AML MANUAL OF NEXT LAYER

Title	**ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM (AML / CFT) Policies and Procedures**
Department	Compliance Department
Information Classification	Public
Policy Supported	Next Layer - Compliance Program
Current version	1.1
Review Cycle	Annually
Due Date for Review	June 2024

POLICY APPROVAL

The undersigned acknowledge that they have reviewed the Next Layer AML/CFT Policies and Procedures and agree with the approach it presents. Any further changes to this Policy in future can only be recommended by the Compliance Officer/ General Manager/ Director/ CEO

	Name and Designation	Date	Signature
Prepared by	Compliance Officer:	05/16/2023	
Reviewed by	General Manager:	05/16/2023	
Approved by	Director Investment & Business Development:	05/16/2023	

POLICY VERSION CONTROL REVISION - Revision History

Ver.	Policy Name		Reason for Implementation	Next Scheduled Review Date
1.0	AML/CFT Policies and Procedures		AML/CFT Laws/ FATF	June 2024

TABLE OF ACRONYMS

ACO Alternate Compliance Officer

AML/CFT Anti-Money Laundering and Countering the Financing of Terrorism

Bank Secrecy Act BSA For Anti-Money Laundering and Countering the Financing of Terrorism Act, as amended.

AML/CFT Regulations Anti-Money Laundering and Countering the Financing of Terrorism Regulations

CDD Customer Due Diligence

CO Compliance Officer

CTTR Cash Transaction Threshold Report

EDD Enhanced Due Diligence

FATF Financial Action Task Force

FIU Financial Intelligence Unit

Manual AML/CFT Compliance Manual

ML Money Laundering

STR Suspicious Transaction Report

TF Terrorism Financing

TERMS AND DEFINITIONS

1. Anti-Money Laundering (AML)

AML refers to the procedures, laws and regulations designed to stop the practice of generating income through money laundering.

2. Authorised Officer

A law enforcement officer of the Police Force
An officer of the Anti-Corruption Commission of and
An officer of the Revenue Commission.

3. Beneficial Owner

Beneficial Owner means a natural person or persons who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted and includes those persons who exercise ultimate effective control over a legal person or arrangement.

4. Beneficiary

Beneficiary includes a natural person or a legal entity or arrangement, who received money or benefits from a benefactor.

5. Cash

Cash includes notes and coins in or of any other country which is a legal tender and accepted as a medium of exchange in the country of its issue, postal orders, bearer cheques which passes title thereto upon delivery including travellers' cheques, bank drafts and bearer bonds.

6. Cash Transaction Threshold Reports

A report that Reporting Entities are required to file with the FIU when executing cash transactions above the prescribed threshold in terms of the Bank Secrecy Act BSA.

7. Central bank of (CBS)

Supervisor and regulator of Bureau de Change, Commercial banks, Non-Bank Credit Institutions, Financial Leasing institutions, Payment service providers/operators, Non-bank deposit taking Institutions.

8. Compliance Officer (CO)

An official who is responsible for monitoring and reporting suspicions related to money laundering and/or terrorist financing to the FIU.An officer appointed under the Bank Secrecy Act BSA, the supervisory authority.

9. Countering the Financing of Terrorism (CFT)

CFT refers to laws, regulations, and other practices that are intended to restrict access to funding and financial services for those whom the government designates as terrorists.

10. Customer Due Diligence (CDD)

Customer due diligence (CDD) is the act of performing background checks and other screening on the customer to ensure that they are properly risk-assessed before being onboarded. CDD is at the heart of Anti-Money Laundering (AML) and Know Your Customer (KYC) initiatives.

11. Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) is an additional measure applied to know more about the customer and his business activities to confirm purpose & source of funds are legitimate and matches the profile of the customer.

12. Financial Action Task Force on Money Laundering (FATF)

It is an intergovernmental organization founded in 1989 on the initiative of the G7 to develop policies to combat money laundering and terrorist financing.

13. Financial Intelligence Unit of (FIU)

The FIU is responsible for ensuring compliance with anti-money laundering and counter terrorist financing legislation. It acts as the central authority centre for receiving information on suspected money laundering transactions and is responsible for disseminating information to law enforcement and supervisory agencies for prosecution.

14. Know Your Customer (KYC)

KYC refers to the process of collecting and verifying the identity of prospective clients and assessing potential risks when entering a business relationship and thereafter throughout the established business relationship.

15. Politically Exposed Person (PEP)

Politically exposed person (PEP) is a person who has a prominent public function, or a relative or known associate of that person. it can be head of state, political figure,charge de affairs,public office holdersand prominentfigures that have public influence..

16. Reporting Entity

An entity or person specified in the AML/CFT Laws.

17. Risk Assessment

Risk Rating is a scientific method to identify potential risk from customers. It is also known as Risk Based Approach of customer segmentation.

18. Risk Based Approach (RBA)

Risk Based Approach is a process which enables us to identify potential risks based on profiling of the customers/transactions and apply the necessary measures/controls proportionate to the risk identified

19. Shell Banks

Shell banks are banks that do not have any significant office or physical presence and are existing on paper and not regulated by the Central bank of or a foreign regulatory authority.No business shall be done with shell banks and prohibit business with banks that allows it customers to do business with shell banks.

20. Suspicious Transaction Reporting (STR)

A report on an activity or a transaction or series of transactions made, to be made or attempted to be made, by a reporting entity under the Bank Secrecy Act BSA. All suspicious and/or unusual transaction or customers are reported to the FIU.

21. Transaction Monitoring

Transaction monitoring refers to the monitoring of customer transactions, including assessing historical/current customer information and interactions to provide a complete picture of customer activity.

22. Watch list screening

To prevent block identified persons from conducting transactions, international bodies like OFAC UN, EU, UK LIST etc. issue notices / circulars of sanctioned persons. The person / entity / beneficial owner is screened

against such lists.

1. INTRODUCTION

1.1 ABOUT NEXT LAYER

Nextlayer provides IT consulting services to help businesses develop and implement IT strategies that align with their goals and objectives. Their team of experienced IT professionals can provide guidance on everything from cloud migration to cybersecurity and compliance. Located in Sheridan, Wyoming.

1.3 PURPOSE OF THIS POLICY

This Compliance Manual has been established to articulate the commitment of Next Layer management and employees in adopting the highest standards of compliance with relevant legislations; namely the AML/CFT, as amended and AML/CFT regulations which will aid the business house from being used for illegal purposes. The Manual comprehensively explains the various aspects of the Compliance Program that has been adopted by the Company. Failure to comply with the Bank Secrecy Act BSA and Regulations, order, determination, or directive issued under the Act is subjected to sanctions and penalties.

1.4 REVIEW OF POLICY

The Policy will be reviewed annually as of 30th June or even earlier as per changes advised by the regulator / FIU.

1.5 USER OF NEXT LAYER AML/CFT POLICY

This AML / CFT Policy is for use of the CEO, Directors, Partners, and Employees of Next Layer.

1.5.1 Services

Nextlayer's network and security solutions play a critical role in supporting secure and reliable payment transactions. The company's firewall and intrusion detection and prevention solutions help protect clients' data and networks from cyber threats, while its virtual private network (VPN) solutions provide secure remote access to payment processing systems.

Bitcoin wallets are digital wallets used to store, send, and receive bitcoin, a type of digital currency that operates independently of central banks and can be used for online payments. Bitcoin wallets can be software-based, stored on a computer or mobile device, or can be hardware-based, stored on a physical device similar to a USB drive.

To make online payments with bitcoin, a user typically needs to have a bitcoin wallet that contains a sufficient amount of bitcoin to cover the cost of the transaction. The user then sends the bitcoin from their wallet to the recipient's bitcoin address, which is a unique identifier used to receive bitcoin payments.

Many online merchants and service providers now accept bitcoin payments, either directly or through third-party payment processors. Some popular payment processors for bitcoin payments include BitPay, Coinbase Commerce, and GoCoin. These services can help merchants to accept bitcoin payments, convert them to traditional currencies, and manage their bitcoin transactions.

One benefit of using bitcoin for online payments is that it offers a decentralized and secure method of payment that is not subject to the same fees, processing times, or other limitations associated with traditional payment methods such as credit cards or bank transfers. However, the value of bitcoin can be highly volatile, and it may not be widely accepted by all merchants or service providers. Additionally, bitcoin transactions may be subject to certain legal and regulatory requirements, depending on the jurisdiction in which they occur.

2. WHAT IS MONEY LAUNDERING AND FINANCING OF TERRORISM?

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.
Illegal arms sales, smuggling, and the activities of organised crime, including for example drug trafficking and prostitution rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to “legitimise” the ill-gotten gains through money laundering. When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

The Financing of Terrorism is defined as an offence established when a person by means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they will be used in full or in part, in order to carry out a terrorist act or activity.

2.1 STAGES OF MONEY LAUNDERING

Though money or other assets can be laundered by various methods, generally, the process of money laundering comprises three stages, during which there may be numerous transactions that could alert a firm to the money laundering activity:

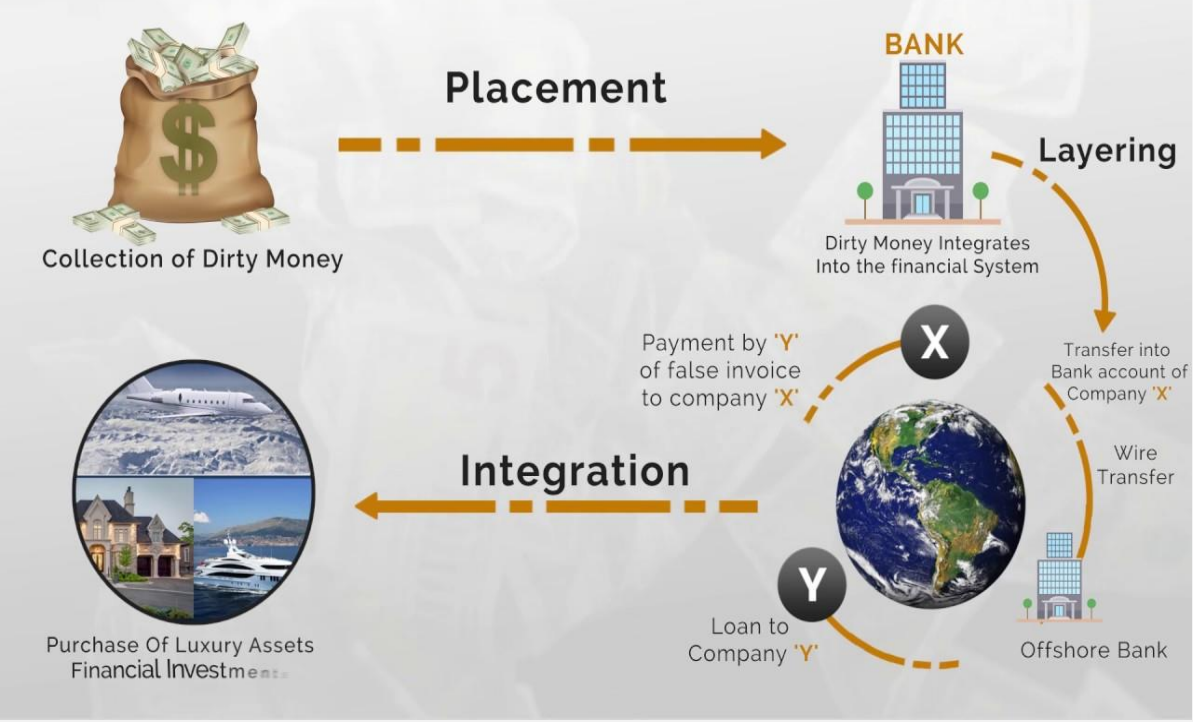
1. **Placement**

Placement is the physical deposit of criminal proceeds derived from illegal activity. Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller checks or deposited into accounts at financial institutions.

