clmarkets

Anti-Money Laundering and Counter-Terrorism Financing Program "AML/CTF Program"

CLMarkets Ltd. · Suite 305, Griffith Corporate Centre, Beachmont, Kingston, St. Vincent and the Grenadines · support@clmforex.com

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING PROGRAM "AML/CTF PROGRAM"

INTRODUCTION

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (the "AML/CTF Act") became effective on 12 December 2006. However, some parts of the AML/CTF Act commenced in a phased approach up to December 2008.

CLMarkets Limited trading as Core Liquidity Markets ("CLM") is a Reporting Entity on the basis that it provides a Designated Service (as defined in section 6 of the AML/CTF Act).

Pursuant to the AML/CTF Act a Reporting Entity must have and comply with an AML/CTF Program. The AML/CTF Program is divided into Part A (general) and Part B (customer identification).

This AML/CTF Program has been prepared so that CLM can assess the potential money laundering and terrorist financing ("ML/TF") risks to which it may be exposed and to manage those risks within the legislative framework.

This AML/CTF Program was adopted by CLM on July 25th 2013. The AML/CTF program was last updated on September 11th 2018.

PART A

The primary purpose of Part A of this AML/CTF Program is to identify, mitigate and manage the risk that CLM may reasonably face (inadvertently or otherwise) by facilitating money laundering or terrorism financing through the provision of its designated services.

In this AML/CTF Program, "we", "us" or "our" means CLM.

BUSINESS OVERVIEW

CLM is a company structured primarily to provide general advice, dealing and market making services in derivatives and foreign exchange contracts to both retail and wholesale clients.

CLM' primary mode of operandi is by way of an electronic trading platform which operates over the Internet i.e. CLM gives clients direct online access to the rates/prices in the derivatives and foreign exchange markets at which CLM is prepared to deal.

THE PURPOSE OF AML/CTF RISK ASSESSMENT

The purpose of our AML Risk Assessment is to identify, mitigate and manage our potential ML/TF risk. This Part A of the AML/CTF Program formally documents that in identifying our ML/TF risks, CLM has considered the risk posed by the following factors:

(a) our customer types, including beneficial owners of customers and any Politically Exposed Persons (PEPs) (domestic, international organisation and foreign);

(b) the source of funds and wealth of our customers;

(c) the nature and purpose of the business relationship with our customers;

(d) control structures of non-individual customers, and the beneficial owners of our customers;

(e) the types of designated services we provide;

(f) the methods by which we deliver our designated services;

(g) the foreign jurisdictions with which we deal.

The identification of the ML/TF risks potentially faced by CLM enables us to design and implement the controls and measures required to mitigate and manage these risks.

CLM has conducted a full risk assessment of the business which has formed the basis of this program. The purpose of this risk assessment is to identify what ML/TF risks exist for CLM when providing designated services. The two risk types: business risks and regulatory risks have both been considered.

The risks identified have then been assessed/measured in terms of a combination of:

- Likelihood that these will occur

- Impact of the consequence of loss or severity of damage that may result if these do occur

Scales of likelihood and impact within a risk matrix have been combined to generate a matrix of risk scores. Risk appetite, tolerance and treatment has also been defined.

CLM is committed to ensuring that its procedures and policies prevent its services (and products) from being used to facilitate money laundering or terrorist financing.

WHY IS CLM AT RISK?

Some of the risk themes currently faced by CLM have been set out below (this list is not exhaustive).

- Live chat facility;
- CLM's customer base is growing and from all over the globe;
- Interactions are non-face to face; preferred by criminals;
- Various electronic forms of payment credit cards used to trade
- E-payments is a known method to dispose of illegally obtained funds,

i.e. spending or receiving illegitimate money via trading accounts.

HOW WE IDENTIFY, MITIGATE AND MANAGE ML/TF RISK

- Risk Factors

For the purposes of the AML/CTF Act and Rules, in identifying its ML/TF risks, CLM has considered the risks posed by the seven factors listed in paragraph 2 above and set out in detail below. Thus, certain customer types, source of funds and wealth, business relationships and control structures, designated services, delivery methods, foreign jurisdiction considerations are all factors that can result in a higher ML/TF risk.
At a high-level, risk factors that we may reasonably face are identified as follows:

(i) Customer Types, (including beneficial owners of customers);

- Any politically exposed persons PEP's (domestic, international organisation and foreign);

- Customers who are identified as being persons or entities which support terrorist activity or are named in government lists or with credible sources in respect of corruption and/or criminal activity;

- Nature, volume and frequency of trading having regard to the financial standing of the customer;

- Customers (not necessarily PEPs) based in, or conducting business in or through, a high risk geographic location, or a geographic location with known higher levels of corruption or organized crime, or drug production/distribution;

- Opportunities are presented for criminals to engage in transnational activities have expanded with globalisation and advancements in information and communications technologies. Cyber-criminal activities increasingly affect the financial security of online business. It is widely accepted that the financial and insurance industry is the 'target of choice' for financially motivated cyber criminals;

- Professional service providers such as lawyers, accountants, investment brokers or other professionals holding accounts for their customers or acting on behalf of their customer and where we would be required to place an unreasonable reliance on the professional service provider;

- Requests for undue levels of secrecy with a transaction;

- Whether the customer is a long-standing customer or undertakes occasional transactions; and

- the customer's business activities place the customer in a high-risk category;

- Customers who wish to use pre-paid credit cards and the associated risks with the digital payments arena.

