhances international co-operation on AML/CFT.

The Bank takes Cognizance of the following

- Jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures apply.
- Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progressing addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies.

7.4 Alternative Remittance Systems (Hundi, Hawala etc.)

Extra vigilance is required by the Bank to distinguish between formal money transmission services and other money or value transfer systems through which funds or value are moved from one geographic location to another through informal and unsupervised networks or mechanisms. This is required in order to ascertain the sources of such funds and the legitimacy of the transaction/s.

7.5 Correspondent Banks and Remittance Houses and Agents

Prior to commencing Banking relationships with Correspondent Banks, other foreign Financial Institutions, Remittance Houses or Agents, the Bank should gather sufficient information with regard to their Ultimate Beneficiary Owners and shareholders, management, major business activities and licenses and, money laundering prevention and detection efforts. It is also the duty of the Bank staff to ensure that the purpose of the account is exclusively for Correspondent

Banking /Remittance activities and that the Bank is effectively supervised by the relevant authorities for their Due Diligence and AML standards in the country they operate.

Cargills Bank will refuse to enter into, conduct business and/or provide services to such institutions that are located in jurisdictions that have poor KYC standards or have been identified as being 'non-co-operative' in the fight against Money Laundering (ML) and Terrorist Financing (TF). It is also imperative that the Bank staff ensure that their Correspondent Financial Institutions/Remittance House/Agents do not undertake business with Shell Financial institutions.

At the onset of relationships a comprehensive completed questionnaire covering AML/CFT/KYC and CDD will be obtained from all Correspondent Banks/Financial Institutions/Remittance Houses and Agents.

Please refer Annex 2 - Master Account Opening Circular to which is annexed the list of documents to be obtained from Correspondent Banks prior to initiating a relationship.

7.6 Shell Banks

Cargills Bank Shall not conducts business with Shell Banks/Shell Companies and/or Institutions. It is our policy to prohibit offering any Service to Shell Banks and Companies.

It is also imperative that the Bank staff ensures that their Correspondent Financial Institutions/Remittance partners do not undertake business with Shell Financial Institutions, and other shell companies. If any information pertaining to doing business with Shell Banks/Company is received, the matter should be brought to the immediate attention of the Bank's Compliance Officer.

7.7 Treasury Dealings

With regard to dealings in Forex, money market, bonds, securities, precious metals etc. confirmations should be obtained from the counter-parties on their adherence to AML/CFT guidelines to prevent transactions with non-Compliant countries/entities.

7.8 Trade Finance/Letters of Credit and other contingencies

Trade-based Money Laundering and Terrorist Financing usually involves invoice manipulation and uses trade finance routes and commodities to avoid financial transparency, laws and regulations.

The use of these facilities need to be reviewed from time to time by the Trade and Relationship/Branch staff. Facilities requested by customers who have borrowing facilities or large deposits with other institutions should be brought under close scrutiny.

All trade facilities/services shall only be offered to customers who maintain accounts with the Bank and whose KYC is in place and subject to Enhance Due Diligence.

7.9 Agents and Service Providers

Cargills Bank shall maintain a current list of all its Agents and Service providers in all countries in which the provider and its agents operate.

Bank must ensure every Agent and service provider are Compliant with the Bank's policy on Anti-Money Laundering and Suppression of Terrorist Financing.

The Bank needs to further ensure that every service provider and agent have undergone full KYC and CDD at the time of onboarding and commencement of business relationship

Any deviations to the Bank's AML policy is to be reported to the Bank's Compliance Officer no sooner the same is brought to light.

8. Suspicious Transaction/Business

Whilst all unusual transactions are not automatically linked to Money Laundering, unusual transactions become suspicious if they are considered inconsistent with a customer's known legitimate business, personal activities or with the normal business for the type of account created.

The following are some – but certainly not all areas where staff should remain vigilant to possible Money Laundering situations. The fact that any of the following do occur does not necessarily lead to a conclusion that Money Laundering has taken place, but they could well raise the need for further enquiry. A key to recognizing suspicious transaction/transaction patterns is to know enough about the customer to recognize if they are unusual for that particular customer.

