Guidelines on
Prevention of Money Laundering
&
Combating Financing of Terrorism

Green Delta Securities Limited

Table of Content

List of Abbreviations

GDSL	:	Green Delta Securities Limited.
ML/TF	:	Money Laundering/ Terrorist Financing
AML/CFT	:	Anti-Money Laundering/Combating the Financing of Terrorism
BFIU	:	Bangladesh Financial Intelligence Unit
APG	:	Asia Pacific Group on Money Laundering
ATA	:	Anti Terrorism Act
ATO	:	Anti Terrorism Ordinance
BB	:	Bangladesh Bank
BDT	:	Bangladesh Taka
CMI	:	Capital Market Intermediaries
CDD	:	Client Due Diligence
CTC	:	Counter Terrorism Committee
CEO	:	Chief Executive Officer
FATF	:	Financial Action Task Force
FCBs	:	Foreign Commercial Banks
FlU	:	Financial Intelligence Unit
GoB	:	Government of Bangladesh
ICRG	:	International Cooperation Review Group
KYC	:	Know Your Client
MD	:	Managing Director
MLPA	:	Money Laundering Prevention Act
MLPO	:	Money Laundering Prevention Ordinance
NCC	:	National Coordination Committee on AML/CFT
NCCT	:	Non-cooperating Countries and Territories
PM	:	Portfolio Manager
STR	:	Suspicious Transaction Report
SAR	:	Suspicious Activity Report
UNCAC	:	United Nations Conventions Against Corruption
UNODC	:	UN Office on Drugs and Crime
UNSCR	:	United Nations Security Council Resolution

1. Introduction

1.1. REGULATORY REGIME

As per Anti Money Laundering Act, 2012 Bangladesh Bank has included all stock broker and stock dealers, portfolio managers and merchant bankers, securities custodian and asset managers as reporting agency (Ref: BFIU Circular No: 06/2012 dated 30/12/2012). Bangladesh Bank has also issued directives to all institutions related to capital market or Capital Market Intermediaries (CMI) in the mentioned circular to prevent money laundering and combat terrorist financing as reporting agency.

1.2. RISK MANAGEMENT STRATEGY

a. All CMI need to establish an 'Anti Money Laundering and Combating Financing of Terrorism Compliance Unit (AML/CFT Compliance Unit) headed by a senior executive of the organization, And if applicable, CMI will establish internal monitoring and control system by designating an officer at branch level. CMI will also develop strategies and programs to define AML/CFT Compliance Unit's work area and duties and prepare a detailed guideline which will be approved by the board of directors.

b. Every CMI will arrange "Independent Audit" after certain period interval to mitigate risks regarding AML/ CFT.

1.3. KNOW YOUR CUSTOMER

a. All CMIs need to collect correct and detail information of their customers and preserve the documents for specified time mentioned in the circular.

b. All CMIs need to update all existing client's information that opened accounts before September 30, 2010.

c. Every CMI will have a detailed Customer Acceptance policy.

d. CMI will ensure Customer Due Diligence.

e. All customers' information need to be updated after certain period interval.

f. Identify Beneficiary Owners of based on collected documents and other sources.

g. CMI will adopt enhanced due diligence for Politically Exposed Persons (PEPs).

1.4. TRANSACTION MONITORING AND SUSPICIOUS TRANSACTION IDENTIFICATION AND REPORTING

a. CMI will report to all suspicious transactions as per provided format to Bangladesh Financial Intelligence Unit, Bangladesh Bank.

b. If BO or related account's applicant (individual or institution) or beneficiary whose name is black listed by UN Security Council or Government of Bangladesh or any other suspicious individual or institution will be also reportable to Bangladesh Bank by CMI.

c. CMI will report to Bangladesh Bank on half yearly basis according to prescribed format.

d. CMI will not disclose any information related to suspicious transaction to client or other individual or institution at any stage.

1.5. OTHER DIRECTIVES:

a. CMI will follow proper screening mechanism to appoint own officers to mitigate AML/CFT risks.

b. CMI will arrange internal training for all officers to ensure awareness regarding AML/CFT

c. Acts, directives or any other legal publications.

d. CMI will prepare a guideline titled "Guidelines on prevention of money laundering and combating financing of terrorism for capital market intermediaries" which need to be approved by the board of directors of CMI.

e. Prepared and approved Guideline needs to be submitted to Bangladesh Bank within 3 months from the date of circular.

1.6. APPLICABILITY OF GDSL GUIDANCE NOTES VIS-A-VIS GUIDANCE NOTES ISSUED BY THE BFIU

As per the guideline issued by BFIU (Circular no 06/2012) of Bangladesh Bank GDSL developed the policy incorporating the followings:

a. Policy positions of Cosmopolitan Finance Limited (GDSL) on Anti Money Laundering and Anti — Terrorism Finance issues; and

b. Guidance on how to implement those policies in practice during day-today operations.

These GDSL guidance notes have been prepared keeping in mind the **Guidance Notes on Prevention of Money Laundering and Terrorist Financing** issued by the Bangladesh Financial Intelligence Unit (BFIU) of Bangladesh Bank. While every effort has been made to include all relevant aspects of the Guidance Notes on Prevention of Money Laundering and Terrorist Financing issued by the BFIU, circumstances may arise where specific guidance may not be available in the GDSL guidance notes. In such circumstances, the **Guidance Notes on Prevention of Money Laundering and Terrorist Financing** issued by the BFIU shall be consulted and followed.

This page intentionally left Blank

2. Basic of Money Laundering & Terrorist Financing

2.1. WHAT IS MONEY LAUNDERING

Money laundering can be defined in a number of ways. But the fundamental concept of Money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origins. Most countries subscribe to the definition adopted by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention, 1988) and the United Nations Convention against Transnational Organized Crime (the Palermo Convention, 2000).

According to Section 2(v) of the Money Laundering Prevention Act 2012 (MLPA 2012):
"Money laundering means -

i. Knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:-
    1. Concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
    2. Assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;
ii. Smuggling money or property earned through legal or illegal means to a foreign country;
iii. Knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or
iv. Concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;
v. Converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;
vi. Acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;
vii. Performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;
viii. Participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above;"

2.2. TERRORIST FINANCING

Terrorist financing can be simply defined as financial support in any form of terrorism or of those who encourage, plan, or engage in terrorism. In this guideline, the term "terrorist financing" has the same meaning as in Article 7 of the Anti Terrorism (Amendment) Act, 2012 in the following manner:

i. Suppression of the Financing of Terrorism (1999), United Nations defines TF in the following manner: Suppression of the Financing of Terrorism (1999), United Nations defines TF in the following manner: If any person or entity knowingly provides or expresses the intention to provide money, services, material support or any other property to another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person, entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

ii. If any person or entity knowingly receives money, services, material support or any other property from another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

iii. If any person or entity knowingly makes arrangement for money, services, material support or any other property for another person or entity where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

iv. If any person or entity knowingly instigates another person or entity to provide or receive or make arrangement for money, services, material support or any other property in such a manner where there are reasonable grounds to believe that the same have been used or may be used in full or partially by a terrorist person or entity or group or organization for any purpose, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

2.3. THE LINK BETWEEN MONEY LAUNDERING AND TERRORIST FINANCING

The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. Funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of fund for terrorist activities, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

A significant difference between money laundering and terrorist financing is that the funds involved in terrorist financing may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets to persons/organizations (e.g. foundations or charities) to support terrorist activities

2.4. THE REASON OF COMMITTING MONEY LAUNDERING & TERRORISM FINANCING

Criminals engage in money laundering for three main reasons:

First, money represents the lifeblood of the organization that engages in criminal conduct for financial gain because it covers operating expenses, replenishes inventories, purchases the services of corrupt officials to escape detection and further the interests of the illegal enterprise, and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.

Second, a trail of money from an offense to criminals can become incriminating evidence. Criminals must obscure or hide the source of their wealth or alternatively disguise ownership or control to ensure that illicit proceeds are not used to prosecute them.

Third, the proceeds from crime often become the target of investigation and seizure. To shield ill-gotten gains from suspicion and protect them from seizure.

Terrorism financing is done mainly to facilitate an extremist group by providing financial support aiming to establish or circulate their ideology. Such financial assistance may be provided directly or indirectly or may be attempted and amount of money may be significantly low with several in numbers.