CUSTOMERS' SOURCE OF FUNDS AND

WEALTH

- Sources of wealth - the origin of the entire body of wealth gives an indication of the volume of wealth of the customer. Whether it is at the expected level;

- Source of funds – the origin of funds or assets which are the subject matter of the business relationship between the customer and CLM.

- Where the origin of wealth or source of funds cannot be easily verified.

(ii) The nature and purpose of the business relationship with its customers,

- Risks arising from changes in the nature of the business relationship, control structure or beneficial owner of CLM's customers;

- Intended type and level of transactions to be carried out and risks associated with those transactions. Larger transactions present higher AML/TF risk.

(iii) The control structure of non-individual customers

- CLM can only be satisfied that it knows who the beneficial owner is if they know who ultimately owns or controls the customer – either directly, or indirectly through interests in the customer's beneficial owner(s);

- Where there is a failure to identify who ultimately controls the business relationship preventing developing a clear understanding of the AML/TF risk associated with the business relationship;

- Where the structure of the customer/entity renders it difficult to identify the true controlling owner, or where there is no legitimate commercial rationale for the structure.

(i) The Types of Designated Services We Provide

The list of Designated Services (located in Section 6 of the AML/CTF Act) has been reviewed and the ones that CLM provide have been identified and ranked as low.

Forex

Designated Service	Description	Risk Ranking
Item 33	Provision of a designated service in the capacity of agent of a person, acquiring or disposing of: (a) a security; or (b) a derivative; or (c) a foreign exchange contract; on behalf of the person, where: (d) the acquisition or disposal is in the course of carrying on a business of acquiring or disposing of securities, derivatives or foreign exchange contracts in the capacity of agent; and (e) the service is not specified in the AML/CTF Rules	Low
Item 35	Provision of a designated service in issuing or selling a security or derivative to a person, where: (a) the issue or sale is in the course of carrying on a business of issuing or selling securities or derivatives; and (b) in the case of an issue of a security or derivative–the issue does not consist of the issue by a company of a security of the company or of an option to acquire a	Low

Designated Service	Description	Risk Ranking
	security of the company; and (c) in the case of an issue of a security or derivative—the issue does not consist of the issue by a government body of a security of the government body or of an option to acquire a security of the government body; and (d) in the case of an issue of a security or derivative—the issue is not an exempt financial market operator issue; and (e) such other conditions (if any) as are set out in the AML/CTF Rules are satisfied	

Forex/ Bullion

Item 54	Provision of a designated service in the capacity of holder financial services license, making arrangements for a person to receive a designated service (other than a service covered by this item).	Low

Bullion

Item 1	Selling bullion, where the selling is in the due course of carrying on a business*	Low

(i) Foreign Jurisdictions

- Countries identified by credible sources as providing funding or support for terrorist activities or who have terrorist groups working within the country;

- Countries subject to sanctions, embargoes or similar measures;

(i) Methods by which we Deliver Designated Services

- Online
- Telephone
- Live chat facility

- Countries identified by credible sources as having significant levels of corruption and/or criminal activity;

- Countries identified by credible sources as lacking appropriate AML/CTF legislation/ systems/ measures or controls;

- Countries identified by the FATF as non-co-operative countries and territories;

- Countries identified by credible sources as being tax havens;

- Countries that are materially associated with production and/or transnational-shipment of illicit drugs.

By way of an example a Risk Matrix which was formulated from the Financial Action Task Force on Money Laundering ("FATF") Guidance Note, entitled "Guidance on the risk based approach to combating money laundering and terrorist financing," sets out general risk assessment criteria.

A RISK BASED AML/CTF PROGRAM

This AML/CTF Program is risk based.

The following diagram, formulated from the FATF "Guidance on the risk based approach to combating money laundering and terrorist financing", sets out the suggested risk assessment and management controls process that should be implemented.

Risk Assessment Link to the AML/CTF Risk Management

Identify, verify and then assess the customer

The following steps are performed in identifying, verifying and performing a risk assessment of the customer:

STEP 1. Initial (or minimum) KYC information is obtained to identify and verify the customer as required by the AML/CTF Rules

CLM will initially seek to identify and then verify the customer is who they claim to be. As a result, initial questions / information must be obtained to identify (and verify) the person. This is referred to as "Know Your Client information" or "KYC information".

Beneficial owners and control structures are determined and KYC information is collected and verified. CLM review the parties to the trust deed; identify major shareholders; understand the customer's management structure; and understand the rights and responsibilities of senior managers to determine control structures.