2. **Layering**

Layering is the separation of criminal proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. The funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.

3. **Integration**

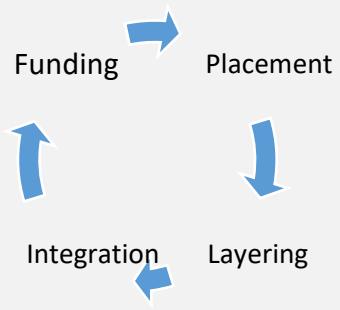
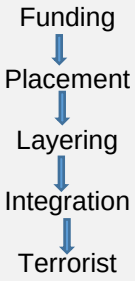


Integration is the provision of apparent legitimacy to the proceeds of crime. If the layering process has succeeded, integration places the laundered proceeds back into the economy in such a way that they appear as normal (business) funds or other assets i.e The funds are re-introduced into the economy and used to purchase legitimate assets or to fund other criminal activities.

2.2 DIFFERENCE BETWEEN MONEY LAUNDERING & TERRORIST FINANCING

The most basic difference between terrorist financing and money laundering involves the origin of the funds in question. Terrorist financing uses funds for an illegal political purpose or terrorism, but the money itself is not necessarily derived illegally. On the other hand, money laundering involves the proceeds of illegal activity. The purpose of laundering is to enable these illegal funds to appear legitimate.

	Money Laundering	**Terrorist Financing**
Motivation	Profit making	Ideological
Source of funds	Illegal source	Illegal/Legal
Intention	Disguise the origin of resources to make it appear legitimate	To intimidate a population or to compel a government or international organization to do or abstain from doing any specific act through the threat of violence
Unlawfulness of the funds	Source/Origin of dirty funds	Purpose intended for use

Life Cycle	Circular	Linear
		

2.3 INDICATORS OF MONEY LAUNDERING AND FINANCING OF TERRORISM

There may be numerous reasons why a particular transaction or series of transactions, are considered suspicious, reasons which may be unrelated to the value of such transaction. A transaction may be considered as suspicious as the result of a combination of different factors, which individually are relatively insignificant, but when taken together raise an alert that the transaction may be related to money laundering or terrorism financing. The context in which the transaction occurs may also be significant, and this will vary depending on the type of business and the nature of the customer.

A suggestive list as per Annexure I lists some examples of indicators which may be helpful when assessing whether there are reasonable grounds for assessing a transaction as suspicious. In addition to general indicators, there may be other more specific indicators relating to particular industries, which can lead to the conclusion that a particular transaction is suspicious.

The simplest form of money laundering is to deposit accumulated illegal cash in the banking system or to exchange it for value items and thereafter use the funds for legitimate activities.

Also, electronic funds transfer systems between financial institutions enable cash to be switched rapidly between accounts in different names and different jurisdictions making the "Know Your Customer" tests difficult to apply.

2.4 OFFENCE OF MONEY LAUNDERING

(1) Pursuant to AML/CFT Laws of FATF a person is guilty of money laundering if;

A. he or she directly or indirectly acquires property from the proceeds of criminal conduct.
B. knowing or believing that property is or represents the benefit of criminal conduct or being reckless as to whether the property is or represents such benefit, the person, without lawful authority or excuse (the proof of which shall lie on the person) —

a) converts, transfers or handles the property, or removes the property from the Country.

b) conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights associated with the property; or
c) acquires, possesses or uses the property.

(2) Removing property from the Country shall include references to removing it from another country or territory and moving property within the Country or a country or territory in preparation for or for the purpose of removing it from the Country or the country or territory in question.

(3) Any person who participates in such conduct as described in subsections including but not limited to, aiding, abetting, assisting, attempting, counselling, conspiring, concealing, or procuring the commission of such conduct commits the offence of money laundering as a principal offender and shall be liable to be tried and punished accordingly.

2.5 BENEFIT FROM CRIMINAL CONDUCT

As per Bank Secrecy Act BSA, Criminal Conduct includes any payments or other rewards received by the accused, including the pecuniary advantage which the accused has obtained, in connection with criminal conduct carried on by him or her.

Criminal conduct which constitutes any act or omission against any law of the Country including the financing of terrorism and for the avoidance of doubt includes the offence of money laundering whether committed in the country or elsewhere.

Money laundering is accordingly not restricted to particular kinds of criminal activity but can arise in connection with all serious crime that yields proceeds, such as drug or people trafficking, corruption, fraud (including tax evasion), robbery or theft, forgery, smuggling, counterfeiting and extortion.

It is not necessary to show that any person has been convicted of a predicate crime, nor is it necessary to specify a particular crime.

It is of no defence that relevant criminal conduct was committed before the commencement of the AML Act, or outside , as long as it is also a crime under the law of the country where it occurs. It is also no defence that criminal conduct was committed by someone else, as long as the person charged has the requisite knowledge/belief.

2.6 PROCEEDS OF CRIME

The crime of money laundering is not restricted to operations connected with money obtained from drug trafficking but include many types of criminal activity that can yield proceeds. This includes among others terrorism, fraud, robbery or theft, forgery, smuggling, counterfeiting and extortion. In , it includes all criminal activities that are punishable by imprisonment for life or for a period not exceeding 15 years or by a fine not exceeding SCR 5,000,000 Section 3(4) or to both. The offence is also

committed by a person who aids, abets, or in any way assists or prepares, the commission of money laundering.

2.7 KNOWLEDGE, BELIEF AND RECKLESSNESS

'Mens rea' or guilty knowledge covers all persons who know, believe, or are reckless as to whether property represents the benefits of criminal conduct. Recklessness is defined as disregarding a substantial risk that property is or represents the benefit from criminal conduct and is assessed in all the circumstances. Belief includes thinking that something is probably true.

Whenever it is objectively reasonable in the circumstances to conclude that a person had the required mental state, the burden of proof shifts to the defendant to raise a reasonable doubt. Actual knowledge does not have to be specifically proved. Money laundering can be committed by body corporates. In those cases, it is sufficient to prove knowledge, belief, or recklessness by any director, officer, employee or agent acting in the course of his or her duty. The relevant individual may also be prosecuted personally. Auditors, accountants, and persons directing or controlling a body corporate are also vulnerable to prosecution if they assisted or consented to the offending.

It should be carefully noted that in circumstances where a suspicious transaction report (STR) is made to the FIU under Section 48 of the Bank Secrecy Act BSA 2020 and the FIU does not issue a direction preventing the relevant service or transaction from proceeding, if that service or transaction does in fact constitute the crime of money laundering, the fact that an STR was made will not be a defence. Any participant with the required Mens rea is vulnerable to prosecution.

2.8 KNOWLEDGE UNDER THE ' AML LAW

The definition of money laundering covers those operations where a person knows, or should have reason to believe, that the money with which they are concerned is derived, obtained or realized, directly or indirectly, from an unlawful activity as described above.

It is only necessary that the person should have knowledge or reasonable grounds for knowledge of the unlawful source of the funds to be guilty of the offence. Positive knowledge is not the test; knowledge may be inferred from objective factual circumstances.

What knowledge entails in the case of corporate bodies is clearly stated in the law. It is sufficient that a director, officer, employee or agent of the body corporate acting in the course of his employment or agency had that state of mind. Guilty knowledge of any employee can result in an offence being committed by the employer (as well as by the employee).

2.9 THE NEED TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

It is universally recognised that failure by national authorities to participate in international efforts to prevent, detect and punish money laundering makes crime a

viable proposition. Money laundering destabilises financial institutions, compromises the integrity of financial systems, distorts commerce, harms victims, and by distorting markets prejudices the rights and opportunities of ordinary citizens, for example in domestic land purchases. Criminals will seek to make use of national and international financial systems to carry out and to benefit from the proceeds of their crime. Money launderers attempt to conceal the true origin and ownership of criminal proceeds by converting ('laundering') those proceeds into apparently legitimate assets. Financiers of terrorism may begin with legitimately sourced funds, but then misuse the financial system in a similar way as other criminal organisations to obscure both the source and destination of those funds. It is essential that criminals are prevented from enjoying the fruits of these criminal activities.

The Bank Secrecy Act BSA and Prevention of Terrorism Act were enacted to prevent, detect, and combat the use by criminals of financial and non-financial institutions for the purpose of the laundering of criminal proceeds or the financing of terrorist acts, activities or groups. The overriding principle is that reporting entities as defined in the Bank Secrecy Act BSA should follow and apply the provisions of the law which reflect the FATF's international standards for the prevention and detection of money laundering and terrorist financing.

3. WHAT IS FINANCIAL ACTION TASK FORCE (FATF)?

In response to mounting concern over money laundering, the Financial Action Task Force on Money Laundering (FATF) was established by the G-7 Summit that was held in Paris in 1989.

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF is therefore a "Policy-Making Body" created in 1989 that works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. The FATF has 40+9 recommendations in order to meet this objective. 40 Recommendations on Anti-Money Laundering & 9 on Combating – Financing Terrorism are recognised by all international bodies like International Monetary Fund (IMF) & World Bank (WB) as the international standards for combating the relevant crimes.

The Recommendations set minimum standards for action from each country to implement according to their particular circumstances and constitutional frameworks. Those not complying with these minimum FATF standards are declared as Non Co-operative Countries and Territories (NCCT); from 13/10/2006, no country is reported in NCCT list of FATF.

FATF-Money Laundering Offences are those where 'Funds' are derived from:

1. Participation in an organised criminal group and racketeering;
2. Terrorism, including terrorist financing;
3. Trafficking in human beings and migrant smuggling;
4. Sexual exploitation, including sexual exploitation of children;

5. Illicit trafficking in narcotic drugs and psychotropic substances;
6. Illicit arms trafficking;
7. Illicit trafficking in stolen and other goods;
8. Corruption and bribery;
9. Fraud
10. Counterfeiting currency;
11. Counterfeiting and piracy of products;
12. Environmental crime;
13. Murder, grievous bodily injury;
14. Kidnapping, illegal restraint and hostage-taking;
15. Robbery or theft;
16. Smuggling
17. Extortion;
18. Tax crimes
19. Forgery;
20. Piracy; and
21. Insider trading and market manipulation.

For more information, please refer: www.fatf-gafi.org

4. REGULATIONS OF THE LAW OF COMBATING TERRORIST CRIMES AND ITS FINANCING 2019

The framework of Anti-Money Laundering standards is contained in ' Bank Secrecy Act BSA 2019. It is well equipped to fight against money laundering and terrorism financing, it assists the regulators and law enforcement agencies to prevent, detect, and combat the use by criminals of financial and non-financial institutions for the purpose of the laundering of criminal proceeds or the financing of terrorist acts, activities or groups.

The Act is for the prevention, detection and combating of money laundering and terrorist financing activities; for collection, analysis and managing information on suspicious financial transactions and activities; to create and empower institutions to suppress money laundering and the financing of terrorism and for matters connected therewith or incidental thereto.