2.5. WHY WE MUST COMBAT MONEY LAUNDERING

a. Money laundering has potentially devastating economic, security, and social consequences. Money laundering is a process to making crime worthwhile. It provides the fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal enterprises. This drives up the cost of government due to the need for increased law enforcement and health care expenditures to combat the serious consequences that result.

b. Money laundering diminishes government tax revenue and therefore indirectly harms honest taxpayers. It also makes government tax collection more difficult.

c. Money laundering distorts asset and commodity prices and leads to misallocation of resources. For financial institutions it can lead to an unstable liability base and to unsound asset structures thereby creating risks of monetary instability and even systemic crises.

d. One of the most serious microeconomics effects of money laundering is felt in the private sector. Money launderers often use front companies, which comingle the proceeds of illicit activity with legitimate funds, to hide the ill-gotten gains. These front companies have access to substantial illicit funds, allowing them to subsidize front company products and services at levels well below market rates.

e. The International Money Fund has estimated that the magnitude of money laundering is between 2 and 5 percent of world gross domestic product, or at least USD 800 billion to USD 1.5 trillion. In some countries, these illicit proceeds dwarf government budgets, resulting in a loss of control of economic policy by governments

f. Among its other negative socioeconomic effects, money laundering transfers economic power from the market, government, and citizens to criminals.

g. The social and political costs of laundered money are also serious as laundered money may be used to corrupt national institutions. Bribing of officials and governments undermines the moral fabric in society, and, by weakening collective ethical standards, corrupts our democratic institutions.

h. Money laundering erodes confidence in financial institutions and the underlying criminal activity, such as fraud, counterfeiting, narcotics trafficking, and corruption, weaken the reputation and standing of any financial institution. Actions by banks to prevent money laundering are not only a regulatory requirement, but also an act of self-interest. A bank tainted by money laundering accusations from regulators, law enforcement agencies, or the press risk likely prosecution, the loss of their good market reputation, and damaging the reputation of the country.

i. It is generally recognized that effective efforts to combat money laundering cannot be carried out without the co-operation of financial institutions, their supervisory authorities and the law enforcement agencies

2.6. STAGES OF MONEY LAUNDERING

There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a house, car or jewellery) to passing money through a complex international web of legitimate businesses and ‘shell’ companies (i.e. those companies that primarily exist only as named legal entities without any trading or business activities). There are a number of crimes such as bribery, extortion, robbery and street level sales of drugs where the initial proceeds usually take the form of cash that needs to enter the

financial system by some means. These proceeds of crime have to enter the financial system by some means so that it can be converted into a form, which can be more easily transformed, concealed or transported. The methods of achieving this are limited only by the ingenuity of the launderer and these methods have become increasingly sophisticated.

Despite the variety of methods employed, money laundering is not a single act but a process accomplished in 3 basic stages which are as follows:

- Placement - the physical disposal of the initial proceeds derived from illegal activity.
- Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.
- Integration - the provision of apparent legitimacy to wealth derived criminally. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

a. The three basic steps may occur as separate and distinct phases. These steps may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity. They may also occur simultaneously or, more commonly, may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organization

2.7. VULNERABILITIES OF THE FINANCIAL SYSTEM TO MONEY LAUNDERING

Money laundering is often thought to be associated solely with banks and moneychangers. However, in reality financial institutions, both banks and nonbanks, including capital market intermediaries, are susceptible to money laundering activities. Whilst the traditional capital market investment do offer a vital laundering mechanism, particularly in the initial conversion of cash to stock. Capital market investments schemes are one of the most attractive vehicles to the launderer.
Laundering activities are therefore more susceptible

- Entry of cash into the financial system;
- Cross-border flows of cash; and
- Transfers within and from the financial system.

Some banks and non-banking financial institutions including capital market intermediaries may additionally be susceptible to the attention of the more sophisticated criminal organizations and “professional money launderers”. Such organizations, possibly under the disguise of front companies and nominees, may create large scale but false international trading activities in order to move their illicit monies from one country to another.

Investment and merchant banking businesses are more likely to find them being used at the layering and integration stages of money laundering. The liquidity of many investment products particularly attracts sophisticated money laundering since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.

The liquidity of a mutual funds may attract money launderers since it allows them quickly and easily to move their money from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy.

Lump sum investments in liquid products are clearly most vulnerable to use by money launderers, particularly where they are of high value. Payment in cash should merit further investigation, particularly where it cannot be supported by evidence of a cash based business as the source of funds.

Insurance and investment product providers and intermediaries should therefore keep transaction records that are comprehensive enough to establish an audit trail. Such records can also provide useful information on the people and organizations involved in laundering schemes.

This page intentionally left Blank

3. Vulnerabilities of ML/TF in Capital Markets

The securities products can be utilized in the layering and integration stages of money laundering once illicit assets are placed in the financial system.

3.1. BROKER-DEALERS

A specific vulnerability associated with broker-dealers is their reliance on another financial institution's CDD/KYC process. A broker-dealer might assume that, because another financial institution has opened an account for a Client, so the Client does not pose ML/TF risks for them. The CDD/KYC vulnerability is most problematic in relation to the funding of a securities account.

3.2. ASSET MANAGERS, CUSTODIAN AND PORTFOLIO MANAGERS

Role of the asset manager, custodian and portfolio manager is generally to advice on the composition of an investment portfolio or to hold securities of local or foreign clients or to manage the contents of investment accounts for retail or institutional Clients respectively.

Portfolio management typically involves the provision of financial services in a managed relationship with Clients who are often of high net worth. The value and complexity of products offered to high net worth Clients, together with the international nature of the business, make the provision of wealth management services potentially attractive to money launderers, to disguise their illicit assets. The custodian services, regardless the nationality of an investor, has same potential to money launderer as portfolio management and asset management services.

3.3. TRUST, NOMINEE, AND OMNIBUS ACCOUNTS

Trust and nominee accounts present ML/TF vulnerabilities in the layering and integration stages. An omnibus account is an account established for an entity that is acting as an intermediary on behalf of multiple individuals or entities. Accordingly when a CMI opens a bank account with its own name (pooled account) in a bank, then the accumulated fund of all Clients got the identity of CMI.

3.4. SHELL COMPANIES

Shell companies can also be used to introduce illicit funds into a financial system and/or generate illicit funds through manipulative or fraudulent securities activities, For example, a brokerage account can be opened in the name of shell companies and used to engage in fraudulent conduct with regard to low priced, illiquid, low

volume or privately placed securities. In addition, a shell company can be established to accept payments from criminal organizations for non-existent services. These payments, which appear legitimate, can be deposited into depository or brokerage accounts and used to purchase securities products that are easily transferable or redeemable.

3.5. MARGIN TRADING

One of the unique characteristics of the securities industry is that it can be used to both disguise the proceeds of criminal activity and to generate further profits. The use of margin account trading involves the investor borrowing funds to carry out trading. The securities themselves are used as collateral for the loan. By influencing the timing and value of trades (and leverage), a launderer can potentially use the proceeds of a scheme to generate more funds.

3.6. TRANSFER PRICING

Large capitalization stocks are subject to a high degree of transparency and, subject to general market forces, generally fluctuate within an established price band. It is noted, however, that the market price on small capitalization stocks, which may be rarely traded, can be subject to more extreme price movements. In addition, the price of such an illiquid stock may be substantially affected by relatively small transactions. This mechanism has been exploited for money laundering purposes where block trades of illiquid stocks are transacted at a pre-agreed price between two parties. In such transactions, parties agree to the initial purchase of an illiquid security at an artificially low price with the same security being bought back some time later by the original seller or an associate at a significantly higher price.

3.7. CHEQUES

Money launderers can purchase pay orders/bank draft, pay order with cash over a period of time or through a series of transactions in order to avoid threshold currency reporting requirements. These cheques can then be deposited into securities accounts until a desired amount is reached and used to purchase a security, which is then sold or transferred.

Cheques from a depository account also present ML/TF vulnerability because they may unreasonably affect the securities intermediary's risk analysis, in particular with respect to CDD/KYC obligations.

Another vulnerability identified is the increasing use of the securities industry in offshore jurisdictions by criminals attempting to avoid domestic seizure of their assets. The ease by with which funds could be

transferred electronically facilitates this. The use of this method of disguising funds has resulted in a reduction in the effectiveness of domestic seizure/forfeiture actions, marking a change in the laundering techniques used by criminals.

3.8. LOW PRICED SECURITIES AND PRIVATE PLACEMENT

Low priced securities refer to low-value equity interests in companies that are publicly traded or are about to become so. The issuers of these shares generally have legitimate business operations and revenue streams. However, some publicly traded low priced securities are really shell companies that may be used for a reverse merger. In any event, shares in these issuers will often be represented with physical securities that can be deposited with a securities intermediary. .These shares are not likely to be traded on traditional exchanges, but rather in Over-The-Counter ("OTC") markets or on bulletin boards. Such stocks typically have very low trading volume but, unlike bearer securities, ownership of these shares will often be registered with the issuer and/or a transfer agent. The ML/TF vulnerabilities posed by these securities are two- fold. First- these types of securities are often used to generate illicit assets through market manipulation, insider trading, and fraud.