CLM has strict KYC procedures to verify the applicant's identity. Manual verification is under taken when a customer does not pass electronic verification (EV). World Check (for international clients)

STEP 2. Identify whether a customer is a PEP

CLM determines whether any customer or beneficial owner is a PEP (domestic, international organisation or foreign). Where a customer is determined to be a PEP, CLM collect and verify KYC information. CLM then determine whether the PEP poses a high ML/TF risk. Additional due diligence measures and risk management systems are implemented where the PEP is high ML/TF risk or a foreign PEP. Foreign PEP's are always classified as high risk.

If a customer is a foreign PEP or a domestic or international organisation PEP who is assessed as being a high ML/TF risk, CLM take additional measures such as taking reasonable measures to establish the source of wealth and funds; and require senior management approval before providing the PEP with designated services or establishing or continuing the business relationship with them.

STEP 3. Additional KYC information is obtained to identify and verify the customer where the identity is unclear or non-verifiable

If the minimum KYC information is considered insufficient and CLM is unable to identify and verify the customer, then further (additional) questions must be asked of the customer so that the identity of the customer can be verified with confidence.

STEP 4. A risk assessment is performed with respect to that customer

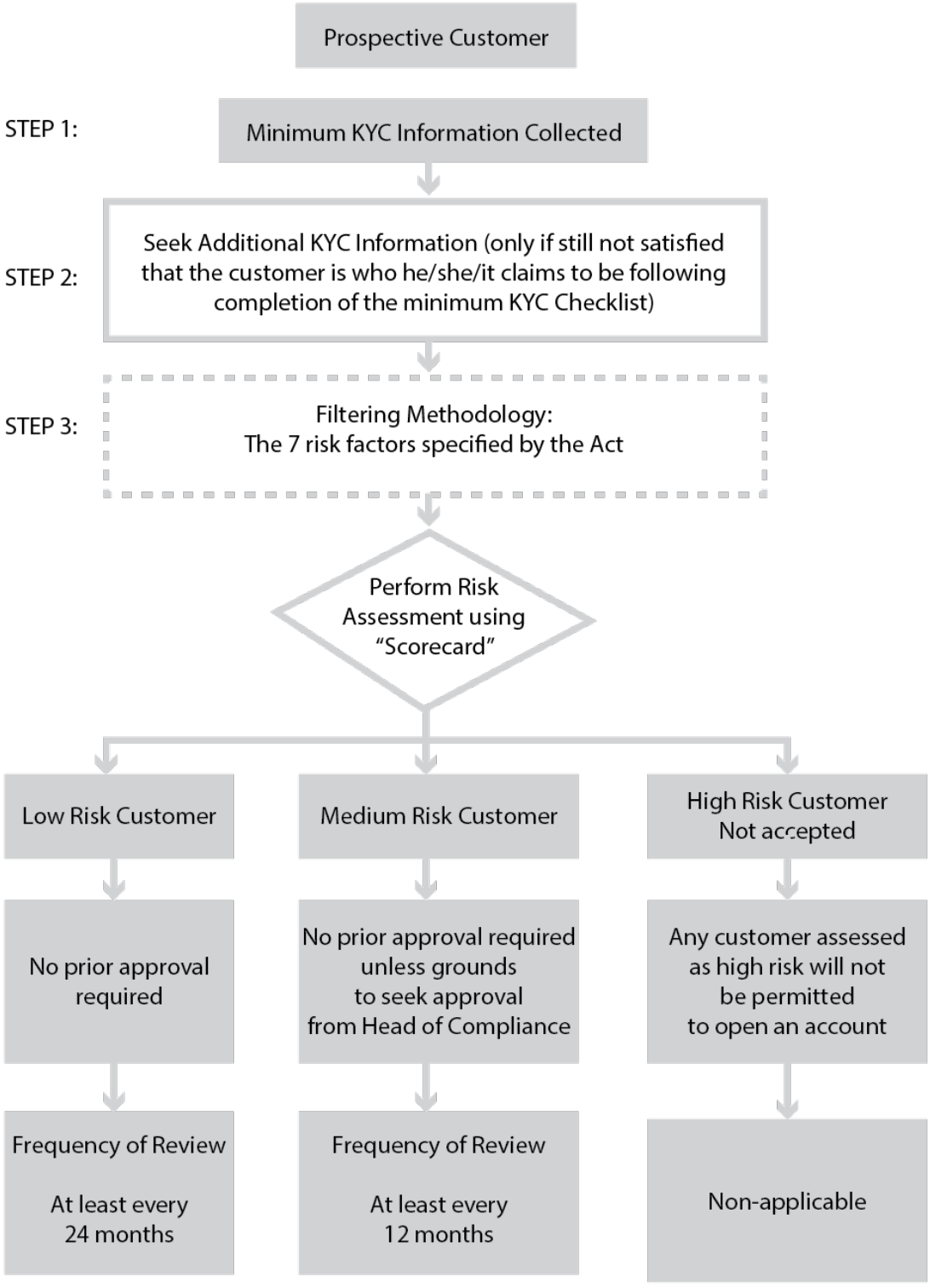
CLM is then required to carry out a risk assessment as to its exposure to facilitating money laundering and/or terrorism financing by its customer in order to identify, mitigate and manage the risk identified. To mitigate risk, CLM has taken the decision that Customers deemed to be high risk at the outset are not offered an account.