The Act requires all the Bureau De Change to apply CDD, maintain records, monitor transactions, ensure that accounts are in true names, and ensure that money transmissions include originator information, identify and assess money laundering and terrorist financing risks, establish and maintain internal policies, report suspicious transactions and appoint a Compliance and Reporting Officer and register with FIU.

5. FINANCIAL INTELLIGENCE UNIT (FIU)

The General Directorate of Financial intelligence shall be under the oversight of the President of the State Security, and shall enjoy adequate operational independence. It shall act as a national central agency to receive suspicious transaction reports, or other information or reports relating to money laundering, predicate offenses or proceeds of crime as provided for by this Law and its Implementing Regulations, to analyze such reports and information, and to disseminate the results of its analysis to competent authorities, either spontaneously or upon request. The President of the State Security shall determine the organizational structure of the Directorate and the Implementing Regulations shall identify its governance, mandate and its methods of operation

5.1 PRIMARY FUNCTION OF FIU

Similar to other FIUs, the FIU's core statutory function as espoused by the FATF is to serve as the national centre to receive, analyse, interpret financial data on suspected transactions of money laundering and, in case a crime is suspected, to disseminate information to Law Enforcement Authorities (LEAs) spontaneously to decide whether a preliminary investigation should be launched and upon request.

5.2 OTHER FUNCTIONS OF FIU

1. Monitor, supervise, create awareness and train reporting entities, supervisory authorities and the public in respect to their obligation under the Bank Secrecy Act BSA 2019;
2. Establish cooperation with domestic and international institutions and foreign counterparts, entrusted with the responsibility for organizing an effective AML/CFT regime;
3. Exchange information with foreign FIUs based on partnership principles in accordance with the Statute of the Egmont Group of Financial Intelligence Units and in accordance with the Memoranda of Understanding;
4. Enforce compliance with the AML/ CFT Act by creating risk profilesin cases of non-compliance and file suspicious report with Financial monitoring Unit or CTR as the case may be;
5. The FIU is also expressly empowered to issue guidelines and prescribed forms, such as those in this document, and to provide training to reporting entities in relation to customer identification, record keeping and reporting obligations, and the identification of suspicious transactions.

Next Layer is accountable to the FIUvia Central Bank for compliance with the AML/CFT obligations. Those obligations expressly override any duty of confidentiality or non-disclosure that might otherwise apply to the reporting entity

6.1 ROLES OF CENTRAL BANK OF (CBS)- ANTI-MONEY LAUNDERING AND COUNTERING TERRORISM FINANCING (AML/CFT) SECTION

1. Conducts risk-based AML/CFT supervision of financial institutions and other entities falling under the supervisory ambit of CBS, which includes:
    a. On-site examination of financial institutions in accordance with relevant legislation to ensure adherence.
    b. Off-site supervision of financial institutions to ensure that they are complying with regulatory and prudential requirements, and where necessary, recommends appropriate supervisory action or imposition of penalties for non-compliance.
2. Collaborates with other national agencies in the fight against money laundering and financing of terrorism.
3. Coordinates activities on AML/CFT issues at regional and international levels.
4. Researches and formulates policies and procedures for better implementation of the AML/CFT regulatory framework.

7. COMPLIANCE OFFICER (CO)

Who shall be responsible, for ensuring the compliance with the provisions of the Bank Secrecy Act BSA, with the approval of CBS.

7.1 THE MAIN RESPONSIBILITIES OF A COMPLIANCE OFFICER

a) Establishing and maintaining a manual of compliance and procedures in relation to our business
b) Identify and assess money laundering and terrorist financing risks
c) Registering Next Layer with FIU in online platform (goAML)
d) Ensuring that staff comply with the provisions of the Bank Secrecy Act BSA and any other law relating to money laundering or financing of terrorism and the provisions of any manual of compliance and procedures
e) Ensure employees are trained to recognize suspicious transactions and trends and particular risks associated with money laundering and financing of terrorism
f) Acting as a liaison between the business house and the supervising authority and the FIU in matters relating to compliance with the provisions of the Bank Secrecy Act BSAor any law relating to money laundering or financing of terrorism
g) Introducing training procedures for staff to ensure that all are fully trained and updated with latest guidelines from time to time
h) Establishing an audit function to test its anti-money laundering and financing of terrorism procedures and systems
i) Screen persons before recruiting them as employees
j) Be responsible for the implementation and on-going compliance of the reporting entity's internal programmes, controls and procedures in relation to its business with the requirements of the Bank Secrecy Act BSA 2019.
k) Be responsible for ensuring that the staff of the reporting entity comply with the provisions of the Bank Secrecy Act BSAand any other law relating to money laundering and terrorist financing activities
l) Be familiar with the provisions of the guidelines that may be issued by the FIU and the relevant supervisory authority
m) Have unrestricted access on demand to all books, records and employees of the reporting entity as may be necessary to fulfil his or her responsibilities

n) Receive and review reports of suspicious transactions, or suspicious activities made by the staff of the reporting entity and, if sufficient basis exists, report the same to the FIU in accordance with the Act
o) Ensure Cash Transaction Threshold (CTTR) are filed with the FIU on a as per the Schedule of the Bank Secrecy Act BSA
p) Report daily transaction that is carried out by or through it involving cash transactions that are under the limit of CTR
q) Monitor the United Nations Security Council Resolutions (UNSCR) list disseminated by FIU/CBS
r) Comply with all relevant obligations under Bank Secrecy Act BSAlaws and with the internal compliance manual. CO should review arrangements on a regular basis, both to verify compliance with internal procedures and to ensure that those procedures are updated in light of any amendments to the Bank Secrecy Act BSAlegislation.
s) Ensure preparation and submission of the annual Compliance Report to the FIU.

8. REGISTRATION WITH FIU

In line with the requirements of the Bank Secrecy Act BSA . For the purpose of complying with this obligation, the FIU has implemented the goAML platform, an integrated software system developed by the United Nations Office on Drugs and Crime (UNODC) for Financial Intelligence Units worldwide.

In accordance with Next Layer shall notify the FIU of any changes in the particulars furnished, in writing, within a period of 30 days from the date of such change. goAML provides reporting entities the access to make changes to the User's details or the Organisation's details through the platform.

9. INTERNAL CONTROL SYSTEMS AND PROCEDURES

9.1 RISK ASSESSMENT

In accordance with the Bank Secrecy Act BSA Next Layer shall take appropriate measures to identify, assess, and understand its ML/TF risks.
A key step in controlling risk of money laundering and terrorist financing is to exercise due diligence that is commensurate with the risks identified for each type of customer.We have adopted a risk-based approach for the customer's classification, and hence the required due diligence and monitoring. The classification could be on basis of type of relationships, type of activity, type of product and services and residence or activity in high-risk country etc.

Customer due diligence must be performed based on the classification of customers according to perceived risk. From the Customer Due Diligence measures obtained, an initial assessment of the customer's risk profile can be made. In assessing the risks referred above, we shall also take into account the outcome of any risk assessment carried out at national level and any regulatory guidance issued by the FIU or a supervisory authority.

The Compliance Officer shall document the outcome of the risk assessment, regularly update it, and shall submit the same to the appropriate supervisory authority and law enforcement agency upon request.

9.1.1 ENTERPRISE-WIDE RISK ASSESSMENT OF NEXT LAYER

EWRA (Enterprise-Wide Risk Assessment) is prepared taking into consideration the below 5 parameters as per CBS guidelines.

Risk Identification:

1) Customer Risk
2) Counterparty Risk
3) Product Risk
4) Country Risk
5) Delivery Channel Risk

1. Customer Risk: 'Customer risk' in the present context refers to the money laundering risk associated with a particular customer from a Compliance perspective. This risk is based on the risk perceptions associated with the parameters comprising a customer's profile, and the risk associated with the product and channel being used by him

2. Counterparty Risk:

   a) The risk that the other party to an agreement may default is the counterparty risk. Next Layer identifies, measures, monitors and controls counterparty risk prior to establishing the business relationship;

   b) The Exposure limits assigned to counterparties are continuously monitored.counter parties risk can be in any form, it can be inherited risk, riskduring business relationship as change in the nature of business of the parties, the products dealt by counter party and the association of counter party.

3. Product Risk:

Factors that may determine that a customer poses a higher risk include the list below, which is not exhaustive and may also consider other factors;

a) Cross border services providing extra anonymity, including Correspondent or international private banking Banknotes or precious metal trading;
b) Transactions involving third parties, or outsourcing involve higher risks since there are more ways for money launderers to structure the transfer of money, eventually hiding the party that benefits

4. Jurisdictional or Country Risk:

Refers to the money laundering and terrorist financing risks stemming from the country or origin or destination of the funds, or the geographical location of the customer or his business. EDD must always be applied when the: Factors that may indicate that a country poses a higher risk include the list below, which is not exhaustive and may also consider other factors:

- Sanction Countries;

- Countries identified to be involved in supporting of terrorist activities;
- Countries identified by FATF or identified from other trusted sources having an inappropriate money laundering laws and regulations;
- Countries identified with weak governing laws and regulations to combat terrorist financing;
- Countries identified by credible sources as having significant levels of corruption or being a non-transparent tax environment.

Countries which are considered as high risk and are required additional examinations like sanction check, Google search to explore adverse media in case if required we conduct cross verification of given documents if the transaction owner/beneficiary of those countries.

5. Delivery Channel Risk:

A delivery channel is a medium that can be used to obtain a product or service, or through which transactions can be conducted. Delivery channels should be considered as part of the risk of the transactions.

9.1.2 RISK-BASED APPROACH (RBA)

Next Layer adopts a risk-based approach to transaction monitoring, which must include the following components:

- Scrutiny of customer transactions to ensure that the transactions are in line with the knowledge of the customer, his business, risk profile, source of wealth and funds.
- Review of customer records to ensure that documents, data and information collected during the KYC, CDD and monitoring processes are relevant and up to date.
- Ideally performing transaction monitoring on the real time basis, to ascertain whether there has been any breach of rules or whether there is suspicion regarding a particular transaction.
- Using the information collected during the onboarding process that is related to the customer‘s expected monthly activity in order to assess any deviations or identify unusual patterns.
- Investigating any unusual or suspicious transactions and maintain all supporting records for a minimum period of 7 years.
- Following the investigation of unusual transactions, if there are reasonable grounds for suspicion, The Compliance Officer must not later than 2 days report such transactions to the FIU.
- Configuring its monitoring system by defining a sufficient number of rules and parameters in the system so as to effectively identify unusual or suspicious transactions, patterns of activities or customer behaviours.
- Using parameters that reflect and take into account its risk assessment and profile.
- Using parameters tailored for both natural persons and legal entities so as to cater for the different types of transactions effected.

9.2 NATIONAL RISK ASSESSMENT

The National Risk Assessment (NRA) is an activity undertaken to develop risk-based anti-money laundering and countering the financing of terrorism (AML/CFT) actions and facilitate allocation of available resources to control, mitigate, and eliminate risks. The NRA will help the business house to have a more comprehensive and shared understanding of the inherent risks of Money Laundering and Terrorist Financing faced by the business house while conducting its business activities.