Second- these securities can be acquired by investing illicit assets into a company that is about to become public.

3.9. SHORT SELLING

Short selling (where not approved) is a trading vehicle that can be linked to market manipulation or insider trading, which are both predicate offences that could be the basis for ML/TF.

3.10. INSIDER TRADING

Insider trading is unique to the securities industry and generates illicit assets. As a predicate offence for money laundering this type of misconduct is reportable as STR and has proven useful in assisting law enforcement and regulators prosecute such misconduct.

3.11. MARKET MANIPULATION

Market manipulation generally refers to conduct that is intended to deceive investors by controlling or artificially affecting the market for a security. In particular, the manipulator's purpose is to drive the price of a security up or down in order to profit from price differentials. There are a number of methods that manipulators use to achieve these results.

3.12. SECURITIES FRAUD

Securities fraud broadly refers to deceptive practices in connection with the buy and sale of securities. In this regard, securities fraud encompasses insider trading and market manipulation activities and poses significant ML/TF risks for the CMI.

3.13. STRUCTURAL VULNERABILITIES

In addition to the above, GDSL may experience structural vulnerabilities arising from:

a. Failure to develop sufficient capacity to verify the identity and source of funds of their clients.
b. Human resources lacking the adequate skills and training in tracing money laundering and terrorist financing activities.
c. Lack of anti-money laundering software to monitor and report transactions of a suspicious nature to the financial intelligence unit of the central bank,

3.14. THE BENEFITS OF AN EFFECTIVE AML/CFT FRAMEWORK

An effective AML/CFI regime reduces the possibilities of losses to the institutions originating from fraudulent activities. Proper Client identification procedures and determination of beneficial ownership provide specific due diligence for higher risk policies and ensure monitoring for suspicious activities. Such prudential internal controls play a vital role for the safe and sound operation of a financial institution. This enhances public confidence and permits investments in the capital market to be put into productive purposes that respond to consumer needs and help the productivity of the overall economy.

3.15. HOW GDSL CAN COMBAT ML/TF

One of the best methods of preventing and deterring money laundering is a sound knowledge of a Client's business and pattern of financial transactions and commitments. The adoption of procedures by which Banks, Financial Institutions and CMI "know their Client" is not only a principle of good business but is also an essential tool to avoid involvement in money laundering.

Thus efforts to combat money laundering largely focus on those points in the process where the launderer's activities are more susceptible to recognition and have therefore to a large extent concentrated on the deposit taking procedures of CMI i.e. the placement stage.

GDSL keep transaction records that are comprehensive enough to establish an audit trail.

3.16. GDSL's RESPONSIBILITIES

As a reporting organization under the purview of the Money Laundering Prevention Act (MLPA), 2012 GDSL's responsibilities are as follows:

3.16.1. With regard to Money Laundering

a. To maintain complete and correct information with regard to the identity of its customers during the opening and operation of their accounts;
b. To preserve previous records of transactions of any customer's account for at least 5 (five) years from the date of closure;
c. To provide Bangladesh Bank, on its demand, information maintained under (a) and (b) above;
d. To report any suspicious transaction or attempt of such transaction as defined under section 2(z) of the MLPA 2012 to Bangladesh Bank immediately on its own accord.

3.16.2. With regard to Terrorist Financing Activities

According to section 16 of Anti Terrorism (Amendment) Act, 2012, GDSL's responsibilities to combat financing of terrorism are –

a. To take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions which are connected to any offence under the Anti Terrorism (Amendment) Act, 2012 and if any suspicious transaction is identified, to spontaneously report it to the Bangladesh Bank without any delay. (For details please consult Chapter no 9 ATA 2009);
b. The Board of Directors, or in the absence of the Board of Directors, the Chief Executive Officer, by whatever name called, of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15, which are applicable to the reporting agency, have been complied with or not.

4. GDSL’s Institutional Policy

The following statements in this Policy Guidelines should be followed as the institutional commitments:

- All employees are required to comply with applicable laws and regulations and corporate ethical standards.
- All activities carried on by GDSL must comply with applicable governing laws and regulations.
- Each individual in GDSL is responsible to comply the rules and regulations in the normal course of their assignments. It is the responsibility of the individual to become familiar with the rules and regulations that relate to his or her assignment. Ignorance of the rules and regulations is no excuse for noncompliance.
- Staffs are directed to consult with a compliance officer or other knowledgeable individuals when there is a question regarding compliance matters.
- Employees will be held accountable for carrying out their compliance responsibilities.

In order to protect GDSL's reputation and to meet its legal and regulatory obligations, it is essential that GDSL should minimize the risk of being used by Money Launderers. With that view it will be an obligatory responsibility for all GDSL officials, customers and management of the GDSL to realize and combat the situation on this critical risk issues. Considering all these GDSL will ensure the following issues as the institutional policy:

a) Establish clear lines of internal accountability, responsibility and reporting. Primary responsibility for the prevention of money laundering rest with the nature of business which must ensure that appropriate control are in place and operating effectively and GDSL officers are adequately trained.

b) Given its importance in reputation and regulatory terms, the effectiveness of the money laundering prevention regime across all business should form part of the governance oversight responsibilities of all Branch Compliance officer (if applicable)

d) Establish an effective 'Know your customer' policy for the Branch which will contain a clear statement of management's overall expectation matching with local regulations and establishing specific line of responsibilities. Detail guideline on know your customer (KYC) are given in this guidelines. (If applicable)

e) Cooperate with any lawful request for information made by government agencies during their investigation.

5. Anti Money Laundering Policy

5.1. SENIOR MANAGEMENT COMMITMENT

a. The senior management of GDSL including the Managing Director/Chief Executive Officer and the Board of Directors are committed to ensure the compliances with their obligations under the law, which is most important element of a successful anti-money-laundering program.

b. Senior management is aware about that the corporate culture is as concerned about its reputation as it is about profits, marketing, and customer service. As part of GDSL's anti- money laundering policy GDSL will communicate clearly to all employees on an annual basis a statement from MD/CEO that clearly sets forth its policy against money laundering and any activity which facilitates money laundering. Such a statement will be the evidence of the strong commitment of the GDSL and its senior management to comply with all laws and regulations designed to combat money laundering.

5.2. WRITTEN ANTI-MONEY LAUNDERING COMPLIANCE POLICY

a. As per requirements of Guidance Notes on Prevention of Money Laundering, issued by Bangladesh Bank at a minimum, the Board of Directors of each CMI and other financial institution must develop, administer, and maintain an anti- money-laundering compliance policy that ensures and monitors compliance with the Act, including record keeping and reporting requirements. Such a compliance policy must be written, approved by the board of directors, and noted as such in the board meeting minutes. In regard to these requirements, GDSL has prepared this written AML policy to comply with the requirements.

b. This anti-money-laundering compliance policy establishes clear responsibilities and accountabilities within the GDSL to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using its facilities for money laundering and the financing of terrorist activities, thus ensuring that it comply with its obligations under the law.

c. These Policies are tailored to GDSL and is based upon an assessment of the money laundering risks, taking into account GDSL's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to money laundering.

d. It includes standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. Procedures should address its Know Your Customer ("KYC") policy and identification procedures before opening new accounts, monitoring existing accounts for unusual or suspicious activities, information flows, reporting suspicious transactions, hiring and training employees and a separate audit or internal control function to regularly test the program's effectiveness.

e. The anti-money laundering policies will be reviewed regularly and updated as necessary and at least annually based on any legal/regulatory or business/ operational changes, such as additions or amendments to existing anti-money laundering rules and regulations or business.

6. Organization Structure

6.1. STRUC TURE OF AML/CFT COMPLIANCE UNIT

Bangladesh Bank has directed all The Capital Market Intermediaries (CMI) to constitute an "AML/CFT Compliance Unit" headed by maximum one/two tiers below than the MD/CEO and Head of this unit shall directly report the MD/CEO. The head of other separate divisions (where applicable) may be member of AML/CFT Compliance Unit.