The assessment of ML/TF exposure must be risk based. The Act requires an assessment based upon the following risk factors:

(1) the types of customers we have (including beneficial owners and PEPs);
(2) the types of designated services we provide;
(3) the methods by which we deliver our designated services; and
(4) the foreign jurisdictions with which we deal;
(5) Source of funds and wealth of customers
(6) The nature and purpose of the business relationships with its customers
(7) Control structures of non-individual customers and the beneficial owners of customers.

Following this assessment, ML/TF risk of that customer is then measured or classified as low, medium or high.

The process by which CLM will assess risk and formulate and implement management control processes is set out diagrammatically below:



This Part A of the AML/CTF Program is designed to identify, mitigate and manage the possible ML/TF risks posed to CLM and to document the controls and systems to address those risks. Any weakness in this Part A of the AML/CTF Program may impact adversely on the management of the ML/TF risks.

BOARD AND SENIOR MANAGEMENT OVERSIGHT

CLM's Part A program must be approved by its governing board and senior management. Part A must also be subject to the ongoing oversight of the reporting entity's board and senior management. CLM's board and senior management are dedicated to overseeing the AML/CTF program to ensure compliance with the Act.

This AML/CTF Program has been adopted by the Board. Any amendment to this AML/CTF Program is subject to Board oversight and approval i.e. the Board must formally adopt any amendment to the AML/CTF Program.

The AML/CTF Compliance Officer/ Head of Compliance will provide a quarterly report to the Compliance Committee and the Board, which will include AML/CTF Program status reports and incident reports. Quarterly compliance meetings have AML as an agenda item.

This AML/CTF Program has been designed to ensure and demonstrate compliance with the AML/CTF obligations as follows:

TO FORMALLY DOCUMENT POLICIES AND PROCEDURES

Money laundering and terrorist financing schemes can be difficult to identify and criminals can be ingenious in formulating different schemes to facilitate their money laundering or terrorist financing agendas.

Accordingly, for this AML/CTF Program to be effective, it requires regular review, and if necessary amendment, in order that it accomplishes its purpose of identifying, mitigating and managing ML/TF risk.

Further, the AML/CTF Compliance Officer/ Head of Compliance must be notified prior to CLM:

(i) introducing a new designated service to the market;
(ii) introducing new methods of delivery of a designated service; and/or
(iii) introducing any new or developing technology used for the provision of designated services.

This will enable the AML/CTF Compliance Officer/ Head of Compliance to identify any significant changes in ML/TF risks and to formulate controls to mitigate and manage those risks.

Where procedures are updated, staff are formally trained to ensure they are aware of the procedures relevant to their specialized role at CLM.

TO ESTABLISH CUSTOMER IDENTIFICATION PROCEDURES (COMMONLY KNOWN AS "KNOW YOUR CUSTOMER" OR "KYC" PROCEDURES)

The KYC procedures must be risk based having regard to the ML/TF risks relevant to the provision of the service/s offered. The procedures are designed to mitigate and manage the potential ML/TF risks and ensure that CLM is reasonably satisfied as to the true identity of its customers (clients).

The customer identification and verification procedures are detailed in Part B of this AML/CTF Program.

TO IMPLEMENT EMPLOYEE DUE DILIGENCE PROCEDURES / CHECKS

There is a requirement within the AML/CTF Act to perform due diligence on certain representatives of CLM i.e. staff, employees, contractors, those seconded to the company for an interim period etc. The level of due diligence required depends upon the function performed and level of seniority / work performed.

The employee due diligence program includes appropriate risk-based systems and controls for CLM to determine whether to, and in what manner to, screen any prospective employee and also re-screen an employee (where that employee is

transferred or promoted) that may be in a position to facilitate the commission of a money laundering or financing of terrorism offence in connection with the provision of a designated service by CLM.

The employee due diligence program also establishes and maintains a system for CLM to manage any employee who fails, without reasonable excuse, to comply with any system, control or procedure established in accordance with Part A or Part B of this AML/CTF Program (refer policy document entitled, "Disciplinary Action Procedures").

CLM has prepared a Recruitment Policy which covers the vetting of candidates for employment, taking and checking of references and the procedures to be followed in the recruitment process.

The Recruitment Policy requires senior management to conduct a formal interview of the candidate. CLM may also perform skills assessment, reference checks or any combination of these prior to offering a candidate a position. Representatives will be selected on the basis of their experience, skills, qualifications and industry knowledge.

The status of all new members of staff must be identified on their commencement of employment (authority to represent the company and provide a designated service) and the identification must be verified and recorded i.e. CLM will ensure that the identity and past history of a prospective employee (representative) has been verified prior to employment or authority granted to represent the company.