9.3 KNOW YOUR CUSTOMER (KYC)

At Next Layer all transactions should be undertaken only after proper identification of the customer. Photocopies of proof of identification should invariably be retained by the business house after verifying the document in original. Full details of name and address as well as all the details of the identity document provided should also be kept on record. If a transaction is being undertaken on behalf of another person, identification evidence of all the persons concerned should be obtained and kept on record.

9.3.1 KNOW YOUR CUSTOMER" PROCEDURES

KYC Procedures:

- Helps in identifying customers with inappropriate intentions help detect suspicious activity in a timely manner and prevent money laundering or terrorist financing.
- Promote compliance with all regulations
- Promote safe and sound money exchange/transfer practices.
- Minimize the risk of the services being used for illicit activities.
- Protect the 'sreputation.
- Helps the firm prosper.

The objective of KYC policies is to ensure that all reasonable measures are taken to identify the customer by following two main steps:

a) Identification & Verification

Documents and information about the customer are verified against independent sources and checked for correctness.

Depending on the risks associated with each client or transaction, we apply the appropriate KYC process to each customer. Identification of Customer ID,verification must be based on a risk-based approach on the client profile.

b) Registration

We treat our customers with acceptable identifications in accordance with Bank Secrecy Act BSA and Regulatory Standards guidelines. Customer registration is mandatory for all customer executing transactions. KYC is carried out on our customers to confirm who our customers are and to ensure that the funds involved in the transactions originate from legitimate sources and are used for legitimate

purposes. The customer is required to provide all necessary documents and information.

9.3.2 PERSONAL CUSTOMERS IN

A. The following minimum information should be obtained from prospective customers who are resident in :

- True name and any other names usedsuch as aka, orreffered name such as reffered with local or international names, in names of wanted criminals, offenders,public office holders or politicians.;
- Correct permanent residential address, and postal address if applicable;
- Date of birth;
- Occupation;
- Source of fund;
- Purpose of transaction.

Ideally the true name or names used should be verified by reference to a document obtained from a reputable official source which bears a photograph. A current valid full passport or national identity card, not older than 10 years or a Valid Driving License should be requested for currency exchange and Gainful Occupation Permit copy (GOP) for Outward TT remittancesfor inward remittances, the name of party, purpose, contact number, occupation, source of income, purpose of transaction shall be required.

B. In addition to name verification, it is important that the current permanent residential address is also verified. Some of the best means of verifying addresses are:

- Requesting sight of a recent (not older than three months) utility bill, telephone bill, bank or other financial institution statement, or insurance policy which includes a residential address (to guard against forged or counterfeit documents care should be taken to check that the document is original);
- Checking an official register such as the electoral roll;
- Checking a current telephone directory;
- Receiving written confirmation from the person's landlord or employer.To verify the client's claim ofemployment and source of incomeby third partyto which client claims of being employed,tenant, etc.

An introduction from a respected customer personally known to the manager, or from a trusted member of staff, may assist the verification procedure but does not replace the need for address verification, the verification of the client if

its high risk shall be done as per procdeure and no interferance from any staff member or maanger shall be allowed. Details of the introduction should be recorded on the customer's file.

9.3.3 COMPANIES AND OTHER LEGAL ENTITIES

Because of the potential for concealing beneficial ownership, corporate accounts are one of the most high-risk vehicles for money laundering, particularly when opened and ostensibly operated by a legitimate trading company. Additional obligations for opening corporate accounts focus on knowledge of and about the beneficial owners and any other persons authorised to act on behalf of the account holder. Obtaining information on the purpose and nature of the business relationship, including proof of sources of wealth and initial source of funds, is also particularly important, to enable the reporting entity to conduct meaningful ongoing monitoring.

Before a business relationship is established with a legal entity, and at appropriate regular intervals after the relationship is established, measures are taken by way of a company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound up or terminated. Further checks are made whenever we become aware of changes in the management or ownership structure.

The following additional documents should be obtained:

- Institution profile (if applicable)
- Central Bank/ regulatory License (if applicable)
- The original or a certified copy of the Certificate of Incorporation
- Memorandum and Articles of Association
- Resolution of the board of directors to open an account and confer authority on those who will operate it
- Passport copies of all Partners and Board of directors; If any Partner/Board of Director is an expatriate, then copy of GOP/ National ID/ Visa Page is required.
- GOP/ National ID copy of Authorized representative
- Statement of Account (One Month)

9.3.4 TRUST, NOMINEE, AND FIDUCIARY ACCOUNTS

Where a prospective customer is not the beneficial owner, it is necessary as per the Bank Secrecy Act BSA to take reasonable measures on a risk-sensitive basis to identify the ultimate beneficial owner/s and to verify their identity. An application to start a business relationship or to undertake a transaction by a professional adviser, business or company acting as trustee or nominee requires satisfactory evidence of the identity of the trustee, nominee, or fiduciary and the nature of their trustee or nominee capacity or duties. Where an individual nominee who opens a business relationship on behalf of another is not already known to the financial institution then the identity of that nominee or any other person who will have control of the account should also be verified. Enquiries should be made as to the identity of all parties for

whom the trustee or nominee is acting and confirmation sought that the source of funds or assets under the trustee's control can be vouched for. If the applicant is unable to supply the information requested, independent enquiries should be made as to the identity of the person who has actual control or for whose ultimate benefit the transaction is undertaken. The results of the enquiries should be recorded in the account opening file for a definite period with the client record.

Where money is received by a trust, it is important to ensure that the source of the receipt is properly identified, the nature of the transaction is understood, and where possible confirmation made that the payments are made only in accordance with the terms of the trust and are properly authorised in writing. The financial institution must be satisfied as to the bona fides of the trustee. Stockbrokers, fund managers, solicitors, accountants, estate agents, and other intermediaries frequently hold funds on behalf of their clients in “client accounts" with financial institutions. Such accounts may be general omnibus accounts which hold the funds of many clients or they may be opened specifically for a single client, which is either undisclosed to the reporting entity or identified for reference purposes only. Those cases, where it is the intermediary who is the customer, should be distinguished from those where an intermediary introduces a client who himself becomes a customer of the reporting entity, or where the intermediary undertakes transactions on behalf of the client, in which case the identity of the client must be independently verified.

9.3.5 THIRD PARTY TRANSACTIONS

Third Party transactions are those which are carried out by a person (‘representative’) on behalf of another natural person. It involves representative other than the main participants of such transaction. Such representative can be involved in crafting the particulars of the deal or serve as the means of receiving a payment on behalf of a natural person or entity.

In order to identify a third-party transaction and accept transaction by one natural person to another, Next Layer follows the procedures below:

- The beneficial owner shall issue an authorization letter, authorizing the representative the carry out transactions of their behalf in absence of a Power of Attorney. However, the beneficial owner must visit Next Layer physically and sign such authorization letter.
- The Authorization letter must refer to the type of transactions (whether currency exchange or money transfer).
- Authorization letter must include the beneficiary details in the case of a money transfer transaction.
- The signature of the beneficial owner of funds in the letter of authority must be verified against that in the passport, National Identity Card or Driving license
- Both representative and the beneficial owner must be resident.
- Collect and verify the original identification documents of both the parties.
- Record Name and ID details of the representative in the system.
- The beneficial owner must undergo the CDD & EDD process, whenever applicable.

9.3.6 CORRESPONDENT BANKING

Pursuant to the Bank Secrecy Act BSA the shall not enter into a correspondent banking relationship with a bank or other credit institution situated outside unless we;

1. gather sufficient information about the bank or credit institution so as to understand fully the nature of the business of that bank or credit institution

2. are satisfied on reasonable grounds, based on publicly available information, that the reputation of the bank or credit institution and the quality of supervision or monitoring of the operation of that bank or credit institution in the other country are sound, adequate and effective;

3. are satisfied on reasonable grounds, having assessed the anti-money laundering and anti-terrorist financing controls applied by the bank or credit institution, that those controls are sound, adequate and effective including whether it has been subjected to any investigation regarding money laundering or terrorist financing activities or undergone any regulatory action;

4. obtains the approval of the senior management;

5. documents the responsibilities of the bank or credit institution in applying anti-money laundering and anti-terrorist financing controls to customers in the conduct of the correspondent banking relationship;

6. in the case of customers of the bank or credit institution who have direct access to a payable-through account held with the licensed bank in the name of the bank or credit institution, is satisfied on reasonable grounds that the bank or credit institution —

    i. has identified and verified the identity of those customers, and is able to provide to the licensed bank, upon request, the documents, whether or not in electronic form, or information used by the credit institution to identify and verify the identity, of those customers;

    ii. has applied Enhanced Due Diligence in relation to those customers;

    iii. is applying Customer due diligence in relation to its customers

9.3.7 SOURCE OF FUNDS

In Next Layer , it is important to determine the source from which our customer finances the current transaction. ‘Source of Fund’ means how the money, involved in the transaction, was originally derived or earned. In Next Layer, we hereby ascertain that our customers pay for a transaction

or several transactions from their own funds and such is generated from a legitimate source.

The following sources of funds are approved in our business:

- Bank Statement
- Salary Payslip
- Personal cash or savings. Supported by detailed latest bank statement
- Withdrawal slip from a bank account, or detailed latest bank statement
- Property Sale Deed
- Income from business, Supported by Audit report or latest profit & Loss statement, or company bank account statement
- Commercial transactions should be supported by valid and comprehensive invoice related to the trade activities of both parties
- Bank Loan
- Lottery/Prizes
- Imported cash from abroad
- Any legitimate source etc.

Not Approved Sources:

Criminal proceeds including money laundering, drug trafficking, theft, forgery etc.

Counter staff should apply his 'Due Diligence' knowledge and skill in ensuring the cash brought to his counter is relevant to the transaction and apparently generated through legitimate source; where suspicious on legitimacy of the source, more information should be requested; support documents may or be requested/obtained for extreme suspicion.

The concerned staff will determine if a person is a Politically Exposed Person (PEP). If the customer is a Politically Exposed Person, the relationship will be entered into only with approval of senior management. The identification can be done from consent form obtained from the cllient for declaration also an independent system of online tools shall be used that is governement databases of different countriesand politicians.

9.3.8 SHELL BANKS

A shell bank is a bank, or an institution engaged in equivalent activities that;

a) is incorporated in a country in which it has no physical presence involving meaningful decision making and management; and

b) is not subject to supervision by the Central Bank of or a foreign regulatory authority, by reason that it is not affiliated to any financial services group that is subject to effective consolidated supervision.

Pursuant to Bank Secrecy Act, Next Layer shall not enter into a business relationship with a shell bank and we shall take appropriate measures to

ensure that we do not enter into, or continue, a banking relationship with a bank that is known to permit its accounts to be used by a shell bank.

9.3.9 CUSTOMER SCREENING

An automated real-time screening of all parties involved in transactions is performed against the following lists to check and ensure that customer's name does not appear in any list (of known specially designated nationals (SDN) or suspected terrorists or terrorist organizations or even PEP.

- OFAC sanctions
- UN sanctions
- EU sanctions
- UK List
- UNSCR list disseminated by supervisory authority
- Internal watch lists compiled internally for high-risk persons.