As per Bangladesh Bank guideline, the structure of GDSL AML/CFT Compliance unit is as follows:

Official Designation	AML/CFT Compliance Unit
Head of compliance	Head of AML/CFT Compliance Unit
Head of Financial	Member
Head of Business	Member
Head of IT	Member
Any Member of invitation	

6.2. FUNCTIONS OF AML/CFT COMPLIANCE UNIT:

a. The AML/CFT compliance unit will assess the various types of ML/TF risk e.g. product risk, service risk, customer risk, country risk, and establish necessary measures for preventing those risks.

b. It will review the AML/CFT policies regularly considering the risk based approach.

c. It will update the legal, regulatory, business or operational changes including AML/CFT rules or regulations as and when required but at least once a year.

d. It will implement the necessary AML/CFT policies, procedures and controls so as to deter criminals from adopting various techniques of ML/TF using their business services.

e. It will supervise the implementation of necessary measures for preventing ML/TF risk and assess the effectiveness of applied measures.

f. It will arrange necessary training for its staff.

g. It will ensure that necessary steps are taken to identify suspicious transaction and report the same to the BFIU directly.

h. It will place Memorandum (Assessment Report) before the Board of Directors/Appropriate Authority half yearly basis regarding the status of the AML/CFT initiatives undertaken by the GDSL. (Format given in **annexure-3**)

6.3. FUNCTIONS OF HEAD OF AML/CFT COMPLIANCE UNIT

a. Circulate BFIU circulars/instructions of BFIU and Policy Guidelines to the branches (if applicable) and concern offices.

b. Monitor, review and coordinate, implement and enforces CMI's AML/CFT Compliance Policies formulate the policy of identification procedure "Know your Client (KYC)" for detecting of suspicious transactions / account activities in line with the Circulars/Guidelines issued by BFIU, Bangladesh Bank.

c. Respond queries of the branches (if applicable) to money laundering and terrorist financing apprehensions.

d. Report to the BFIU, Bangladesh Bank regarding suspicious transactions/activities of the Clients.

e. Issue necessary instructions to the branches. (if applicable)

f. Ensure timely reporting of STR/SAR and compliance to the BFIU instructions.

g. Extend all sorts of cooperation to Internal Audit Team, BFIU Inspection Team and other Law enforcing Agencies as and when required and appropriate.

6.4. FUNCTIONS OF BRANCH/ UNIT HEAD (IF APPLICABLE)

a. The Branch/Unit head will ensure that the AML/CFT issues are in place in their Branch/unit and the respective law, BFIU circulars and instructions are meticulously followed at all level.

b. S/he will be responsible for educating and updating the officers of the branch regarding AML/CFT issues, circulars and strategies.

c. S/he will ensure that STR identification and reporting system is effectively in place within the branch/unit.

d. In the monthly meeting of the Branch the AML/CFT agenda will come as an important one and the proceedings shall be recorded properly.

e. In case of new accounts s/he shall ensure that the policy and identification procedure "Know your Client (KYC)" have been meticulously followed.

f. S/he will ensure the preservation of complete and up-to-date account records of the Clients.

g. S/he will ensure the periodical reporting of AML/CFT issues.

h. S/he will report the unusual/suspected transactions to AML/CFT compliance unit for further advice and guidance.

i. S/he will extend all sorts of cooperation to Internal Audit Team, BFIU Inspection Team and other Law enforcing Agencies as appropriate.

j. S/he will consider any negative information from any sources, matter of suspicion.

6.5. FUNCTIONS OF ACCOUNT OPENING OFFICER

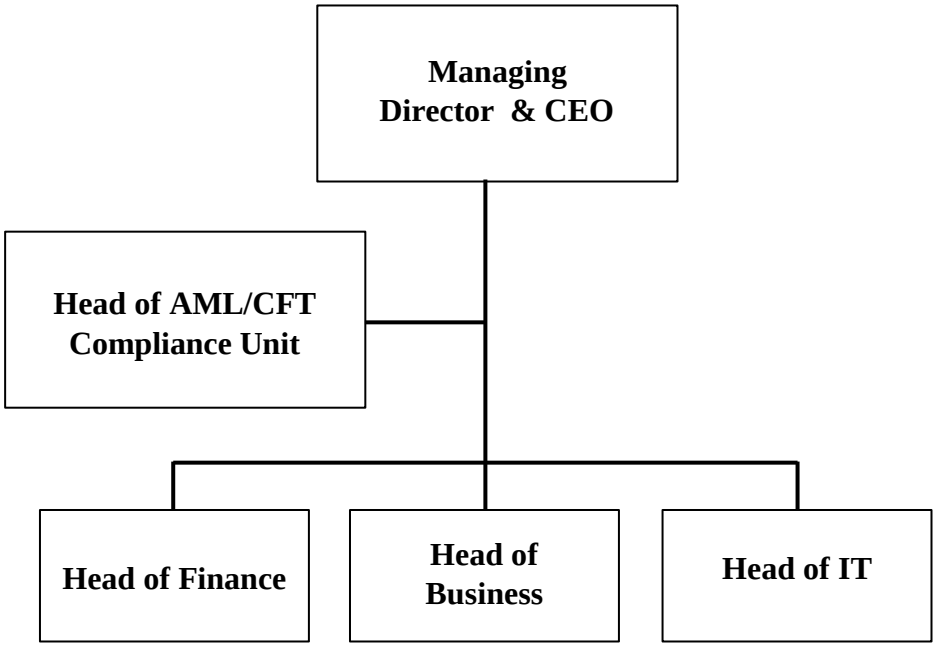
a. Perform due diligence on prospective clients prior to opening an account.

b. Shall be vigilant regarding the identification of account holder and the suspicious activity of a prospective client while opening an Account.

c. Ensure all required documentation is completed satisfactorily as per this Guideline.

d. In case of new accounts, s/he will follow the policy of identification procedure "Know your Client (KYC)" and analyze the track record accounts.

e. Ensure that customer information are verified and undertake reviewing of customer information after a certain period



7. Know Your Customer

7.1. KNOW YOUR CUSTOMER PROGRAM

The adoption of effective Know Your Customer (KYC) program is an essential part of GDSLs risk management policies. Having sufficiently verified/corrected information about customers - "Knowing Your Customer" (KYC) - and making use of that information underpins all AML/CFT efforts, and is the most effective defense against being used to launder the proceeds of crime.

GDSL with inadequate KYC program may be subject to significant risks, especially legal and reputation risk. Sound KYC Policies and Procedures not only contribute to the GDSLs overall safety and soundness, they also protect the integrity of its system by reducing money laundering, terrorist financing and other related offences.

7.2. KNOW YOUR CUSTOMER (KYC) PROCEDURE

Money Laundering Prevention Act 2012 requires all reporting agencies to maintain correct and concrete information with regard to identity of its customer during the operation of their accounts.

7.2.1. Nature of Customer's Business

When a business relationship is being established, the nature of the business that the customer expects to conduct with GDSL should be ascertained at the outset to establish what might be expected later as normal activity. This information should be updated as appropriate, and as opportunities arise. In order to judge whether a transaction is or is not suspicious, GDSL need to have a clear understanding of the business carried on by its customers.

7.2.2. Identifying Real Person

GDSL must establish to its satisfaction that it is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate any account, or transact business for the customer. Whenever possible, the prospective customer should be interviewed personally. This will safeguard against opening of fictitious account.

7.2.3. Document is not Enough

The best identification documents possible should be obtained from the prospective customer i.e. those that are the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine or as being sufficient to establish identity so verification will generally be a cumulative process. The overriding principle is that GDSL must know who its customers are, and have the necessary documentary evidence to verify this. Collection of document is not enough for KYC, identification is very important.

7.3. CUSTOMER PROFILING:

a. Followings are required:
   1. Obtaining and documentation of the customer's basic background information.
   2. Use the information to evaluate the appropriateness of the customer's transaction activity.
   3. Identifying the customer's source of fund.

b. KYC profile should disclose:
   - The customer expected transaction trend
   - The source of wealth
   - Net worth

c. KYC profile should be upgraded! Updated by:
   1. Regular review of transaction activity and balance fluctuation report
   2. Newspaper and Magazine article, financial statement, brochures, industry activities relating to the customer.
   3. Periodical discussion with the client relating to their business activities including future plan of the business for the next 12 month.

d. Customer Due Diligence (CDD):
   As per FATF new standards GDSL requires various Customer Due Diligence measures

7.3.1. Normal CDD measures:

a. Identifying the customer and verifying that customer identity using reliable, independent source documents, data of information,
b. Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner such as that GDSL is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include GDSLs understanding the ownership and control structure of the customer,
c. Understanding and as appropriate, obtaining information on the purpose and intended nature of the business relationship,
d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transaction being conducted are consistent with the GDSL's knowledge of the

customer, their business and risk profile, including where necessary the source of funds.