THE EMPLOYEE DUE DILIGENCE PROCEDURES

Once employed (or appointed to represent the company), employees (representatives) that are identified as "high risk" will be subject to closer and more frequent monitoring. This includes monitoring of the representative's customer accounts and relationships (i.e. monitoring will be undertaken more frequently than that prescribed by the regular intervals pursuant to internal audit procedures). In addition, these representatives may be subject to transactional limits until such time that comprehensive training in policies and procedures has been completed.

Examples of representatives to be considered as "high risk" include the following:

(i) Representatives who are in a position of dealing with customers or circumstances which are identified as high risk.
(ii) Representatives in "key" positions.
(iii) Representatives that provide unusual or extraordinary activities.
(iv) Representatives who fail to conform to the company's or Group's compliance systems and/or controls.
(v) Staff promoted to more senior levels with greater AML/CTF responsibilities that are yet to complete further AML/CTF training in policies and procedures.
(vi) Representatives with lavish lifestyles, which cannot be supported by the representative's salary or other practical reason.

The level of staff turnover will also be considered and monitored on a regular basis.

Employees are not allowed to open a trading account with CLM. This is to minimize the risks associated with ML/TF. Customer accounts are subjected to the AML/CTF procedures under the supervision of the AML/CTF Compliance Officer/ Head of Compliance.

The performance of supervisors with respect to compliance with the AML/CTF obligations will be monitored as part of their annual performance review. Should any customer account be managed by the AML/CTF Compliance Officer/ Head of Compliance then these will be reviewed by senior management.

Representatives who fail to comply with the compliance systems and/or controls will be subject to disciplinary procedures, which may include termination of employment (cancellation to represent the company). Representatives that are suspected of facilitating money laundering or terrorism financing will be reported to the appropriate authorities.

AML/CTF RISK AWARENESS TRAINING PROGRAM

Appropriate training with regard to money

laundering and terrorist financing is vital in managing the ML/TF risk. Accordingly, all representatives are required to undergo training in AML/CTF laws and internal policies. In order that our ML/TF controls are successful, training programs are formulated having regard to the representative's level of responsibility and position.
Updated or refresher training will depend upon staff promotions and/or depending upon the level of assessed ML/TF risk of the designated service. Training will be carried out under the supervision of the AML/CTF Compliance Officer/ Head of Compliance and senior management. Ongoing general refresher training for all staff will occur on a periodic basis (at least annually) and monthly AML updates will be provided to all staff.

At a minimum the AML/CTF training program will be designed to enable representatives to understand the following:

(i) the company (or Group's) AML/CTF Policy;
(ii) the company (or Group's) AML/CTF Program;
(iii) the obligations of CLM under the AML/CTF Act and Rules;
(iv) the types of ML/TF risk CLM might face and the potential consequences of such risks;
(v) how to identify signs of ML/TF that arise during the course of carrying out their duties;
(vi) escalation procedures i.e. what to do once a ML/TF risk is identified;
(vii) what employees' roles are in the firm's compliance efforts and how to perform them i.e. the processes and procedures relevant to each person's role;
(viii) the company's (or Group's) record keeping and record retention policy; and
(ix) the consequences (including civil and criminal penalties) for non- compliance with the AML/CTF Act and supporting Rules (Civil penalties of a maximum of $3.4 million for an individual and $17 million for a company apply for non-compliance under the Act);
(x) Monthly closed jurisdiction updates;
(xi) AML Regulatory updates to update and inform staff, to ensure ongoing understanding of obligations.

Training may be developed and provided either in house or by contracted training organizations, external AML Consultants. Delivery of the training may include written updates, educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos.

Records of training are maintained to demonstrate that the person/s attended the training session/s, the dates of training, a brief description of the subject matter of the training provided and the number of hours (or level of accreditation) for attending the course/session/seminar.

Certain key employees exposed to a greater ML/TF risk or those identified as "high risk" will undergo specialized additional training.

AML/CTF COMPLIANCE OFFICER/ HEAD OF COMPLIANCE DUTIES

The AML/CTF Compliance Officer/ Head of Compliance reports to the compliance committee and the Board.
The AML/CTF Compliance Officer's/ Head of Compliance duties specifically in relation to ensuring compliance with the AML/CTF Act and Rules include the following:

(i) monitoring compliance and adherence to the obligations of the AML/CTF Act and Rules;
(ii) receiving an investigating reports of suspicious matters activities;
(iii) adopting a risk based approach to monitor customer activity to identify suspicious activity;
(iv) overseeing communication and training for employees;
(v) ensuring that proper AML/CTF records are maintained;
(vi) reporting suspicious activity to senior management, the Compliance Committee and the Board;
(vii) submitting regular reports to the Compliance Committee (at least quarterly);
(viii) submitting regular reports to the Board (at least annually);
(ix) providing advice to senior management, the Compliance Committee and the Board;
(x) lodging annual compliance report;
(xi) receiving and carrying out directions or orders issued by authorities; and
(xii) Liaison with regulatory bodies and law enforcement in respect of suspicious activity reporting.

The AML/CTF Compliance Officer/ Head of Compliance is authorized to act independently in

order to fulfil the commitments of his role.