While the following provide some examples, recognizing suspicious transactions is a matter of good sense and attention to detail by all staff of the Bank

8.1 Suspicious Cash Transactions

- Unusually large cash deposits made by an individual or a company whose normal business activities would mainly be conducted by cheques or other instruments.
- Substantial increase in cash deposits by any customer without an apparent cause, especially if such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customers.
- Customers who deposits Cash in numerous stages so that the amount of each deposit is small, but the total of which is equal to or exceeds the reporting threshold amount.
- Customer accounts whose transactions, both deposits and withdrawals are mainly conducted in cash rather than in negotiable instruments (e.g. cheques, letters of credit, draft etc.) without an apparent reason.
- Customers who constantly pay-in or deposit cash to cover requests for money transfers or other negotiable instruments without an apparent reason.
- Customers who seek to change large quantities of lower denomination Banknotes for those of higher denomination Banknotes with no obvious reasons.

- Customers who transfer large sums of money outside the country with instructions for payment in cash, and large sums transferred from outside the country in favor of non-resident customers with instructions for payment in cash.
- Unusually large cash deposits using “ATMs” or “cash deposit machines” “Mobile Banking “etc. to if such deposits are not consistent with the business/normal income of the concerned customers.
- Frequent third party cash deposits to the account.
- Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received unexpected large sums of money from abroad.

8.2 Suspicious Transactions using Customer Accounts

- Customers who maintain a number of trustee or customers’ accounts which are not required by the type of business they conduct particularly, if there were transactions which contain names of unknown persons.
- Customers who have multiple accounts and pay-in amounts of cash to each of these accounts, whereby the total of credits is a large amount except, for institutions which maintain these accounts for banking relationships with Banks which extend them facilities from time to time.
- Any individual or company whose account shows virtually no normal personal banking or business-related activities, but is used to receive or disburse large sums which have no obvious purpose or for a purpose not related to the account holder and/or his business
- Customers who have accounts with several financial institutions within the same locality and who transfer the balances of those accounts to one account and subsequently transfer the consolidated amount to a person abroad.
- Paying-in large third party cheques endorsed in favor of the account holder when they do not seem to be relevant to the account holder and his nature of business.
- A large number of individuals who deposit monies into the same account without an adequate explanation.
- Unusually large deposits to accounts that have never witnessed such deposits particularly, if a large part of these deposits are in cash.

8.3 Suspicious Investment Related Transactions

- Purchasing of securities to be held by the financial institution in safe custody, where this does not appear appropriate given the customer's apparent standing. (Financial income etc.)
- Individual or commercial institutions which bring in large sums of money to invest in foreign currencies or securities, where the size of transactions are not consistent with the income of the concerned individual or commercial institutions.
- Buying or selling securities with no justifiable purpose or in circumstances, which appear unusual.
- Investments involving parties that partially/do not comply with AML/CFT guidelines.
- Investments involving parties that have negative news on Worldcheck identified during the Name Screening Process carried out.

8.4 Suspicious Transactions using Electronic Banking Services

- When an account receives numerous small fund transfers electronically, and then the account holder carries out large transfers in the same way to another account
- Where a customer makes regular and large payments using different means including, electronic payments that cannot be clearly identified as bona-fid transactions, or receive regular and large payments from countries known for serious criminal activities.
- Where transfers from abroad, received in the name of a customer of the Banker any financial institution electronically are transferred abroad in the same way without passing through an account (i.e. they are not deposited then withdrawn from the account). Such transactions should be registered in the account and should appear in the account statement.

8.5 Suspicious International Banking and Financial Transactions

- Customers introduced by a Bank outside the country, an affiliate or another Bank, based in one of the countries known for the production or consumption of drugs or other serious criminal activities.
- Building up of large balances not consistent with the known turnover of the customer's business and the subsequent transfer to account(s) held abroad.