7.3.2. Enhanced Customer Due Diligence

GDSL should examine, as far as possible, the background and purpose of all complex, unusual large transactions and all unusual patterns of transactions which have no apparent economic or lawful purpose, where the risk of money laundering are higher, GDSL should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

CDD measures that could be applied for higher Risk business relationship include:

a. Obtaining additional information on the customer.
b. Obtaining additional information on the intended nature of the business relationship.
c. Obtaining information on the source of wealth of the customer.
d. Obtaining information on the reasons for intended or performed transaction.
e. Obtaining the approval of senior management to commence or continue the business relationship.
f. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.

7.3.3. Simplified Customer Due Diligence:

Simplified CDD measures are be applied in cases where GDSL is satisfied that the risk of money laundering or terrorist financing is low.

Circumstances of when the CMI might adopt lesser or reduced CDD measures are:

- Where reliable information on the client is publicly available to GDSL;
- GDSL is dealing with another financial institution whose AML/CFT controls it is well familiar with by virtue of a previous course of dealings; or
- the client is a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, or a listed company that is subject to regulatory disclosure requirements.

7.4. CUSTOMER ACCEPTANCE POLICY

Bangladesh Bank has recommended in the Guidance Notes on Prevention on Money Laundering to develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers including a

description of the types of customer that are likely to pose a higher than average risk to a GDSL. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered.

It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to financial services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as public figures or politically exposed persons should be taken exclusively at senior management level.

The guidelines for Customer Acceptance policy for the GDSL are as follows:

a. No account can be opened in anonymous or fictitious name.
b. Parameters of risk perception are clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers into different risk grade.
c. Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk.
d. Not to open an account or close an account where GDSL is unable to apply appropriate customer due diligence measures i.e. GDSL is unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to GDSL. Decision by the GDSL to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.
e. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practices of financial service as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.
f. Necessary checks before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.
g. The status of a customer may change as relation with a customer progresses. The transaction pattern, volume of a customer's account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measures to monitor customer's activities throughout the business relation.
h. No account should be opened in the name of listed in UN Sanction lists, and directed by Bangladesh Bank or any other sanction lists.

i. No account should be opened through Online. In case of foreign resident account may be opened through Bangladesh Mission or own GDSL branch if available or legal representative obtaining KYC, ETPs, source of income and risk grading.

j. No account should be opened for those customers for whom reports of unusual or suspicious transaction are repeatedly submitted to the BFIU, if it is known, account of such person /entity should not be opened

k. No account should be opened for that customer for whom the collection of information for assessing their overall profile is impossible.

1. No account should be opened for that customer whose activities or transaction are not consistent with the information available on them, their professional activity, their risk profile and the origin of the fund.

m. No account should be opened for that customer failing to provide all information required for the identification and verification of their identity.

7.5. IDENTIFYING AND DEALING WITH PEPs

PEPs are individuals who are or have been entrusted with prominent public functions of a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Another important thing is that not only client, a PEP but also may be a beneficial of an account.

PEPs accounts must be marked as High Risk accounts and consider the followings while opening and maintaining the accounts of any PEPs, GDSL must in place the following Enhanced Due Diligence (EDD):

- Have appropriate risk-management systems to determine whether the client or the beneficial owner is a politically exposed person;
- Obtain senior management approval for establishing (or continuing, for existing clients) such business relationships;
- Take reasonable measures to establish the source of wealth and source of funds; and conduct enhanced ongoing monitoring of the business relationship.

7.6. CUSTOMER IDENTIFICATION

Customer identification is an essential element of KYC standards. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a

need for GDSL to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if GDSL becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible. **No BO or related account will be opened in fictitious/false or anonymous name.**

Once verification of identity has been satisfactorily completed, no further evidence is needed to undertake subsequent transactions. However, information should be updated or reviewed as appropriate and records must be maintained.

7.7. INDIVIDUAL CUSTOMERS

GDSL shall obtain following information while opening accounts or establishing other relationships with individual customers:

i. Correct name and/or names used;
ii. Parent's names;
iii. Spouse name
iv. Date of birth;
v. Current, permanent & occupational address;
vi. Details of occupation/employment and sources of wealth or income
vii. Contact information, such as — mobile/telephone no.

The original, certified copy of the following Photo ID (any one) is required to identify the customer:

i. Current valid passport;
ii. Valid driving license;
iii. National ID card;
iv. Voter ID
v. Employer provided ID card, bearing the photograph and signature of the applicant;
vi. Any other identification documents, which is acceptable to GDSL

Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as sole evidence of identity, e.g. birth certificate, certificate from any local government organs, credit cards, non-Bangladeshi driving license. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which GDSL is unfamiliar, either because of origin, format or language, GDSL must take reasonable steps to verify that the

document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. GDSL should also be aware of the authenticity of passports.

7.8. VERIFICATION OF ADDRESS

One or more of the following steps may be followed to verify addresses:

- Provision of a recent utility bill i.e. electricity, telephone, gas, WASA,
- Municipal! City Corporation holding tax receipt
- Record of home/office visit;
- Sending thanks letter.
- TIN certificate
- Employer certificate (Duly verified)
- Bank statement. (Duly verified)

The information obtained should demonstrate that a person of that name exists at the address given, and that the applicant is that person.

7.9. NON FACE-TO-FACE CONTACT

Where business relation is established without face-to-face contact, GDSL will take appropriate measures to address risks arising from establishing business relations and undertaking transactions through instructions conveyed by clients over the internet, the post or the telephone.

GDSL would take one or more of the following measures to mitigate the risk associated with not being able to have face-to-face contact when establishing business relations:

- Telephone contact with the client at a residential or business number that can be verified independently;
- Confirmation of the client's address through an exchange of correspondence or other appropriate method;
- Subject to the client's consent, telephone confirmation of the client's employment status with the client's employer's personnel department at a listed business number of the employer;
- Confirmation of the client's salary/income details by requiring the presentation of recent bank statements from a bank;
- Certification of identification documents by lawyers or notary publics presented by the Client;
- Requiring the client to make an initial deposit using a cheque drawn on the client's personal account with a bank; and
- Any other reliable verification checks adopted by GDSL for non-face-to-face client

7.10. APPROPRIATENESS OF DOCUMENTS

There is obviously a wide range of documents which might be provided as evidence of identity. It is important for the GDSL to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which are easily forged or which can be easily obtained using false identities.

7.11. JOINT ACCOUNTS

In respect of joint accounts where the surname and/or address of the account holders differ, the name and address of all account holders, not only the first named, should normally be verified in accordance with the procedures set out above.

7.12. CHANGE IN ADDRESS OR OTHER DETAILS

Any subsequent change to the customer's name, address, or employment details of which GDSL becomes aware should be recorded as part of the Know Your Customer process. Generally this would be undertaken as part of good business practice and due diligence but also serves for money laundering prevention.

7.13. INTRODUCER

To identify the customer and to verify of his/her identity, an introducer may play important role. An introduction from a respected customer personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of address as set out above. Details of the introduction should be recorded on the customers file. However, personal introductions without full verification should not become the norm, and directors/senior managers must not request staff to breach account opening procedures as a favor to an applicant.

7.14. CORPORATE BODIES AND OTHER ENTITIES

Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering,

particularly when a legitimate trading company is involved. Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a "brass plate company" where the controlling principals cannot be identified.

Before a business relationship is established, measures should be taken by way of 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, and struck off, wound-up or terminated. In addition, if GDSL becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

No further steps to verify identity over and above usual commercial practice will normally be required where the applicant for business is known to be a company, or a subsidiary of a company, quoted on a recognized stock exchange.

The following documents should normally be obtained from companies:

a. Certified copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
b. Certified copy of the Memorandum and Articles of Association, or by-laws of the client.
c. Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts;
d. Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;
e. Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 10% interest or more or with principal control over the company's assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;
f. Satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;
g. Copies of the list/register of directors.
h. Two recent photographs of the Account Operator(s) duly attested by the Company Secretary/MD/CEO
i. Current & complete information of Account Operator(s)

j. Latest TIN certificate & VAT registration (where applicable)

Where the business relationship is being opened in a different name from that of the applicant, GDSL should also satisfy itself that the reason for using the second name makes sense.

The following persons (i.e. individuals or legal entities) must also be identified in line with this part of the notes:

a. All of the directors who will be responsible for the operation of the account / transaction. All the authorized signatories for the account/transaction.
b. Al1 holders of powers of attorney to operate the account/transaction.
c. The beneficial owner(s) of the company
d. The majority shareholders of a private limited company.

A letter issued by a corporate customer is acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. Where GDSL already knows their identities and identification records already accord with the requirements of these notes, there is no need to verify identity again.