The applicable screening procedure is as follows:

Nature of Transaction	Field Screened
Foreign currency exchange transactions	Screen the customer's name (whether natural person or legal entity).
Remittance	Screen the remitters and beneficiary's names (whether natural person or legal entity) and the name of the beneficiary's bank.
Transactions by legal entity	Screen the name of the authorised person performing the transaction and the name of the legal entity and its owners
Transactions by one person on behalf of another person:	Screen the names of both persons.
Beneficial owners of a customer who is a legal entity	Screen the names of the BOs at regular intervals and at least annually as part of the EDD process.

Explanation
In the event of a hit, the transaction will go into a queue and the same can be released only by the CO. CO will review the reasons for the hit and release it or freeze based on additional information he / she gathers.the laws, related information based for releasingthe alerts for STR shall be maintained by CO and provide with STR reporting as well.

9.4 CUSTOMER DUE DILIGENCE

We shall apply customer due diligence measures in respect of customers, business relationships and transactions, and conduct ongoing monitoring of business relationships.

1. The Customer due diligence measures include the following:

(a) Identifying the customers identity on the basis of documents, data or information obtained from a reliable and independent source or from any other source that we have reasonable grounds to believe and can be relied upon to identify and verify the identity of the customer and if we are unable to obtain such information, we shall prepare and submit a suspicious transaction report to the FIU;

(b) Where the customer is not the beneficial owner, we shall identify the beneficial owner, and take reasonable measures, on a risk-sensitive basis, to verify the identity of the beneficial owner, including, in the case of a legal person or partnership the following information:

i. the identity of the natural person who ultimately has a controlling ownership interest;
ii. the identity of the natural person exercising control through other means;
iii. the identity of the relevant natural person who holds a senior management position;

(d) Obtaining information on the purpose and intended nature of the business relationship and to establish details of the business of the customer or a beneficial owner to enable our business house to identify;

i. complex or unusual large transactions;
ii. unusual patterns of transactions which have no apparent economic or visible lawful purpose; or
iii. any other activity which may be, by its nature, likely to be related to money laundering, financing of terrorism or other criminal conduct; and

(e) Take reasonable measures to ascertain the purpose of transaction that exceeds CTR limit and the origin and ultimate destination of funds involved in the one-off transaction or transfer as part of a business relationship.

2. Where the customer is not an individual, we shall take reasonable measures to identify the customer and verify its identity through the following information;

i. name, legal form and proof of existence;
ii. the powers that regulates and binds the customer, including the name of the relevant persons with a senior management position;
iii. the address of the registered office, and if different, a principal place of business;
iv. verify that any person purporting to act on behalf of the customer is authorised to do so; and
v. Identify and verify the identity of that person.

9.4.1 THE MAIN CDD PROCEDURES USED IN OUR BUSINES HOUSE

- Creating a customer profile and ensure the same profile is used for all

his transactions;

- Identification and verification of the customer's identity
- Complete information of the customer's address, contact number is recorded;
- Source of funds and purpose of transaction must be captured in the system for every transaction;
- Ongoing due diligence of the transactions to be conducted and regular check on the profile of customer, its business and risk profile;
- If a customer refuses to provide his/her valid identity document for verification, the transaction shall be refused, the Compliance Officer will therefore decide whether to file a suspicious transaction report;
- Update KYC information for each customer, retail and company during KYC renewal schedule or whenever documents expire, whichever comes first;the renewal shall be done according with the bi annualrenewal of all customers, however if customer is high risk and pose greater risk of ML TF then renewal shall be required on priority basis before the bi-annualrenewal of all clients database.
- Run every customer and all relevant transactions through the screening software for sanctions;
- All receipts to be signed by the customer;

Where we reasonably believe that performing the customer due diligence process will tip-off the customer, the customer due diligence process shall not be pursued and we shall file a suspicious transaction report under the Bank Secrecy Act BSA.

9.4.2 RISK CATEGORISATION OF CUSTOMERS

- Low Risk Customers (Simplified Due Diligence)

These are customers who do not meet the criteria for being considered High Risk or Medium Risk and for which standard due diligence should be conducted in line with the requirements laid down in the Bank Secrecy Act BSA and Regulation. Simplified due diligence does require identity document verification andscreening to ensure that the risk stated is low risk, then the simplified due diligence can be applied.The timing of obtaining documents, and verification after its identified is low risk client then it can be set accordingly

- Medium Risk Customers (Standard Due Diligence)

Standard due diligence requires you to identify your customer and verify their identity. There is also a requirement to gather information to enable you to understand the nature of the business relationship.

- High Risk Customers (Enhanced Due Diligence)

These customers are those customers that by nature of their activity or their dealing pose a higher risk from money laundering/terrorist financing and enhanced due diligence and enhanced ongoing monitoring should be applied in line with the Bank Secrecy Act BSA and Regulation.

9.5 ENHANCED DUE DILIGENCE (EDD)

Enhanced due diligence means the collection of additional information to verify the identity or source of income of the customer, including adverse media checks, etc.Identification of PEP associates, relationship of client with any ML TF threats, client's businessanalysis, product analysis,delivery channel analysis, maintaining threshold limit of transaction for that client as per tolerance level which business can tolerate risk of the high risk client.Such controls should be relative and proportionate to the level of risk identified and ensure that any risk is mitigated and that the risk is unlikely to be realized – Elaborate on this further – Source of funds, purpose of transactions, Beneficial owner, etc.

Examples of what to look for include but are not limited to:

- Related parties, indirect links to Politically Expose Persons, or other high-risk individuals or entities.
- Litigation, political or regulatory risks
- Overall reputation and integrity
- Source of Wealth and required supporting documents.

As per Bank Secrecy Act BSA 2019, Next Layer shall apply on a risk-sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring in any other situation which by its nature presents a higher risk of money laundering, terrorist financing activities or other criminal conduct on the basis of national risk assessment carried out under Section 30 of the Act.

In accordance to the Bank Secrecy Act BSA 2019, our business shall proportionate to risk, apply enhanced customer due diligence measures and enhanced ongoing monitoring in respect of business relationships and transactions with legal and natural persons from countries which do not apply or fully apply the Financial Action Task Force Recommendations.";

9.5.1 ENHANCED DUE DILIGENCE PROCEDURES

- **EDD FOR NATURAL PERSONS**

During the Enhanced Due Diligence for natural persons, the source of funds and purpose of transaction must be verified.

a) Screen customer information provided, and analyze the risk of MLTF if customer has inherited risk of ML/ TF .
b) Approval of Compliance officer shall be obtained prior to processing the transaction for a new beneficiary.
c) A transaction conducted by representatives of a company supported by an authorization letter issued by the company.
d) Documentary evidence in the form of an invoice or bill of lading or airway bill, other supporting documents justifying the source and purpose of the transaction should be sought in support of trade-based transactions.
e) To seek explanations where the transaction does not make economic sense.
f) Efforts to understand the business activity of the customer, its transactions and customer shall be made before processing the

transactions.

g) The source of the fund and purpose of the transaction must be collected & verified.
h) Proof of source of funds (e.g., bank statements) must be collected for verification if the customer pays in cash.
i) Appropriate evidence must be collected to verify the purpose of the transaction in the event of any doubt or suspicion about the customer's information.
j) The receipt must be signed by the customer and kept in the records in accordance with Bank Secrecy Act BSA together with all KYC supporting documents.
k) Understand who the ultimate beneficiary of this transaction is.
l) Get more information about the remitter and its involvement with the beneficiary.
m) For high risk jurisdiction identified by FATF, and other international agencies for risk of ML/T,Fayment in favour of them shall entail EDD measures on that client.
n) Proper due diligence must be done in order to better understand the nature of the business the customer is dealing.

- EDD must be carried out for FC transactions (sales/purchase) of value equal to or above threshold of USA Financial System Limit

➢ EDD FOR LEGAL ENTITIES

The EDD process must be applied for a customer prior to entering into any business if it is a legal entity. The EDD must include verification of the identity of the legal entity (i.e., its licenses, incorporation documents, etc.) and identification of its ultimate beneficial owners. When dealing with corporate entities, it is of the utmost importance that these customers ' transactions are carried out with due diligence and only after the following on boarding procedure has been completed:

a. KYC form must be completed and signed when the customer has on boarded.
b. Latest Ownership Structure of the entity including the purpose and nature of the business relationship.
c. Collecting copies of the entity's valid licenses from competent authorities.
d. Certifying the copies as "Original Sighted and Verified" by the employee who conducts the KYC process after verification of the originals.
e. Collecting the original Beneficial Owners (BO) identification documents and verifying and retaining the copies after certification.
f. Collecting of authorization letter for representatives of the legal entity conducting transactions on its behalf.
g. Check original identification documents of representatives who are authorized to conduct transactions (and must be kept in the records). Such officials must be residents. Such a representative and the legal

entity should have a relationship.

h. Applying sanction checks and internet searches on the name of the legal entity, the ultimate beneficiary owners, group companies, subsidiaries and the names of legal entity representatives authorized to carry out transactions on their behalf.
i. Collecting information on the source of wealth of the Beneficial Owners if the BO is a High risk customer.
j. The General Manager and the Compliance officer must both approve the relationship with legal entities where the ultimate beneficiary is PEP, The receipt should be signed on behalf of the representative of the legal entity who carries out the transaction and kept in the records together with all supporting documents of KYC.
k. EDD is carried out periodically, i.e., on anbi-annuallyor event-driven basis, i.e., significant changes in business / activity / ownership.

- **EDD- ADDITIONAL PROVISIONS**

EDD process that is efficient and proportionate to ML/TF risks, including the approval of the CEO, General Manager and the Compliance Officer must be applied to establish business relationships or one-off transactions:

- PEPs
- Customers from high risk or increased monitoring jurisdictions as identified by FATF and/or similar bodies
- Unusually complex transactions or those which have no clear economic or legal purpose
- Non-Resident customers
- Any customer and/or transactions which we consider as high risk in line with the ’s internal risk assessment

In Next Layer, regardless of the value of the transaction, the EDD process is carried out for a customer if:

- The customer is reasonably suspected of money laundering or terrorist financing. If suspicion persists even after the EDD, we will report such cases to the FIU immediately.
- There is a material change in the nature or ownership of a customer who is a juridical person.
- There is doubt about the reliability or adequacy of information previously obtained in relation to the customer
- The customer is a legal entity.

In Next Layer, we also conduct EDD process on its existing customers, if:

- Material change in the nature or ownership of a customer
- Doubt about the reliability of information previously received about/from the customer
- Other reasons which Next Layer may deem as appropriate

9.6 POLITICALLY EXPOSED PERSON (PEP)

PEP is defined in the Bank Secrecy Act BSA-

(a) An individual who is or has been, during the preceding three years, entrusted with a prominent public function in:

i. ; or

ii. Any other country; or

i. An international body or organisation;

(b) An immediate family member of a person referred to in paragraph (a); or

(c) A close associate of a person referred to in paragraph (a).

1. Prominent public function includes

i. Heads of state, heads of government, ministers and other senior politicians;

ii. Senior government or judicial officials;

iii. Ambassadors and chargés d'affaires;

iv. Persons appointed as honorary consuls;

v. High-ranking officers in the armed forces;

vi. Members of the Boards of Central Banks;

vii. Members of the Boards of state-owned corporations; and

viii. Influential political party officials.

Immediate family member of a person specified in paragraph (b) includes:

i. A spouse

ii. A partner, that is an individual considered by his or her national law as equivalent to a spouse;

iii. Children and their spouses or partners, as defined in paragraph (b);

iv. Parents; and

ii. Siblings.