- Frequent requests for foreign currency drafts or other negotiable instruments, for no obvious reason.
- Frequent paying-in of foreign currency drafts in large amounts for no obvious reasons, particularly if originating from abroad.

8.6 Suspicious use of Letters of Credit (LC)

- Where the applicant of LC (customer of Bank) and the beneficiary of LC are same individuals/ entities.
- Where the Bank's customer who opens these letters is the beneficiary and the owner of the shipping company.
- Where amounts on letters of credit submitted by the customer to the Bank and to the Customs/Ports/Airport authorities do not match the original.
- Where the size of the facilities are not in line with the securities on hand, nature of business and net-worth of the customers.
- Where such trade is not consistent with the customer's usual business.

8.7 Suspicious Loan Transactions:

- Customers who repay loans before the expected time and in larger amounts than anticipated.
- Customers who request loans against assets held by the financial institutions or third party, where the origin of these assets is not known, or the assets are inconsistent with the customer's standing.
- Non-resident individuals who request loans secured by Bank guarantees issued by foreign Banks where the purpose of the transaction is questionable.
- Loan transactions against pledge of deposits with financial institutions outside the country, especially if these were in countries known for the production, processing or consumption of drugs or other criminal activity

9. Recognizing and Reporting Of Suspicious Transactions

In accordance with the local Laws and regulations it is an offence to fail to report suspicion of Money Laundering and/or Terrorist Financing. Failure to report such circumstances is punishable on conviction for heavy fines and/or imprisonment.

9.1 How to report a Suspicious Transaction

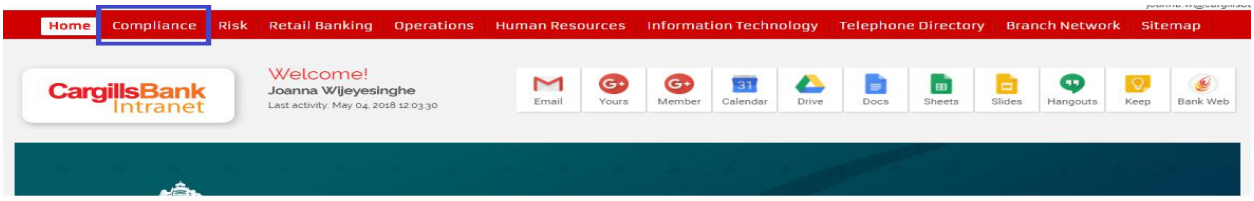
To reiterate, the law requires all employees of the Bank to report any reasonable suspicion that they may have about a customer or his/her transactions. The law also requires the Bank to have appropriate effective reporting procedures in place. It also requires that all employees follow these procedures using them correctly as they are intended to be used.

Reporting Procedures

1. Completing the STR form made available on the Bank's intranet

Any staff member who identifies a suspicious transaction/customer and deems it required to be reported to the Bank's Compliance Department could download the STR format made available on the Bank's intranet and forward the same to Compliance marked "Confidential"

The format is to be found as shown below



Master circular on Account opening Circular (Annexure 01).pdf View Download	782k	v. 1	Aug 14, 2017, 3:10 PM	Anne Denis
PEP Local list Memorandum.pdf View Download	1495k	v. 2	Mar 3, 2017, 2:21 PM	Tilantha Gunatilaka
Related Party Transaction Policy.pdf View Download	678k	v. 1	Feb 5, 2018, 2:03 PM	Anne Denis
Risk Based Approach Circular (Annex 02).pdf View Download	863k	v. 1	Aug 14, 2017, 2:21 PM	Anne Denis
Suspicious Transactions Report-(Annex 04) (3) (1) AMLCFT Policy.pdf View Download	185k	v. 1	Aug 24, 2017, 2:55 PM	Dilani Perera
PRODUCT NOTES - NEW FOREIGN EXCHANGE ACT				
Business Foreign Currency Accounts_BFCA.docx View Download	23k	v. 2	Feb 5, 2018, 3:20 PM	Anne Denis
CTRA Explanatory Note.docx View Download	502k	v. 2	Feb 5, 2018, 3:20 PM	Anne Denis
DFA Product Note.docx	23k	v. 2	Feb 7, 2018, 4:40 PM	Rashika Daniel

CONFIDENTIAL

Kindly fill in CAPITAL. Read the instructions before filling the form.