When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering activity, even though authorized signatories have not changed.

7.15. COMPANIES REGISTERED ABROAD

Particular care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. Such companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their final destination. In such circumstances, GDSL should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh's. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.

7.16. PARTNERSHIPS AND UNINCORPORATED BUSINESSES

In the case of partnerships and other unincorporated businesses whose partners/directors are not known to GDSL, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable).

An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose.

7.17. Powers OF ATIORNEY/NOMINEE/MANDATE TO OPERATE ACCOUNTS

The authority to deal with assets under a power of attorney/Nominee/Mandate constitutes a business relationship and therefore, where appropriate, it may be advisable to establish the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept.

7.18. IDENTIFICATION OF BENEFICIAL OWNERS AND VERIFICATION OF THEIR IDENTITIES

GDSL should assess and determine the measures which would be appropriate to determine the beneficial owners. GDSL should be able to justify the reasonableness of the measures taken, having regard to the circumstances of each case.

GDSL will assess and determine the measures which would be appropriate to determine the beneficial owners, if any and would be able to justify the reasonableness of the measures taken, having regard to the circumstances of each case.

7.19. RELIABILITY OF INFORMATION AND DOCUMENTATION

GDSL obtains information or documents from the client or a third party, it would take reasonable steps to assure that information or documents are reliable and where appropriate, reasonably up to date at the time they are provided to.

Where the client is unable to produce original documents, GDSL will accept documents that are certified by qualified persons, such as lawyers and accountants or any respectable person acceptable to GDSL.

7.20. RISK CATEGORIZATION — BASED ON ACTIVITY/KYC PROFILE

When opening accounts, the concerned officer must assess the risk that the accounts could be used for "money laundering", and must classify the accounts as either High Risk or Low Risk. The risk assessment may be made using the KYC Profile Form in which following seven risk categories are scored using a scale of 1 to 5 where scale 4-5 denotes High Risk, 3- Medium Risk and 1-2 Low Risk:

- Occupation or nature of customer's business
- Net worth / sales turnover of the customer
- Mode of opening the account
- Expected value of monthly transactions
- Expected number of monthly transactions

KYC Profiles and Transaction Profiles must be updated and re-approved at least animally for "High Risk" accounts (as defined above). There is no requirement for periodic updating of profiles for "Low Risk" transactional accounts. These should, of course, be updated if and when an account is reclassified to "High Risk", or as needed in the event of investigations of suspicious transactions or other concern.

7.21. REVIEW AND UPDATE

GDSL will review all the information related with their clients that they preserved, after a certain period of time. If there any substantial changes in client's business, profession, address, status or and other things, GDSL will update that and preserve duly.

This page intentionally left Blank

8. Transaction Monitoring Process

8.1. MEANING OF "SUSPICIOUS TRANSACTION"

The reporting of suspicious transaction is the excellent tool for mitigating AML/CFT risks. All staffs of GDSL should be vigilant to detect suspicious transaction or activity done by their clients.

STR/SAR means a formatted report of suspicious transactions! activities where there is a reasonable ground to believe that funds are the proceeds of crime or may be linked to money laundering or terrorist financing, insider trading & market manipulation related activity or the transactions do not seem to be usual.

Section 2(z) of Money laundering Prevention Act, 2012 defines Suspicious
Transaction as follows:

- That deviates from usual transactions;
- With regards to any transaction there is ground to suspect that (1) the property is the proceeds of an offence, (2) the financing of terrorist activities, a terrorist group or an individual terrorist
- Any transaction or attempted transaction that are delineated in the instructions issued by Bangladesh bank from time to time for the purpose of the ACT

Section 2(16) of ATA, 2009 (including amendment of 2012) defines Suspicious Transaction as follows:

- Which is different from usual transactions;
- Which invokes presumption that
  - i. it is the proceeds of an offence,
  - ii. it finances to terrorist activities, a terrorist group or an individual terrorist; which is any other transactions or an attempt for transactions delineated in the instructions issued by the Bangladesh Bank from time to time for the purposes of this ACT;

8.2. REPORTING RESPONSIBILITIES

All reporting organizations in Bangladesh are required to submit Suspicious Transaction Reports (STR) or Suspicious Activity Reports (SAR) to Bangladesh Bank.

GDSL is legally obligated to submit STR/SAR as a reporting organization under the MLPA 2012 and the Anti Terrorism Act 2009 (as amended in 2012).

8.3. REASONS FOR REPORTING OF STR/SAR

STR/SAR submission is necessary on the part of GDSL for the following reasons:

- It is a legal requirement in Bangladesh;
- It helps protect GDSL from reputation damage, penalty and/or facing criminal proceedings;
- It helps to protect GDSL from unfounded allegations of assisting criminals, including terrorists;
- It assists the authorities to investigate money laundering, terrorist financing, and other financial crimes.

8.4. HOW TO IDENTIFY A SUSPICIOUS TRANSACTION

Identification of STR/SAR may be started identifying unusual transaction and activity. Transactions may be unusual in terms of the complexity, nature, volume, and time of the transaction(s) etc.
Generally the detection of unusual transactions/activities may be sourced as follows:

- Comparing the KYC profile, if any inconsistency is found and there is no valid reasonable explanation.
- By monitoring customer transactions.
- By using red flag indicator.

Simply, if any transaction/activity is consistent with the provided information by the customer can be treated as normal and expected. When such transaction/activity is not normal and expected, it may treat as unusual transaction/activity.

8.5. TRANSACTION MONITORING TOOLS

The purpose of this monitoring of GDSL is to be vigilant for any significant changes or inconsistencies in the pattern of transactions or any fraudulent activities, insider trading & market manipulation activities. Inconsistency is measured against the stated original purpose of the accounts. The following areas could be monitored:

- Transaction type
- Frequency
- Pattern of transaction
- Unusually large amounts
- Geographical origin/destination
- Activity related to account
- Possible trade related to market manipulation

- Possible trade related to insider trading
- Any type of fraudulent activates

8.6. SUSPUICIOUS TRANSACTION/ACTIVITY REPORTING PROCESS

STR/SAR reporting in GDSL shall follow the following 3 stages:

8.6.1. Identification

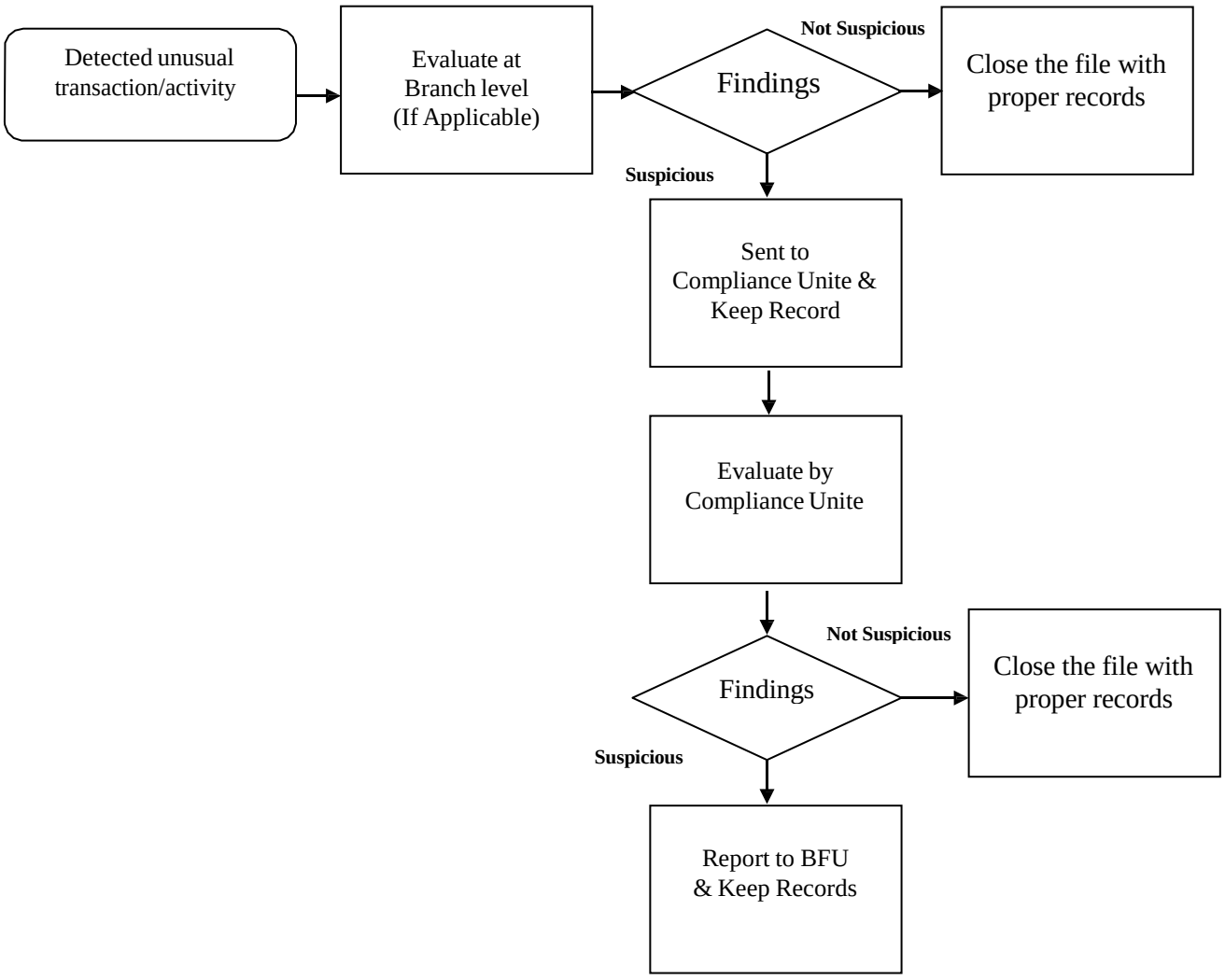
This stage is very vital for STR/SAR reporting. Monitoring mechanisms should be more rigorous in high-risk areas of GDSL's business. The mechanism should be supported by adequate systems to alert management and other appropriate staff (e.g., relationship officer, transaction processing officer, compliance officer) of unusual /suspicious activity. Training of staff in the identification of unusual /suspicious activity should always be an ongoing activity. Considering the nature of business GDSL must be vigilant in KYC and sources of funds of the customer to identify STR/SAR.