The AML/CTF Compliance Officer/ Head of Compliance, under the direction of the Board, will ensure that any government or FATF findings concerning the approach to money laundering and/or terrorism financing prevention, in particular countries or jurisdictions, is assessed and appropriate changes made to the AML/CTF Program. Amendments will be communicated to those representatives affected by the changes.

ONGOING CUSTOMER DUE DILIGENCE

Ongoing customer due diligence is an important component in mitigating and managing the ML/TF risks (potential and identified). CLM maintains an ongoing relationship with its customers through updating KYC information, implementation of a transaction monitoring program (TMP) and by conducting enhanced customer due diligence.
CLM has systems in place to determine when further KYC or beneficial owner information should be collected or verified to review and update information. All customer records are reviewed and updated where the ML/TF risk warrants this. This applies to both new and pre-existing customers.

(a) All new accounts are screened for errors by the new accounts team with supervision and guidance from the AML/CTF Compliance Officer/ Head of Compliance.

(b) Sales and support staff maintaining an ongoing relationship/ contact with clients. This contact is both for commercial purposes, to provide ongoing technical support and also for the purposes of updating and maintaining KYC information by verifying name, date of birth and address. All notes are recorded in Salesforce in the company's account information. Customers are requested to provide evidence in the form of proof of address documentation (such as a utility or bank statement) to action a change of address on the system;

(c) Each member of the CLM sales team maintains a list of their own customers. This list is monitored on a daily basis. Contact is therefore maintained with all customers. Those customers not actively trading are contacted to incentivize a return to trading. Those actively trading will be contacted to ensure everything is running smoothly and that they are happy with the platform performance. Ongoing monitoring is undertaken during this process and KYC information verified to ensure it is up to date. Further, if any suspicion is aroused, further KYC is collected and the SMR procedure is followed;

(d) Initial courtesy calls are made to clients at the beginning of the relationship when a demo account is downloaded. At this stage the sales team ascertain the trading experience of the applicant and will canvass trading strategies and intended length of the relationship and spend. This enables CLM to monitor and identify any unusual trading activity, patterns of spend with reference to the disclosed strategies and relationship length.

(e) Sales staff accept withdrawal requests and will flag to the accounts team if there any discrepancies or attempted third party withdrawal requests;

(f) New accounts staff re-verify customers if any errors are identified on an account, or any suspicion is formed;

(g) The accounts and trading teams review transactions, including trading and electronic fund transfers, in the context of other account activity to determine if a transaction is suspicious. A formal TMP is in place;

(h) the AML/CTF Compliance Officer/Head of Compliance is responsible for monitoring adherence to the AML/CTF Act, will document when and how it is carried out, and will report suspicious activities to the appropriate authorities;

(i) exception reports are utilized to identify possible ML/TF risks and include monitoring transaction size, location, type, number and nature of the activity;

(j) the AML/CTF Compliance Officer/ Head of Compliance conducts an appropriate investigation before reporting a suspicious matter.

Instances where CLM re-verify for the purposes of updating and maintain KYC information on all customers

CLM ensures that the information it retains about its customers is up to date. The trading team monitor customer account activity, including trading and electronic fund transfers on an ongoing basis. Staff are trained to identify "triggers" for the requirement to update KYC information. For example, disconnected telephone numbers, returned mail.

Staff are trained to identify and verify beneficial ownership information for all non-individual customer types on an ongoing basis. Where beneficial owner or true controllers are determined, additional KYC information is collected and verified.

RISK BASED TRANSACTION MONITORING PROGRAM (TMP) TO MONITOR TRANSACTIONS

CLM has a risk based transaction monitoring program (TMP) to monitor transactions of customers, including regard to complex, unusual large transactions and unusual patterns of transactions which have no apparent economic or visible lawful purpose

Staff in the new accounts team manually monitor accounts to ensure that there isn't fraudulent activity on the accounts, staff review ID, and look for layering of funds using the trading accounts.

Transactions are monitored by staff on an ongoing basis. Customers are monitored on an ongoing basis in order to identify any suspicious activity; Staff are required to review deposit alerts, and trading activity. Suspicious patterns are reported to Manager of team in the first instance. This information is communicated to the AML/CTF Compliance Officer/ Head of Compliance who will apply enhanced customer due diligence

Accounts and sales staff are trained to look for specific activity which is deemed a Red flag trigger, as follows:-

(i) The customer engaging in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements.

i. especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds

(ii) The customer attempts to make frequent or large deposits of currency, insists on or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.

(iii) For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

(iv) The customer has accounts in, a country identified as a non- cooperative country or territory by the Financial Action Task Force.

(v) The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

(vi) The customer's account indicates large or frequent wire transfers, immediately withdrawn without any apparent business purpose.

(vii) The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose

(viii) The customer makes a funds deposit for the purpose of pursuing a long-term trading strategy, followed shortly thereafter by a request to transfer the proceeds out of the account.