PART A: DETAILS OF REPORT	
1.1 Date of sending report	
1.2 Is this a replacement to an earlier report? ☐No	
1.3 Date of sending original report if this is a replacement report	N/A

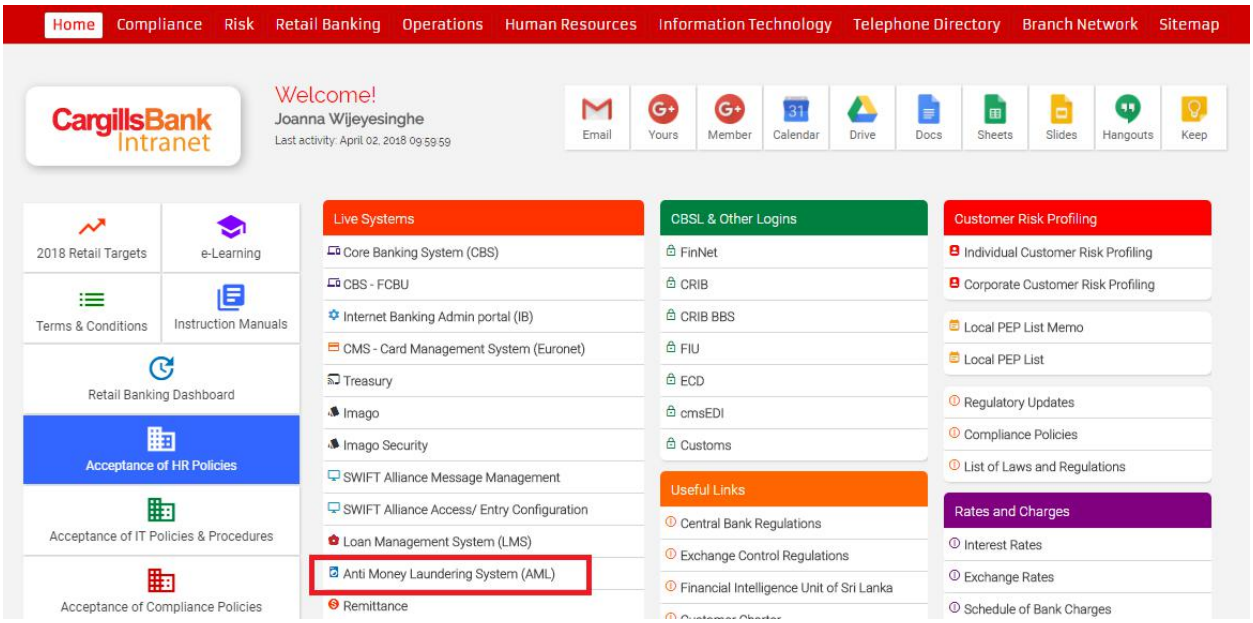
PART B: INFORMATION ON CUSTOMERS					
a)	Account Holder				
1.	Name in full (if organization, provide registered business/organization name)				
2.	NIC No./ Passport No./Nationality/Business Registration No.				
3.	Gender	Male		Female	
4.	Country of Residence				
5.	Business/ Employment Type				
6.	Occupation (Where appropriate, principle activity of the person conducting transaction				
7.	Occupation Description				
8.	Name of Employer (Where applicable)				
9.	Residential/Registered Address				
10.	Country				
11.	Details of Other Business/Related Accounts	**Existing A/c.**	**Date Opened**	**Balance**	
12.	Telephone No.				
13.	Date of last review of customer details				
Brief description of customer's relationship with the bank					
b. Person conducting suspicious transactions (If not, the holder in what capacity)					
14.	Name in Full (If organization, provide registered business/organization name)				
15.	NIC No./ Passport No./Nationality/Business Registration No.				
16.	Gender	Male	MALE	Female	
17.	Country of Residence				
18.	Business/ Employment Type				
19.	Occupation (Where appropriate, principle activity of the person conducting transaction)				
20.	Occupation Description				
21.	Name of Employer (Where applicable)				
22.	Residential/Registered Address				
23.	Town				