8.6.2. Evaluation

After identification of STR/SAR at branch level/Unit Head should evaluate the transaction/activity to identify suspicion y tactfully talking with the customer or through any other means. In this regard, concerned branch level/Unit Head must be tactful considering the tipping-off provision of the acts. If the branch level/Unit Head is not satisfied, he should forward the report to Head of AML/CFT Compliance Unit who will then address it to other AML/CFT Compliance Unit members. After receiving the ST report, AML/CFT Compliance Unit should also evaluate the report whether the STR/SAR report should be sent to BFIU or not. At every stage of evaluation (whether reported to Bangladesh Bank or not) proper records shall be kept by respective compliance officer.

8.6.3. Reporting

This is the final stage and GDSL should submit STR/SAR to BFIU if GDSL is still suspicious of transaction or any activity of a customer. The flow 'chart given below shows STR/SAR identification and reporting procedures:



8.7. "SAFE HARBOR" PROVISIONS FOR REPORTING

Safe harbor provisions protect Merchant Bank and employees from legal action when they report suspicious transactions or activities to the relevant authorities in good faith. In section (28) of MLPA, 2012 provides the safe harbor for reporting.

Divulge of any information or information related to STR/SAR is strictly prohibited under section 6 of MLPA, 2012. No person of CMI will divulge any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of MLPA, 2012.

8.8. SUSPICION INDICATORS

The following are examples of common indicators that may point to a suspicious transaction, whether completed or attempted as explained below;

- Client provides false information or information that seems unreliable.
- Client offers money, gratuities or unusual favors for the provision of services that may appear unusual or suspicious.
- It is observed that a client is the subject of a money laundering, terrorist financing, and insider trading or market manipulation related investigation.
- It is known from a reliable source (that can include media or other open sources), that a client is suspected of being involved in illegal activity.
- A client name listed under UN or Local sanctions list. A new or prospective client is known to you as having a questionable legal reputation or criminal background.
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).
- Client attempts to convince employee not to complete necessary documentation required for the transaction/CDD process.
- Client makes inquiries that would indicate a desire to avoid reporting.
- Client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client is quick to volunteer that funds are “clean” or “not being laundered.”
- Client appears to be collaborating with others to avoid record keeping, Client identification or reporting thresholds.
- Client provides doubtful or vague information.
- Client produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Client refuses to produce personal identification documents.
- Client only submits copies of personal identification documents.
- Client wants to establish identity using something other than his or her personal identification documents.
- Client’s supporting documentation lacks important details such as a phone number.
- Client inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.
- Client presents different identification documents at different times.
- Client alters the transaction after being asked for identity documents.
- Client presents different identification documents each time a transaction is conducted.
- Accounts that have been inactive suddenly, experience large investments that are inconsistent with the normal investment practice of the Client or his/her financial ability.

- Any dealing with a third party when the identity of the beneficiary or counterparty is undisclosed.
- Client attempts to purchase investments with cash.
- Client admits or makes statements about involvement in criminal activities.
- Client does not want correspondence sent to home address.
- Client appears to have accounts with several financial institutions in one area for no apparent reason.
- Client repeatedly uses an address but frequently changes the names involved.
- Client shows uncommon curiosity about internal systems, controls and policies.
- Client presents confusing details about the transaction or knows few details about its purpose.
- Client appears to informally record large volume transactions, using unconventional bookkeeping methods or “off-the-record” books.
- Client over justifies or explains the transaction.
- Client is secretive and reluctant to meet in person.
- Client is nervous, not in keeping with the transaction.
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Client’s home or business telephone number has been disconnected or there is no such number when an attempt is made to contact Client shortly after opening account.
- Normal attempts to verify the background of a new or prospective Client are difficult.
- Client appears to be acting on behalf of a third party, but does not tell you.
- Client insists that a transaction be done quickly.
- Inconsistencies appear in the Client’s presentation of the transaction. The transaction does not appear to make sense or is out of keeping with usual or expected activity for the Client.
- Client appears to have recently established a series of new relationships with different financial entities.
- Client attempts to develop close rapport with staff.
- Client uses aliases and a variety of similar but different addresses.
- Client spells his or her name differently from one transaction to another.
- Client uses a post office box or General Delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
- Client uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the Client or their financial ability.
- Client wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the Client.

- Client frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short time period, inconsistent with the normal practice of the Client.
- Client makes large or unusual settlements of securities in cash.
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Transfers of funds or securities between accounts not known to be related to the Client.
- Several Clients open accounts within a short period of time to trade the same stock.
- Client is an institutional trader that trades large blocks of low priced securities on behalf of an unidentified party.
- Unrelated Clients redirect funds toward the same account.
- Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity.
- Transaction of very large size which may manipulate stock price.
- All principals of Client are located outside of Bangladesh.
- Client attempts to purchase investments with instruments in the name of a third party.
- Payments made by way of third party cheques are payable to, or endorsed over to, the Client.
- Transactions made by employees, or that you know are made by a relative of your employee, to benefit unknown parties.
- Third-party purchases of shares in other names (i.e., nominee accounts).
- Transactions in which Clients make settlements with cheques drawn by or remittances from, third parties.
- Unusually large amounts of securities or stock certificates in the names of individuals other than the Client.
- Client maintains bank accounts and custodian or brokerage accounts at offshore banking centers with no explanation by Client as to the purpose for such relationships.
- Proposed transactions are to be funded by international wire payments, particularly if from countries where there is no effective anti-money laundering system.

9. Record Keeping

9.1. RECORD KEEPING OBLIGATIONS

GDSL will preserve any type of records at least for five years after termination of relationship.

Such records may contain as follows-

- Account opening records;
- Client identity documents;
- Accounts or transactions
- Signature cards, account operating agreements or account applications
- Certain records created in the normal course of business
- Confirmations of purchase or sale;
- Trade authorizations;
- Powers of attorney and joint account agreements; and
- All correspondence, including electronic mail, about the operation of accounts.
- Client statements
- Suspicious transaction report records
- Identification information on all records
- Identification documents
- Keeping Client identification information up to date
- Beneficial Ownership Records
- Politically Exposed Foreign Person Determination and Related Records

9.2. STR AND INVESTIGATION RELATED RECORD KEEPING

It is known that a client or his transaction is under investigation, GDSL would not destroy any records related to that client without the consent of the BFIU or conclusion of the case even though the five-year time limit may have been elapsed. To ensure the preservation of such records GDSL would maintain a register or tabular records of all investigations and inspection made by the investigating authority or all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:

a. The date of submission and reference of the STR/SAR;
b. The date and nature of the enquiry;
c. The authority who made the enquiry, investigation and reference; and
d. Details of the account(s) involved.

10. Training

Employee training and awareness are an integral part of the GDSL compliance program for combating money laundering and terrorism financing. Employees in different business functions need to understand how GDSL's policy, procedures, and controls affect them in their day to day activities.