CLM ALSO HAS AN ENHANCED DUE DILIGENCE PROGRAM

Although it is CLM's policy not to accept customers identified as high risk at the outset, it has implemented an enhanced due diligence program to include systems and controls to ensure, where appropriate, measures such as clarifying, analyzing, verifying or updating beneficial owner information collected from the customer; or collecting further beneficial owner information (such as the source of the beneficial owner's funds and wealth) are taken.

CLM has implemented systems so that ongoing due diligence is conducted on the business relationship and scrutinizing transactions to ensure that the transactions are consistent with the knowledge of the customer, and their business and risk profile.

Enhanced due diligence will be undertaken for all high risk customers and transactions and where:

(a) there is a requirement to access further information in order to clarify & update KYC info;
(b) obtain further KYC info;
(c) consider and investigate the suspicious transaction;
(d) verify or re-verify information;
(e) undertake more detailed analysis and monitoring regarding transactions; and
(f) lodge a suspicious matter report.

Where it is determined that enhanced due diligence should be applied, the process will be as follows;

1. AML/CTF Compliance Officer/ Head of compliance will conduct a thorough investigation to determine the source of the customer's and each beneficial owner's wealth;
2. Check the validity of the account registration details;
3. Review any linked accounts;
4. Re-verify KYC information;
5. Analyze the customer's past transactions and possibly monitor future transactions if deemed necessary;
6. The purpose or nature of specific transactions
7. Check IP address where possible to detect any suspicious connection sources
8. Determine if a suspicious matter report should be lodged in accordance with process set out below

Monitoring will be conducted either:

- **MANUALLY**

The AML/CTF Compliance Officer/ Head of Compliance and senior management will ensure that a sufficient sample of activity will be selected to enable the identification of matters of concern, such as patterns of unusual size, volume, type of transactions, foreign jurisdiction factors, or any of the "triggers" identified.

It is proposed that representatives will review transactions (including trading and electronic fund transfers) in the context of other customer activity to determine if a transaction lacks financial rationale or is suspicious because it is an unusual transaction or strategy for that customer, or

- **ELECTRONICALLY**

CLM may also seek to utilise automated (exception) reporting that will include a comprehensive sample of activity and monitor things such as transaction size, location, type, number and nature of the activity.

The AML/CTF Compliance Officer/ Head of Compliance, will be responsible for performing these ongoing monitoring activities.

They will document when and how it is carried out and will report suspicious activities to senior management and/or the appropriate authorities (where required). The AML/CTF Compliance Officer/ Head of Compliance will conduct an appropriate investigation before reporting a suspicious matter.

Employee guidelines with examples of suspicious money laundering activity and lists of high-risk customers that may warrant further scrutiny will also be prepared and distributed to those concerned.

In addition to regular reviews, circumstances may arise in which an otherwise low risk customer will be elevated to high risk.

For example, a customer on commencement of the relationship may be classified as low risk. However, after a change in client circumstances or activities, the risk profile of the customer may be elevated to medium or high. An example of this is a client's change of country of residence.

In circumstances where the customer's risk profile is elevated, further measures and controls will be implemented to mitigate and manage against potential ML/TF risks, including the following:

(i) Immediate notification to all appropriate representatives / business units;
(ii) further KYC information and verification procedures performed;
(iii) an increase in the level on monitoring (i.e. in accordance with the new classification or rating of the customer risk, being medium or high and monitoring intervals commensurate with the identified risk);
(iv) Increased monitoring of transactions in

accordance with senior managements requirements in respect of the *customer* or transaction.

SUSPICIOUS MATTER REPORTING (SMRS)

CLM has implemented monitoring and reporting systems in respect of designated services offered across all relevant business units.

Relevant employees are trained to identify and report suspicious matters to the Head of Compliance AML/CTF Compliance Officer/ Head of Compliance.

The AML/CTF Compliance Officer/ Head of Compliance is adequately trained to investigate suspicious matters, prepare, lodge and retain records of suspicious matter reporting.

Staff are trained to be aware of potential indicators that will trigger a suspicion. The aim is to identify those prospective (or existing) customers that are seeking to use the services offered by CLM for money laundering or terrorist financing purposes, thereby triggering reporting obligations to the relevant authorities.

The AML/CTF Compliance Officer/ Head of Compliance is responsible for submitting SMR's, however staff are aware that it is a shared responsibility to be vigilant in respect of any suspicious matters.

An SMR must be submitted by the AML/CTF Compliance Officer/ Head of Compliance within three business days of forming the suspicion. If the suspicion relates to the financing of terrorism, the SMR must be submitted within 24 hours of forming the suspicion.

Staff are trained to avoid "tipping off" in respect of suspicious matters to avoid wrongfully disclosing to others, information about a suspicious matter. Staff are aware that this is an offence.