7

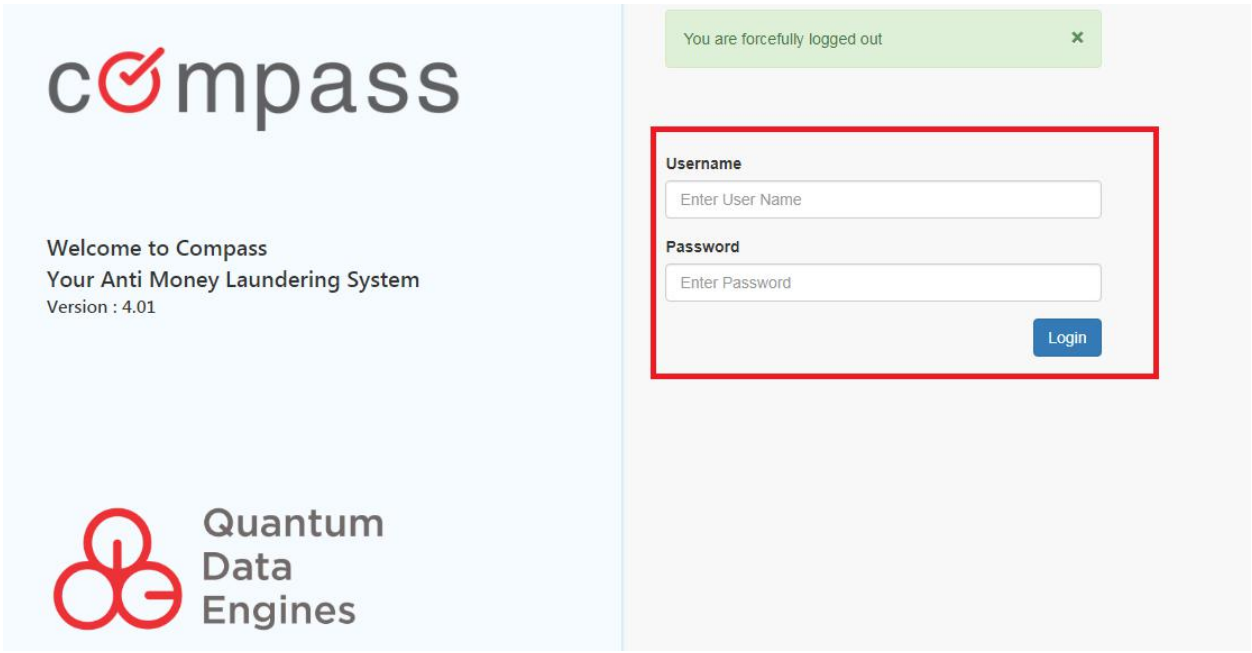
Please refer Annex 4 for the STR format.

2. Through the Compass AML system

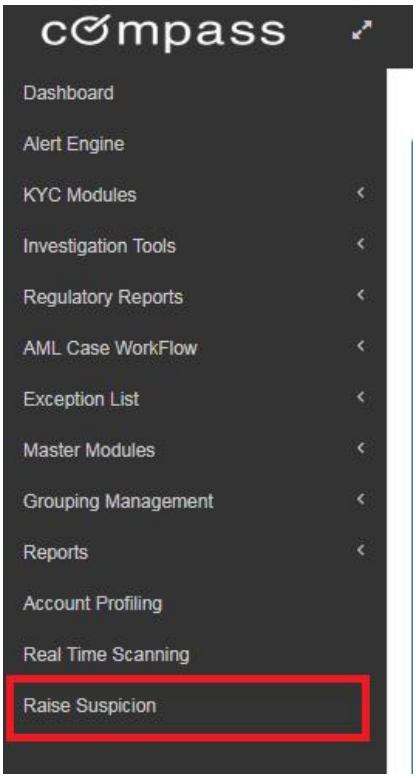
Intranet → Anti Money Laundering Systerm (as shown in the below print screen)