2. For the purposes of above point (c), close associates of a person includes:

(a) Any person who is known to have joint beneficial ownership of a legal person, partnership, trust or any other close business relations with that legal person, partnership or trust;

(b) Any person who has sole beneficial ownership of a legal person, partnership or trust which is known to have been set up for the benefit of that legal person, partnership or trust.

3. In determining whether a person is a close associate of a person specified in above point (a), we shall have regard to public information or such information that we have in our possession.

4. For the purpose of Politically Exposed Persons, our business house shall, in addition to the measures provided in Bank Secrecy Act:

   (a) Obtain the approval of the senior management before a business relationship is established with the customer.

   (b) Take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or one-off transaction.

   (c) Where the business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

   (d) Apply such other measures provided for in the guidelines issued by the FIU or respective supervisory authority to compensate for the higher risk of money laundering, terrorist financing activities or other criminal conduct.

It shall be noted many PEPs hold positions that can be abused for the purpose of laundering illicit funds or other predicate offences such as corruption or bribery. Because of the risks associated with PEPs, the FATF Recommendations require the application of additional AML/CFT measures to business relationships with PEPs. These requirements are preventive in nature and should not be interpreted as meaning that all PEPs are involved in criminal activity.

9.7 OBLIGATION TO CEASE TRANSACTION

If the is unable to verify the customer's identity using reliable and independent sources of data or information, then we will take below steps as stipulated in Bank Secrecy Act BSA;

- Not carry out a transaction with or for the customer
- Markclient high risk
- Maintain record of that customer
- Maintaindatabase of that client for future screening of anysuspicious activity associated with that client if anyassoicate or business arises in future.
- Not establish a business relationship or carry out a one-off transaction with the customer;
- Immediately terminate any relationship with the customer
- And consider whether we should make a suspicious transaction report to the FIU in accordance to the Bank Secrecy Act BSA.

9.8 ONGOING MONITORING

The CDD obligations are supplemented by the general obligation by which Next Layer conduct ongoing monitoring of all business relationships
Ongoing monitoring has two key components:

- Scrutinising transactions undertaken throughout the relationship to ensure that the transactions are consistent with the 'sknowledge of the customer, the business and risk profile and the source of funds of the customer.

- Keeping all CDD information and documentation up to date

The objective of the ongoing monitoring obligation is to identify activities of customers during the course of a business relationship which are not consistent with the knowledge of the customer, or the purpose and intended nature of the business relationship, and which need to be assessed for the possibility that the exchange may have grounds to report a suspicion of money laundering or terrorist financing. Next Layer is accordingly obliged to monitor all dealings with a customer, to the extent reasonably warranted by the customer's risk profile, for consistency and pattern of transactions.

When scrutinizing the source of funds Next Layer seeks to discover the origin and the means of transfer for funds that are directly involved in the transaction (for example, business activities, proceeds of sale). When scrutinizing the source of wealth we seek to discover the activities that have generated the total net worth of the customer (that is, the activities that produced the customer's funds and property). Internalizing the two key ongoing monitoring requirements is therefore fundamental to the proper discharge of CDD obligations and should be a central focus by the CO.

9.9 SUSPICIOUS TRANSACTION REPORT (STR)

Next Layer shall in accordance with make a suspicious transaction report (STR) in any situation in which we:

a) Have knowledge or reasonable grounds to suspect that any service or transaction may be related, directly or indirectly, to the commission of criminal conduct (as defined in the Bank Secrecy Act BSA, including an offence of money laundering or of terrorist financing or to money or property that is or represents the benefit of criminal conduct;
b) Have information that may be relevant to an act preparatory to an offence or to money or property that is or represents the benefit of criminal conduct;
c) Has information that may be relevant to an investigation or prosecution of a person for criminal conduct; or
d) Have Information that may be of assistance in the enforcement of the Bank Secrecy Act BSA or the Proceeds of Crime Act.

The obligation to make STRs under the Bank Secrecy Act BSA complements the duties of disclosure to the Commissioner of Police under the Prevention of Terrorism Act. that Act require all persons (not just reporting entities) to disclose to the Police any information that will assist in the prevention or detection of terrorist acts, including information about any property in his or her possession or control that is known to be owned or controlled by or on behalf of a terrorist group, in the circumstances set out in that Act.

The reporting entity shall always perform the compliance procedures as per relevant laws and regulations.

9.9.1 RECOGNISING SUSPICIOUS TRANSACTIONS

As the types of services and transactions which may be used by a criminal or money launderer are almost unlimited, it is impossible to provide an exhaustive list of indicators of suspicious activity as listed in Annexure I. The simplest form of money

laundering is to deposit accumulated illegal cash in the banking system or to exchange it for valuable items and thereafter to use the items or funds for legitimate purposes.

There may be numerous reasons why a service, transaction, or pattern of transactions could be considered suspicious, reasons which may be unrelated to the value of the transaction and appear trivial or insignificant when considered in isolation. The context in which the service or transaction occurs may also be significant, and this will vary depending on the type of business and the nature of the customer.

A transaction which is consistent in nature and extent with a customer's known, legitimate business or personal activities or with the normal business profile for that type of account is less likely to be suspicious. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a service, transaction, or pattern of transactions is unusual. Developing and maintaining customer profiles is critical in this regard.

9.9.2 STR'S AND THE ROLE OF THE COMPLIANCE OFFICER

As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of account.

Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or series of transactions is unusual. Developing a customer profile will assist our business house with identifying suspicious transactions. When there are reasonable grounds to believe that any transaction or proposed transaction is likely to constitute an offence of money laundering or the financing of terrorism, then as required by laws and regulations, the Compliance Officer will report suspicions of money laundering or the financing of terrorism to the Financial Intelligence Unit *no later than two working days* after forming that suspicion or receiving the information. In the course of business if any employee has reasonable grounds to believe that any activity carried out or proposed constitutes an offence of money laundering or the financing of terrorism the employee or officer should consult the Compliance Officer. The Compliance Officer will consider the matter further and decide on what to do, and if it is thought to be likely to constitute an offence then the CO will, on behalf of Next Layer., notify the FIU in writing with full particulars.

Where a potentially suspicious transaction or service has been identified by any staffs of Next Layer, the Compliance Officer must examine the relevant records to confirm whether there are reasonable grounds to suspect that the service or transaction may be related, directly or indirectly, to the commission of serious criminal conduct (including money laundering or terrorist financing).

The degree of decision-making responsibility placed on the CO is significant. In forming an independent judgement about whether there are reasonable grounds for suspicion, he/she should consider all other relevant information available within the Company concerning the person or business to which the initial report relates. This

may include a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship, and referral to identification and other records held. If after completing this review, the CO decides that reasonable grounds or suspicion exist, then he/she must immediately proceed to make an STR to the FIU.

STRs should be submitted on the applicable prescribed form, as set out in Annexure II to these guidelines. It is essential that all relevant fields are completed, that the core reason for the suspicion is explained, and that the form is dated and signed or otherwise authenticated. When deciding to make an STR, we ensure that funds will not be transferred or property disposed of or put beyond reach of the courts of . If there is any possibility of these events occurring, we make contact with the FIU by telephone at the earliest opportunity so that appropriate directions can be given to preserve the status quo.

Where an STR is made in relation to a service or transaction in respect of property in its possession or control, Next Layershall continue business and if FIU or any govt body prohibits business with specific customer than shall cease to do business with that customer, or in other case except with the written consent of the FIU). After that 5-day period, unless the FIU has issued an administrative freezing direction under the AML Act, we may proceed with the service or transaction.

The ensures non-disclosure of the contents of the STR or report or any information likely to identify any person who prepared or made the STR or handled the underlying transaction. The only exceptions are disclosures for law enforcement purposes.

9.9.3 REPORTING OF SUSPICIOUS TRANSACTIONS THROUGH INTERNAL SUSPICIOUS TRANSACTION REPORT (ISTR'S)

It is the obligation of all Next Layer staff to report suspicious and unusual transactions to the Compliance Officer. When potentially suspicious transactions are identified by a member of staff, they should be immediately report to the Compliance Officer through the STR form.

The CO will perform an investigation and if confirmed as suspicious, then the case will be reported to FIU in the form of a Suspicious Transaction Report (STR). The Compliance Officer shall maintain records relating to ISTRs and STRs, including the customer and transaction information and details of any action taken as a consequence. Failure to report suspicious and unusual transaction to the Compliance Officer shall attract disciplinary action.

9.9.4 ESCALATION PROCESS OF TRANSACTIONS AND QUERIES

In Next Layer, the escalation process when an Employee suspects a transaction to be unusual / suspicious could be summarized as follows:

1. Escalates his/her suspicion to the CO via an ISTR immediately
2. Upon receipt of the report from the staff, the Compliance Officer shall verify and do further investigation, EDD on the transactions etc.

3. Escalation happens automatically through the system.
4. When there is any suspicious activity or transaction identified through rule alert the case is created in case management for future monitoring and escalated to CO for review and approval.
5. Mark the customer as high risk and should conduct an EDD for future transactions However, the Compliance Officer can block the customer for future transactions based on the severity of the issue.butthe customer privacy should be maintained and no staff should refuse customer on the ground that he has been refused for transactionbecause STR has been filed on him/her or he is marked high risk and further inestigation ison him/her.
6. Come up with the decision whether it should be reported (STR) to FIU.

9.9.5 TIPPING OFF

The Bank Secrecy Act BSA requires all officers, employees, and agents of reporting entities to exercise the utmost confidentiality on issues related to money laundering and terrorist financing.

All staff should note that he/she must not inform any customer/colleague that the customer is being scrutinized for possible involvement in suspicious activity related to money laundering, or that a competent authority is investigating his possible involvement in suspicious activity relating to money laundering or terrorist financing. If the employee reasonably believes that performing CDD will tip-off a customer or potential customer, employee may choose not to pursue that process. If the employee decides to do so then he/she must promptly notify the CO who will decide whether an STR should be filed.

When reporting suspicious transactions to the FIU, the business house are obliged to maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and to make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person.

Pursuant to the Bank Secrecy Act BSA a person (and without prejudice to the generality of the foregoing a reporting entity, its officers, employees or agents) who, knowing or suspecting that;

A person commits a tipping-off offence if;

a) A person discloses to the customer that his activities and/or behaviour is subjected to STR.
b) Sending out STR copies to suspected persons or entities and or spreading to internal Staff.
c) A person discloses to the third party or the Customer involved that an investigation is on-going.
d) Any such disclosure is likely to prejudice any investigation that might be conducted following the disclosure.
e) The disclosure reaches the person involved or the third party of the crime giving them enough time to destroy evidence or prepare for their defence or escape.

9.9.6 TIPPING-OFF OFFENCE

It is an offence to notify or disclose (i.e tipping-off) information to a customer or any third party in relation to an STR submitted in accordance with the Bank Secrecy Act BSA.

10. ANTI-MONEY LAUNDERING & COMPLIANCE EMPLOYEE TRAINING

10.1 INTRODUCTION

Employee training is one of the four pillars of an effective AML/CFT program and key to any financial institution's fight against money laundering and terrorist financing. Comprehensive AML/CFT training is provided to all employees, including senior management ,Directors and CEO/Founder.