10.1. POLICY STATEMENT

All GDSL employees shall undergo education and training on combating money laundering and terrorism financing within two years of joining and at least once every two years thereafter.

10.2. GENERAL TRAINING

A general training program should include the following:

- General information on the risks of money laundering and terrorist financing schemes, methodologies, and typologies;
- Legal framework, how AML/CFT related laws apply to Portfolio Manager and their employees;
- Institution's policies and systems with regard to customer identification and verification, due diligence, monitoring;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees;

10.3. JOB SPECINC TRAINING

10.3.1. New Employees

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting any suspicious transactions should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so.

10.3.2. Customer Service/Relationship Managers

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and terrorist financiers and their efforts are vital to the organization's strategy in the fight against money laundering and terrorist financing. They must be made aware of their legal responsibilities and should

be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

It is vital that 'front-line' staffs are made aware of the organization's policy for dealing with non-regular (walk-in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

10.3.3. Processing (Back Office) Staff

The staffs, who receive completed Account Opening, and cheques for deposit into customer's account must receive appropriate training in the processing and verification procedures. The staffs, who are in a position to deal with account opening, or to accept new customers, must receive the training given to relationship managers and other front office staff above. In addition, the need to verify the identity of the customer must be understood, and training should be given in the organization's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the AML/CFT Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

10.3.4. Audit and Compliance Staff

These are the people charged with overseeing, monitoring and testing AML/CFT controls, and they should be trained about changes in regulation, money laundering and terrorist financing methods and enforcement, and their impact on the institution.

10.4. REFRESHER TRAINING

In addition to the above compliance requirements, training may have to be tailored to the needs of specialized areas of the company's business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities. Training should incorporate trends and developments in an institution's business risk profile, as well as changes in the legislation. Training on new money laundering and terrorist financing schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions activity.

10.5. SCREENING MECHANISM FOR RECRUITMENT

One of the major purposes of combating money laundering and terrorist financing activities is to protect GDSL' s from risks arising out of money laundering and terrorist financing. To meet this objective, GDSL shall have to undertake proper screening mechanism in the different appointment procedures so that GDSL does not face money laundering risk by any of the officer as instructed by AML.

Annexure

ANNEXURE- 1

SUSPICIOUS TRANSACTION REPORT (STR)

(INDIVIDUAL/JOINT CLIENT)

A. Reporting Institution

1. Name of the institution:	
2. Name of the Branch:	

B. Details of Report :

1. Date of sending report	
2. Is this the addition of an earlier report?	Yes : ☐ No : ☐
3. If yes, mention the date of previous report	

C. Suspect Account Details:

1. BO Account Number	
2. Folio number/ Client Code	
3. Name of the Account:	
4. Nature of the account: (Margin/Non Margin Portfolio/Others, pls. Specify)	
5. Nature of ownership: (Individual/Joint/Proprietorship! Partnership/company, pls. specify)	
6. Date of opening	
7. Address	

D. Account holder details (In case of Individual)

1. 1. Name of the account holder:	
2. Address:	
3. Profession (In details):	
4. Nationality:	
5. Other account(s) number (if any):	
6. Other Business:	
7. Father's name:	
8. Mother's name:	
9. Date of birth:	
10. Operators! Mandate holder Information	
11. Contact: Mobile No! Email	
12. Bank Account Details	
13. TIN	

2.	1. Name of the account holder: (In case of Individual)	
	2. Relation with the account holder mention in sl. No. Dl	
	3. Address:	
	4. Profession	
	5. Nationality	
	6. Other account(s) number (if any)	
	7. Other business	
	8. Father's Name	
	9. Mother's name	
	10. Date of birth	
	11. Contact: Mobile no/Email	
	12. Bank account details	
	13 TIN	

E. Introducer Details

1. Name of introducer	
2. BO and Client Code number	
3. Relation with account holder	
4. Address	
5. Date of opening	
6. Whether introducer is active! Inactive client	

F. Reasons for considering the transaction(s) as unusual suspicious?

a. ☐ **Identify of clients**
b. ☐ **Activity in account**
c. ☐ **Background of client**
d. ☐ **Multiple accounts**
e. ☐ **Nature of transaction**
f. ☐ **Value of transaction**
g. ☐ **Other mention (Pls. Specify)**

(Mention summary of suspicion and consequence of events)
Use separate sheet if needed)

G. Name of the associates and volume of transaction

(Mention summary of suspicion and consequence of events) **(Use separate sheet if needed)**

H. Documents to be enclosed

1. Account opening from along with submitted documents
2. KYC Profile
3. Transaction Statement
4. Other supporting document (if any)

Signature:

(Authorized officer of AML/CFT Unit)

Name:

Designation:

Phone:

Date:

SUSPICIOUS TRANSACTION REPORT (STR)

(Corporate Client)

A. Reporting Institution:

1. Name of the institution:	
2. Name of the Branch:	

B. Details of Report:

1. Date of sending report	
2. Is this the addition of an earlier report?	Yes : ☐ No : ☐
3. If yes, mention the date of previous report	

C. Suspect Account Details:

1. BO Account Number:	
2. Folio number! Client Code:	
3. Name of the Account:	
4. Nature of the account: (Margin/Non Margin/Portfolio/Others, pls. Specify)	
5. Nature of ownership: (Individual/Joint/Proprietorship! partnership/company, pls. specify)	
6. Registration No.:	
7. Registration No. & Authority:	
8. Address in details	
9. Contact Details	
10. List of related Directors/Partners (at least 2, with contact details):	
11. Operators! Mandate holder Information:	
12. Bank Account Details	
13. TIN	
14. BIN	

D. Reasons for considering the transaction(s) as unusual suspicious?

- **a.** ☐ **Identify of clients**
- **b.** ☐ **Activity in account**
- **c.** ☐ **Background of client**
- **d.** ☐ **Multiple accounts**
- **e.** ☐ **Nature of transaction**
- **f.** ☐ **Value of transaction**
- **g.** ☐ **Other mention (Pls. Specify)**

(Mention summary of suspicion and consequence of events)
Use separate sheet if needed)

E. Name of the associates and volume of transaction

(Mention summary of suspicion and consequence of events) **(Use separate sheet if needed)**

F. Documents to be enclosed

1. Account opening from along with submitted documents
2. KYC Profile
3. Transaction Statement
4. Other supporting document (if any)

Signature:

(Authorized officer of AML/CFT Unit)
Name:
Designation:
Phone:

ANNEXURE -2

Internal Suspicious Transaction I Activity Report Form

Strictly Private & confidential.

To	Anti Money Laundering Compliance Officer	Date :
From	Head of the branch/ Unit	Branch / Department
	Job Title	STR/ SAR Ref No.

Client/ Business Name	Account Number(s)
Transaction Date (s)	Copies of Transactions and Account Details Attached

Description of Transaction(s), (Name of transaction, Origin & destination of Transaction etc)
Reasons for suspicion (Give as details as possible) Signature branch/Unit head
ACTION TAKEN TO VALIDATE • Acknowledgement sent to the originator on_____. • Reviewed account documentation • Discuss wit the relationship manager/branch manager • Other **AGREED SUSPICIOUS** Yes / No Comments Signature Date.

ANNEXURE-3

Internal Assessment / Control Checklist

- Has GDSL Established separate "AML/CFT Compliance Unit (AML/CFT Compliance Unit)" and appoint sufficiently senior head of AMT/CFT Compliance Unit?
- Has the senior management of GDSL sufficiently committed to place AML/CFT measures over the institutions?
- Has the board of Directors approved AML/CFT policies & procedures and follow up the implementation status of AML/CFT policies and procedures?
- Have branch/unit carried out a review of processes in its day to day business to identify where money laundering is most likely to occur? (If applicable)
- Is this review regularly updated?
- Has branch/unit established procedures and controls to prevent or detect money laundering? (if applicable)
- Is the effectiveness of such controls tested?
- Is all staff aware of AML/CFT policies and procedures?
- Is all staff aware of their responsibilities with regard to money laundering?
- Do they receive regular money laundering training?
- Are all members of staff sufficiently capable of identifying suspicious transactions?
- Are your systems capable of highlighting suspicious transactions (he. those not conforming to usual parameters)?
- Do all members of staff know the identity of their Head of AML/CFT Compliance Unit?
- Do you thoroughly check and verify the identity of all your Clients?
- Do you have Client accounts in the name of fictitious persons/entities?
- Do you know the identity of the beneficial owner of all your corporate clients?
- Is this identity verified?
- Are all suspicious transactions reported to BFIU?