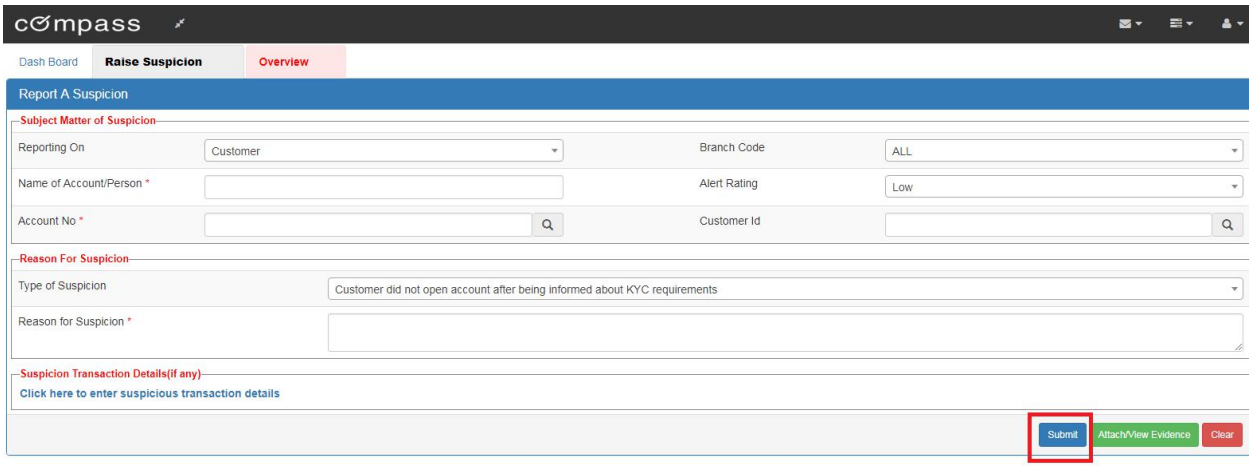
Enter your User ID and Password in the field highlighted in Red



Go to Option “Raise Suspicion”



Provide the requested details in the respective Tab and the click on"Submit"



Efficient reporting procedures and their correct use are required, when suspicious transaction have been identified

- The suspected customer is not alerted
- The matter is dealt with quickly and professionally
- The external authorities are notified and provided with the necessary records, inappropriate

Report your suspicions with supporting information/documents in the format annexed herewith . Staff need to ensure that the supporting information sent is relevant to the suspicion so that it could be passed on to the Financial Intelligence Unit (FIU) of the Central Bank of Sri Lanka.

The report should be sent to the Compliance Officer based at the Head Office in Colombo directly via email and should be followed up with a hard copy of the same been couriered to the Compliance Department in a sealed envelope marked “Confidential”.

Role of the Compliance Officer on receiving the Report

When the Compliance Officer receives the Suspicious Transaction Report, (STR) the Compliance Officer will conduct further Due Diligence and decide whether the report gives rise to knowledge or suspicion that customer is involved in Money Laundering or Terrorism Financing.

If the Compliance Officer believes that the suspicions may be justified and requires further investigation, it must be reported to the Financial Intelligence Unit (FIU) within 2 working days.

The Bank may make further inquiries within the parameters of its own records but it does not need to carry out the more detailed criminal investigations on the suspicion raised. It is the responsibility of the law enforcement agencies to do so. If the Authorities feel the report is worth further investigation, they would conduct same.

The employee has a duty to assist the Compliance Officer in reporting the STR, by making sure that the information provided –

- Describes why there are reasonable grounds for suspicion and what they are
- Contains accurate information
- Is timely and not delayed

9.2 The importance of timing

It is very important that there is no delay in reporting. It is the duty of all employees to report suspicion as soon as they have established reasonable grounds, and collected the relevant supporting material.