10.2 OBJECTIVES

To help employees recognize suspicious activity that may be related to money laundering or terrorist financing; to instruct them as to how to proceed in such cases; to comply with laws and regulations; and to help them keep abreast of changes in laws, rules, regulations, policies and procedures.

Moreover, the provision of training:

- Enhances staff knowledge and skills and enables them to successfully fulfil their duties and responsibilities.
- Upgrades the product knowledge of front line, operations and support services staff, thereby assisting in the sales process and business development.

The topics in Training will include:

General information: Background and history pertaining to money laundering controls, what money laundering and terrorist financing are, why the bad guys do it, and why stopping them is important;

a. The identification and prevention of money laundering;
b. Follow-up procedures for unusual or suspicious activities;

Also covered in the training will be topics on;

- Legal framework: How the AML/CFT Laws apply to institutions and their employees
- Responsibility of the employees under local laws and regulations for obtaining sufficient evidence of identity, recognizing, and reporting knowledge or suspicion of money laundering and terrorist financing
- Sanctions for anti-money laundering violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment
- How to react when faced with a suspicious client or transaction & procedures for reporting suspicious transactions
- How to respond to customers who want to circumvent reporting requirements

- Internal policies, such as customer identification and verification procedures and CDD policies
- Legal recordkeeping requirements
- Suspicious Transaction reporting requirements
- Currency transaction threshold reporting requirements
- Duties and accountability of employees
- Tipping off
- Record Retention.

The Compliance Officer will be responsible for coordinating the necessary training and will maintain records of training courses and those employees who attend training.
The training will be documented and provided to FIU/ CBS, when requested, that all relevant members of staff have received training on the matters listed above.

10.3 TRAINING RECORDS

The records showing the dates when AML/CFT training was given, the nature of the training and the names of the staff who received the training will be maintained. On successful completion of the training, the employees are issued certificates.

10.4 TRAINING FREQUENCY

The frequency of AML/CFT training is conducted as follows:

New employees:
Fresher: Immediately before commencing work on the counter.
Experienced: within 3 months from joining.
In addition to this, staff will also be sent to AML/CFT trainings to external agencies

Assessment: All attendees in the training program are assessed and the results of the testing process forms one of the factors determining the frequency of refresher training.

Training materials:
The topics covered by AML/CFT training are tailored to the different roles of employees and, thereby, the different levels of risk exposure they have.

The training material is reviewed and updated at regular intervals and whenever there is a change in AML/CFT laws, regulations, the Standards or the policies and procedures of the business house.

Our Training material includes the following topics:
General information:

- Background and history to money laundering and terrorist financing.
- ML/TF definitions, typologies and recent trends.
- What motivates criminals and why stopping them is important.
- AML/CFT legal and regulatory framework: How the laws, regulations and standards apply to business houses and their employees.
- Regulatory responsibilities, duties and accountability of employees.

- Industry guidance and other sources of information on AML/CFT.
- AML/CFT internal policies and procedures, such as customer identification and verification, including highlights on recent changes to mitigate the risks.
- Description of KYC process and its importance.
- CDD measures and procedures for monitoring transactions.
- Sanctions screening and PEP screening procedures.
- AML/CFT risks associated with the products and services provided by the Next Layer.
- Emerging ML/TF risks and measures to mitigate these risks.
- Red flags to identify unusual or suspicious transactions, patterns or customer behaviour.
- How to react when faced with a suspicious client or transaction.
- Requirements and procedures for internal and external reporting of suspicious transactions.
- Tipping off.
- Role of the Compliance Officer
- Role of the employees in AML/CFT
- Sanctions for non-compliance with AML/CFT laws and regulations, including criminal and civil penalties, fines and jail terms.
- Disciplinary action for non-compliance with AML/CFT laws, regulations or internal policies and procedures, including termination of employment.
- Cash transaction threshold reporting requirements.
- How to respond to customers who attempt to circumvent transaction reporting requirements.
- Record retention.

Training records:
Following records are maintained:
- Training registers to verify the training history of each employee.
- Training materials.
- Employee sign-off forms.

11. OBLIGATIONS TO MAINTAIN ACCOUNTS IN TRUE NAME

a) We should maintain records in the legal names of the account holders.

b) We should not open, operate or maintain any anonymous account or any account which is in a fictitious, false or incorrect name.

12. MALICIOUS REPORTING

Pursuant to the Bank Secrecy Act BSA any person who wilfully gives any information to the FIU or to an authorised officer, knowing such information to be false, commits an offence and is liable on conviction.

13. RECORD KEEPING REQUIREMENTS

FinCEN has established recordkeeping requirements that apply to financial institutions and other entities subject to the BSA. The specific requirements depend on the type of institution and the nature of the transactions or activities

involved, but some general recordkeeping requirements include:

Currency Transaction Reports (CTRs): Financial institutions are required to maintain a record of each currency transaction that exceeds $10,000 and file a CTR with FinCEN. The record must include the name and address of the person conducting the transaction, the amount and type of currency involved, and the identity of any other parties to the transaction.

Suspicious Activity Reports (SARs): Financial institutions are required to maintain a record of each SAR filed with FinCEN. The record must include a copy of the SAR, any supporting documentation, and any other relevant information.

Customer Identification Program (CIP): Financial institutions must maintain a record of the information used to verify the identity of each customer, including their name, address, date of birth, and other identifying information.

Customer Due Diligence (CDD): Financial institutions are required to maintain a record of the beneficial owners of each legal entity customer, including their name, address, date of birth, and other identifying information.

Record Retention: Financial institutions must maintain records of transactions and other activities subject to AML regulations for a specified period of time, which may vary depending on the type of record and the regulatory requirements. For example, CTRs must be retained for at least five years, while SARs must be retained for at least five years after the date of the last suspicious activity.

13.1 RECORD RETRIEVAL PROCEDURES

The objective of record keeping is to ensure that we should be able to provide the basic information about the customer and to reconstruct the transactions undertaken at the request of the relevant authorities at any given time. The KYC and due diligence documents can be stored in soft / hard copies.
All outward and inward remittance transaction records, foreign currency exchange transaction records will be stored date wise / transaction wise either in the branch or at any secured place based on the volumes. Any request for old records will be documented and the relevant records made available within a reasonable period of say 3 days or as specified by the relevant authority making the request.

13.2 EMPLOYEE SCREENING (KYE- KNOW YOUR EMPLOYEE)

Employees are the most important assets in the . In order to ensure that these assets are also our most powerful defence against money laundering and terrorist financing we should recruit employees with high level of integrity and ethics.

Next Layer takes below listed measures before hiring the employee:

a) A police clearance certificate
b) Collecting of academic qualifications shall be done.
c) Professional Reference
d) Copy of a Valid National Identity card or Passport
e) Curriculum Vitae

14. OBLIGATIONS OF THE EMPLOYEES

Under the BSA and AML regulations, employees have several obligations, including: Training: Financial institutions must provide training to employees on the institution's AML policies and procedures. This training must be appropriate for the employee's position and responsibilities, and must be provided on a periodic basis.

Suspicious Activity Reporting: Employees are required to report suspicious activity to the institution's designated AML officer, who is responsible for determining whether to file a Suspicious Activity Report (SAR) with the Financial Crimes Enforcement Network (FinCEN). Employees must be trained on how to identify and report suspicious activity.

Customer Due Diligence: Employees are responsible for verifying the identity of customers and, for certain types of accounts, identifying and verifying the identity of beneficial owners of legal entity customers. This information is used to assess the risk of money laundering or terrorist financing associated with a particular account.

Recordkeeping: Financial institutions must maintain records of transactions and other activities subject to AML regulations. Employees are responsible for ensuring that the necessary records are created and maintained in accordance with regulatory requirements.

Compliance Oversight: Financial institutions are required to have a compliance program that includes oversight by senior management or a compliance officer. Employees are responsible for following the institution's AML policies and procedures, and for reporting any concerns or issues to the designated AML officer.

14.1 DISCIPLINARY ACTION FOR NON-COMPLIANCE WITH INTERNAL POLICIES AND PROCEDURES AND AML/CFT LAWS

A Non-compliant behaviour can lead to sanctions and penalties from Supervisory Authorities. Depending upon the nature of the non-compliance an employee may be subject to;

- Oral warning
- Written warnings
- Suspension with/without pay
- Termination

15. CORE OBLIGATIONS OF NEXT LAYER

These core obligations can be summarised as follows:

- Registering with FIU. FIU has implemented the goAML platform, an integrated software system developed by the United Nations Office on Drugs and Crime (UNODC) for Financial Intelligence Units worldwide.
- Appointment of an appropriately qualified and experienced Compliance Officer (CO) with responsibility for AML compliance, and to establish and maintain internal procedures and systems (including an audit function and training programme) sufficient to ensure compliance adherence;
- Applying customer due diligence (CDD) measures, and Know Your Customer" (KYC) measures, using a risk-based approach, in respect of all customers, business relationships and transactions;
- Conducting ongoing monitoring of business relationships, including paying special attention to complex, unusual or large transactions with no apparent economic/lawful purpose, and relationships and transactions with persons in high-risk jurisdictions;
- Stops and terminate any existing business relationship whenever unable to apply CDD or ongoing monitoring;
- Ensures maintaining of records, including records of all prescribed CDD measures and all transactions and related correspondence, for at least seven years from the transaction or correspondence date or the end of the business relationship;
- To establish and maintain procedures and systems to implement independent audit arrangements to test our procedures and systems relating to anti-money laundering and terrorist financing activities.
- Submit an annual compliance report to the supervisory authority for information within 90 days after each calendar year
- Report suspicious transactions or attempted transactions to the FIU; and
- To make disclosures required by the FIU, supervisory authority and relevant laws and regulations.
- Report transaction that is carried out by or through it involving cash transactions of 50,000 or more or the equivalent money in the currency of other countries to CBS Financial Surveillance Division on a daily basis.
- Report transactions of our customers involving 5,000 or more or the equivalent money in the currency of other countries to FIU on a weekly basis.

Bank Secrecy Act BSA reflect a risk-sensitive approach to due diligence and monitoring by reporting entities. Next Layer adopts a well organised and systematic approach for conducting CDD and ongoing monitoring of customers according to the different risk ratings of those customers. We follow FATF risk-based approach on defining the type of customer and transaction risk. We apply simplified due diligence" in certain situations that are deemed to be low-risk for money laundering and financing of terrorism and required to implement enhanced measures in situations that are deemed to be high risk.

Next Layer apply CDD measures to all its customers on risk-sensitive basis. This is an overarching, continuing requirement which applies to all customers. Hence it is able to demonstrate to the supervisory authority and to the FIU, that our internal procedures for ongoing CDD are sufficient in light of the particular risks inherent in

our business. Once the identity of a particular customer has been verified and the nature of their business is sufficiently understood, no further evidence of identity needs to be collected unless there is any reason for suspicion, for instance if there is a marked change in the nature or volume of business passing through the account. Next Layer has developed a frame set of the customer profiles based on CDD information obtained. A customer profile will facilitate the ongoing monitoring of accounts and transactions and assist us to identify suspicious transactions or patterns of transactions.

16. COMPLIANCE AUDIT

In accordance with the Bank Secrecy Act BSA a reporting entity shall establish and maintain procedures and systems to implement independent audit arrangements to test its procedures and systems relating to anti-money laundering, and terrorist financing activities.