Further, the consequences of not reporting suspicions immediately to the Compliance Officer could be serious for the employee involved and may include individual fines, imprisonment, or both as set out in the legislation and disciplinary action as per the Cargills Bank policy.

9.3 Tipping Off

Duty of the staff members reporting the suspicion or those aware of the suspicion is not to divulge information to other members of staff or any others including the respective customer/entity and report only to the Bank's Compliance Officer Or her designate.

The Bank will protect persons reporting suspicious transactions if done in good faith and compliance with regulations under the Applicable Laws and Regulation and Directions of FIU, issued from time to time.

The Financial Transaction Reporting Act (FTRA) makes "tipping-off" an offence under the Act (e.g. pre-warning a suspect of an impending Investigation).

In terms of the FTRA, persons making reports under the Act are protected from civil or criminal liability.

Under no circumstances should the customer know that they have been reported for the activity, or that an investigation is underway or may be underway.

This does not mean that the Bank cannot ask the customer for an explanation, or continue to provide them with a normal customer service. But it does mean that the Bank must do so without alerting them to the fact that the Bank may or had already notified the Authorities of suspicion on the transaction carried out by him/her ot the entity. If customers being investigated are alerted, the Bank could be blamed for tipping them off, which is a criminal offence for the individual who alerted the customer to the existence of an actual or potential investigation.

TIPPING OFF A CUSTOMER IS AN OFFENCE

9.4 Sanctions and Name Screening

The Bank is subject to the provisions of various Sanctions programs administered, including those implementing measure circulated by the local and applicable global regulators, financial markets and the industry it operates.

Where such Sanctions or measures have not yet been implemented into legislation at the national level or otherwise in terms of statutory requirements, guidance should be sought from the authority/is about the observance steps to be taken.

Cargills Bank needs to be in compliance with all Directions issued by the FIU on complying with UNSCR, OFAC, UN, EU and all other globally, mandated sanctions lists. Responsibility within Cargills Bank for checking names against sanctions lists or similar restrictive measures rests with the respective Branch/Departments using the screening system subscribed by the Bank.

Please refer Annex 3 for the Procedure Manual on Name Screening

9.5 Bank's Internal Blacklist

Cargills Bank creates CIFs in it's Core Banking System for individuals/entities inquired by the FIU and other Regulatory Authorities of the country and tags them as "Suspicious Customers". New individuals/entities onboarded by the bank are screened against the same and any hits identified are referred to the Compliance Department prior to proceeding with on-boarding.

10. Independent Audit Testing

Bank has entrusted Internal Audit Department with the responsibility to test the implementation and adherence of the Banks KYC/AML Policy. This examination is required to be conducted as part of the audit plan of the Internal Audit Department..The findings/recommendations should be reported directly to the Board Audit Committee.

11. Compliance Monitoring and Testing

The Compliance Department also carries out reviews and testings to verify among other things the implementation and adherence of the AML Policy and related circulars in the Bank and report any non-Compliances to the Board. The reviews are conducted on a risk based approach as per the BIRMC approved compliance programme/plan.

The Compliance function shall monitor and test Compliance by performing sufficient and represented testing based on a Risk methodology adopted. The reports should be submitted to the BIRMC

The reports should cover the risk assessment, the breaches and deficiencies identified and corrective measures recommended. These should be clearly tracked and monitored for completion. The annual Compliance Plan approved by the BIRMC and program for monitoring and testing should set out the risk analysis and Identification.

12. Record Keeping Obligations

In addition to regular Bank record keeping requirements, the Bank's policy under Money Laundering requires that documents concerning customer identification and records relating to transactions undertaken on behalf of customers/non customer (all transactions including cash, wire transfers, purchases/sale of monetary instrument etc.) be maintained for a period of 6 years from the closure of the account enabling to provide a clear audit trail in the event of an investigation.

It is also required that:

- All Anti-Money Laundering monitoring reports made by the Compliance Officer and records of consideration on those reports and of any action taken as a consequence including reporting done to management/auditors/regulators be maintained for a 6 year period for future reviews.
- Records showing the dates of Anti-Money Laundering training and the names and acknowledgement of the staff receiving the training are maintained for a 6 years period.
- All records maintained should be available to authorized persons promptly on request without undue delays

13. Dissemination of New Laws and Regulations

All New Direction and Regulations Received by the bank pertaining to AML/KYC and CDD or related –either to the CEO/MD's office or to any other department should be sent to the Head of Compliance/Compliance Department without delay. These are then required to be forwarded to the applicable respective Business Unit Heads for further action, and subsequently be included on the Banks Intranet for easy reference to all staff. The Head of Compliance shall also include the new laws and Directions amendments as part of the Monthly Compliance Board Papers, for the information of Board members and presented to the Corporate Management for discussion at the monthly management meeting.

14. Training to Staff members (KYC/ AML/CDD)

The Bank shall ensure that the training sessions on KYC guidelines and AML procedures are included in the Training Calendar on an ongoing basis for all staff and Agents of the Bank. The Bank shall arrange to update and modulate these training sessions to the requirements of front line staff, Compliance staff and counter-staff sales staff/Agent staff dealing with customers. It shall be the Bank's focused endeavor to make all those concerned fully understand the rationale behind the KYC and AML procedures and implement them consistently.

Transaction monitoring with a view to detect suspicious cases is the most crucial problem any comprehensive Anti-Money Laundering measures must address. This fact will be dealt with at all training and education sessions

Branch Managers and Heads of Department should additionally educate employees coming under their purview of the importance of KYC and CDD and the requirements on Customer Identification. Special emphasis must be made to train the Account Opening Officers in this regard. An E-learning module has been included in the training calendar of Cargills Bank and all Department Heads and Branch Managers shall ensure that all operational and Front Office staff have gone through same and are familiar with the provisions therein.The E-learning module will be periodically reviewed and updated by the Compliance Department. A report on the training completion records will be presented to the BIRMC/Board Bi-Annually.

15. Customer Education

- In order to educate customers on KYC requirements and the need for seeking certain personal information from the customers/applicants for opening accounts as also to ensure transparency, the Bank shall publish this Policy in the Bank's web-site and place a copy of the same in all branches/offices for reference of the Customer.
- It is the duty and responsibility of Staff to educate the customers and tactfully/convincingly explain the need for customer profile and its relevance in the present adverse conditions of Money Laundering etc. The customers shall be impressed upon the fact that the profile format additionally enables the branch to render better Customer Service.
- An initial resistance by the customers to fill up the exhaustive customer profile formats are an expected initial response and it is foreseen as a temporary phenomenon only. The expected resistance could be overcome if the background could be explained to the customers so that the required information can be gathered.
- Bank shall endeavor to guard against denial of banking services to general public especially to those who are financially/socially under-privileged due to the implementation of Customer Acceptance Procedures on too restrictive basis.

16. Breach of policy

Failure to abide by the Bank AML /CFT policy leads to loss of confidence in the Bank's integrity and fair dealing, severe impact on the Bank shareholders, customers, and the relevant regulatory bodies, and market, and significant adverse publicity and reputational damage, even if no law was broken. As a result, management will take appropriate corrective action in the scope of laws, policies and procedures when breaches of laws, rules and standards are identified that might include "Disciplinary Action", and "Termination of Employment".

Staff members who become aware of breaches of this policy shall raise/escalate such breaches through the procedure laid down in the Cargills Bank Whistle Blowing Policy.

17. Communication of Policy

The Policy will be published on the Bank's Intranet and a cover note will be circulated by AGM Compliance to all staff notifying that the Policy has been reviewed and updated and that all staff are required to read and understand the contents thereof and acknowledge same through the online portal made available on the Bank's Intranet as set out in section 4.5 of this Policy.