Next Layer will appoint internal auditors to conduct a comprehensive annual review of the effectiveness of its AML/CFT controls and procedures and also to;

• Examine the adequacy of CDD policies, procedures and processes, and whether they comply with internal requirements.

• Perform appropriate transaction testing, with particular emphasis on high-risk operations products, services, customers and geographic locations) on sample testing basis.

• Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.

• Assess compliance with applicable laws and regulations.

• Examine the integrity and accuracy of management information systems used in the AML compliance program if any.

• Reviewing policies, procedures, and processes for suspicious activity monitoring.

• Determining the system effectiveness for reports, blacklist screening, flagging of unusual transactions and more.

• Review Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transactions. Testing should include a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines (e.g., legal, private banking, foreign correspondent banking) to the personnel or department responsible for evaluating unusual activity.

• Assess the adequacy of record keeping.

17. RERIODIC REPORTING TO FIU AND SUPERVISORY AUTHORITY

In the United States, the Financial Crimes Enforcement Network (FinCEN) is the FIU. It operates under the U.S. Department of the Treasury and is responsible for administering and enforcing the Bank Secrecy Act (BSA) and other anti-money laundering (AML) regulations.

FinCEN's mission is to safeguard the financial system from illicit use, and to promote national security through the collection, analysis, and dissemination of financial intelligence. It serves as a central point for the collection and analysis of financial transaction data reported by financial institutions and other entities subject to the BSA.

FinCEN works closely with law enforcement agencies at the federal, state, and local levels to investigate and prosecute financial crimes. It also provides guidance and support to financial institutions, regulators, and other stakeholders in order to promote compliance with AML regulations and to improve the effectiveness of the financial system in preventing financial crimes.

The following are the FinCEN reporting threshold requirements for some of the most commonly reported activities:

Currency Transaction Report (CTR) - Financial institutions are required to file a CTR with FinCEN for each currency transaction that exceeds $10,000.

Suspicious Activity Report (SAR) - Financial institutions are required to file a SAR with FinCEN for any suspicious activity that involves at least $5,000 in funds or other assets.

Foreign Bank and Financial Accounts Report (FBAR) - U.S. persons are required to file an FBAR with FinCEN if they have a financial interest in, or signature authority over, one or more foreign financial accounts that have an aggregate value exceeding $10,000 at any time during the calendar year.

Customer Due Diligence (CDD) - Financial institutions are required to establish and maintain a CDD program that includes identifying and verifying the identity of customers and beneficial owners for certain types of accounts, including accounts for legal entities.

Beneficial Ownership (BO) - Financial institutions are required to identify and verify the beneficial owners of legal entity customers that open accounts after May 11, 2018.

17.1 CASH TRANSACTION THRESHOLD REPORTS (CTTR)

Under the BSA, financial institutions, including banks and credit unions, are required to file a Currency Transaction Report (CTR) with the Financial Crimes Enforcement Network (FinCEN) for transactions involving currency over $10,000. The report must include the name, address, and Social Security number or taxpayer identification number of the person making the transaction, as well as other details about the transaction.

.

17.1.3 FAILURE TO REPORT CASH TRANSACTION

In line with the Bank Secrecy Act BSA a reporting entity, which fails to report a cash transaction or wire transfer under or materially misrepresents the amount of such transaction, commits an offence and is liable to a fine for each such failure.

17.2 COMPLIANCE REPORT

In line with Regulation the AML/CFT Regulations, the Compliance Officer shall prepare and submit an annual compliance report to the supervisory authority for information within 90 days after each calendar year and the reporting entities who have not more than five staff members may request authorisation from their respective supervisory authority to submit a compliance report, as may be determined by the supervisory authority, for information.

The Compliance Officer shall submit the Compliance report between 1 January and 31 March of each year to the supervisory authority.

18. ACKNOWLEDEGEMENT

I acknowledge that I have read and understood the provisions of Next Layer's Anti-Money Laundering and Countering of Terrorism Financing Policies and Procedures manual and I am bound to act and abide by them as part of my contract of employment.

I shall perform my duties with due skill, care and diligence pursuant to instructions and/or training received from time to time and to the AML/CFT Policies and Procedures at all times and keep up the Know Your Customer standards.

I will consider the AML/CFT Policy and Procedures, as of paramount importance and agree that they will take precedence over other commercial aspects of managing business and customer relationships.

I further undertake promptly to report any suspicious transactions to the Compliance Officer. I also undertake no to disclose to or inform customer whose transaction is being scrutinized of such action or of any other action taken by the or by the relevant authorities to scrutinize or verify the unusual/suspicious transactions under the relevant laws for the time being.

I also understand the importance of maintaining the confidentiality of customer information. I will keep secure all personal data including name, addresses and other details of the customer. I also undertake that I will not disclose or publicize customer personal data to third parties unless the purpose of disclosure is legitimate, and it is required by regulatory authority.

I hereby sign the undertaking as a token of my compliance with the above and shall remain immune from any criminal, civil or administrative liability and action unless any of my disclosure/reporting is proved tom be made with malicious intention to harm the concerned customer.

Name of Employee: ……

Signature of Employee …… Date:……..

ANNEXURE I-INDICATORS OF SUSPICIOUS SERVICES AND TRANSACTIONS

Below are some examples of suspicious activity in which you could encountered while conducting business.

Suspicious customer behaviour

- Customer is secretive and reluctant to meet in person
- Customer has an unusual, nervous, or excessive demeanour
- Customer is accompanied and watched
- Customer insists that a transaction be done quickly or volunteers the information that a transaction is clean
- Customer shows uncommon curiosity or level of knowledge about record keeping or reporting requirements
- Customer attempts to deter compliance with record keeping or reporting duties, through threats or otherwise
- Customer presents inconsistent or confusing details about a transaction or does not appear to understand it
- Customer appears to have only informal records of significant or large volume transactions
- Customer is reluctant to proceed with a transaction after being told it must be reported
- Customer suggests payment of a gratuity or unusual favour
- Family members or close associates of public officials (PEPs) begin making large transactions not consistent with their known legitimate sources of income.

Suspicious customer identification circumstances:

- Agent, attorney, or financial advisor acts for another person without proper proof of authority.
- Customer is unwilling to provide personal identity information or wants to establish identity using unofficial documents.
- Customer furnishes unusual, suspicious, or inconsistent identification documents is unwilling to provide personal background data;
- Customer is unusually slow in providing supporting documentation or cannot provide properly certified copies.
- Customer spells name differently from one transaction to another, uses alternative names, or uses a consistent address but frequently changes the names of persons involved
- Customer's telephone is disconnected.
- Business customer is reluctant to reveal details of business activity or beneficial ownership
- Business customer is reluctant to provide financial statements and other documents or presents documentation noticeably different from those of similar businesses

Suspicious employee activity:

- Employee exaggerates the credentials, background, financial ability, and/or resources of a customer in internal reporting.
- Employee lives a lifestyle that cannot be supported by his/her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy.
- Employee permits or facilitates transactions where the identity of the ultimate beneficiary or counterparty is not disclosed.
- Employee assists transactions where the identity of the ultimate beneficiary or counter party is disclosed;
- Employee avoids taking holidays

Suspicious Commercial Account Activity

- Business customer presents financial statements noticeably different from those of similar businesses;
- Customer maintains an inordinately large number of accounts for the type of business purportedly being conducted.

Miscellaneous Suspicious Customer Activity: Agent, attorney of financial advisor acts for another person without proper documentation such as power of attorney.

The following examples have been collated from the websites of other FIUs and the FATF. They are not comprehensive or exhaustive and are provided for indicative purposes only.

General risk indicators

- Transactions or business relationships with countries known to have weak AML/CFT controls, as narcotic source countries, or countries known for highly secretive banking and corporate laws (high-risk countries), especially if transactions are complex and involve intermediaries
- Transactions, business activity, or frequent international travel not consistent with customer profile or known legitimate sources of income/wealth
- Unusually/unnecessarily complex or „layered" movement of funds Transactions involving suspected shell entities (corporations with no legitimate reason for existence).
- Large one-off cash transactions without proof of origin of funds
- Frequent and large international money transfers without clear economic reason. Sudden changes in volume or nature of business activity
- Services or transactions for the benefit of persons suspected to be criminals, or persons related to or closely associated with them
- Uncharacteristically large transactions or deposits by family members or associates of public officials (PEPs)
- Client or customer maintains an inordinately large or complex network of accounts / business entities for the type of business purportedly being conducted
- Business client cannot be identified online or in official registers
- Use of undisclosed intermediaries/agents/nominees

Wire transfers

- All transfers to or from high-risk countries that are inconsistent with a customer's business or profile or not satisfactorily explained.
- Frequent wire transfers in large round amounts
- Large number of wire transfers between two accounts without clear economic or business purpose, especially if performed through high-risk countries
- Client sends wire transfers to a country where his company has no business relations or receives wire transfers from legal entities with which he has no business relations.
- Client sends periodic wire transfers from a personal account to a high-risk country without reasonable explanation.
- Large incoming wire transfers on behalf of a foreign client without reasonable explanation, particularly if described as loans from foreign lender
- Funds transferred in and out of an account on the same day or within a relatively short period of time, without reasonable explanation
- U-turn transactions – funds transferred out of jurisdiction and then portion quickly returned, or vice versa.
- Wire transfer payments or receipts with no apparent links to legitimate contracts for goods or services
- Transfers routed through multiple foreign or domestic banks

Part 2	Information on Person/Entity Engaging in Suspicious Activity or Transactions

ANNEXURE VIII- TYPES OF RISKS

Business Risk

Dealers in precious stones and metals
Dealers in real estate
Dealers in used cars
Dealers in luxury goods
Trusts
Auction houses
Non-Profit organizations
Societies such as co-operative societies, charitable institutions, social and professional societies
Companies with what appears to be an unusually or excessively complex ownership structure given the nature of the company's business
Companies that have nominee shareholders or shares in bearer form
Offshore companies
Cash-intensive companies
Foreign financial institutions for banknote exports and imports
Local or foreign entities with whom the Next Layer partners to offer specialized products or services
Commercial brokers or agents

Geographic risk

Customer's country of birth or residence
Country of establishment or incorporation of the customer's business
No physical presence in the country named
A country that has been identified by FATF as high risk or 'non-cooperative'.
A country that has been reported as being involved in drugs, having a high level of corruption or any other criminal activity.
A country that provides funding or support for terrorist activities or that has designated terrorist organizations operating within the country.
A country subject to sanctions, embargos or similar measures issued by, for example, the United Nations.

Customer risk

The customer is reluctant to provide additional details pertaining to the transaction or is conducting a transaction that does not match his profile.
The customer is unwilling to disclose the beneficial owners of a legal entity.
The customer is non-resident.
The customer is a politically exposed person ('PEP'), or a legal entity owned or controlled by a PEP.

Transaction risk

The customer requests a third-party transaction, i.e. to perform a transaction on behalf of another natural person or legal entity.
The customer seeks to conduct a complex or unusually large transaction or unusual pattern of transactions that has no apparent legitimate financial or commercial purpose.
There are difficulties in verifying the source of wealth and origin of the customer's assets.
Non-face-to-face transactions.
Any other transaction that is considered as high risk in accordance with risk assessment.

Correspondent banking risk

Geographic risk: transactions that originate or terminate in high risk jurisdictions
Correspondent bank risk profile: the regulatory environment that it is situated in.