If staff form a suspicion whilst dealing with a prospective (or existing) customers, this suspicion must be referred to the AML/CTF Compliance officer/ Head of Compliance who will make a decision as to whether a suspicious matter report should be submitted

Suspicion is formed when a representative considers that an existing or prospective customer is attempting to use the services offered by CLM for ML/TF purposes and/or any one of the following conditions is met:

(i) the representative suspects on reasonable grounds that the customer is not the person they claim to be;
(ii) the representative suspects on reasonable grounds that the customers agent is not the person they claim to be;
(iii) the representative suspects on reasonable grounds that the provision, or prospective provision, of the service is preparatory to the commission of an offence of financing of terrorism;
(iv) the representative suspects on reasonable grounds that information collected by CLM concerning the provision, or prospective provision of the service may be relevant to the investigation of, or prosecution of, a person or entity for an offence of financing of terrorism;
(v) the representative suspects on reasonable grounds that the provision, or prospective provision, of the service is preparatory to the commission of an offence of money laundering;
(vi) the representative suspects on reasonable grounds that information collected by CLM concerning the provision, or prospective provision, of the service may be relevant to the investigation of, or prosecution of, a person or entity for an offence of money laundering.
(vii) the representative suspects on reasonable grounds that information collected by CLM concerning the provision or prospective provision of services:
(viii) may be relevant to investigation of, or prosecution of a person or entity for an evasion, or an attempted evasion of taxation law;
(ix) may be relevant to investigation of, or prosecution of a person or entity for an evasion, or an attempted evasion, of a law of a State or Territory that deals with taxation; or
(x) may be relevant to investigation of, or prosecution of a person or entity for, an offence against a law of the Commonwealth or of a State or Territory; or
(xi) may be of assistance in the enforcement of the Proceeds of Crime Act 2002 or regulations under that Act; or
(xii) may be of assistance in the enforcement of a

law of a State or Territory that corresponds to the Proceeds of Crime Act 2002 or regulations under that Act;

THRESHOLD TRANSACTIONS REPORTS

CLM will design and implement robust systems to detect threshold transactions covering all prescribed requirements. Currently, the prescribed threshold amount is $10,000 i.e. cash transactions in excess of this amount must be reported to AUSTRAC. CLM has confirmation stating they are not required to report these transactions as these are reported directly from the bank receiving funds.

AML/CTF COMPLIANCE REPORT

An AML/CTF Compliance Report is an annual report which CLM prepares that helps provide authorities with information on our compliance with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), the regulations and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007(No.1)* (AML/CTF Rules). AML/CTF Compliance Report contributes to monitoring of ongoing industry compliance with the AML/CTF Act, the regulations and the AML/CTF Rules. CLM follows the AML/CTF Act obligations and completes an AML/CTF Compliance Report before 31 March of eachyear.

INDEPENDENT REVIEW OF PART A OF THE AML/CTF PROGRAM

A review of Part A of the AML/CTF Program will be undertaken annually. The review will be undertaken either:

- internally i.e. by a person separate from the AML/CTF Compliance Office (or his/her department or direct control); or
- by an external service provider that will be retained to conduct the review.

The purposes of the review will be to:

- assess the effectiveness of Part A of the AML/CTF Program, having specific regard to the ML/TF risks faced by CLM;
- assess whether Part A of the AML/CTF Program complies with the AML/CTF Rules;
- assess whether Part A of the AML/CTF Program has been effectively implemented; and
- assess whether CLM have complied with Part A of the AML/CTF Program.

The result of the review, including any report prepared, will be provided to the Board, the Compliance Committee and senior management.
A draft checklist entitled "Independent Review of the AML/CTF Program".

Record Keeping:

In accordance with meeting legislative obligations, CLM will retain all records relevant to its AML/CTF Program and policies, including the following:

1. the AML/CTF Program and all reviews and addendums to the same;
2. its AML/CTF Policy and all reviews and addendums to the same;
3. transactional records;
4. Customer identification and verification records;
5. Audits and compliance reviews;
6. Suspicious matter reporting (from 13 December 2008);
7. Threshold reporting (from 13 December 2008);
8. Senior management approvals;
9. Customer account/relationship records;
10. Annual compliance reports and other management reports;
11. Training and compliance monitoring reports; and
12. Information relating to the effectiveness of training.

Records in respect of customer identification and verification are retained for 7 years after account closure.
Where CLM (or its agent or intermediary) carries out a customer identification and verification procedure with respect to a prospective customer to whom CLM proposes to provide a designated service, it must make (and retain) a record of:

(i) the procedure (i.e. the Checklist); and
(ii) information obtained in the course of carrying out the procedure (i.e. supporting documentation to verify the identification of the customer); and
(iii) such other information (if any) about the procedure as is specified in the AML/CTF

Rules (currently no further information is specified).

Records in respect of financial transactions are to be retained for 7 years after the date of the transaction.

AML/CTF Program and addendums together with any documentation relevant to the reason for amendment are also to be retained for 7 years after the adoption of the AML/CTF Program and/ or amendments cease to be in force.

SYSTEMS TO RE-ASSESS RISK

CLM will review all areas of its business to identify potential ML/TF risks that may not be covered in the procedures described above. The additional areas of ML/TF risks are in respect of new products, services, distribution channels and developing technologies.
Additional procedures to address these ML/TF risks are as follows:

1. The AML/CTF Compliance Officer/ Head of Compliance will be consulted by any person having responsibility for a new service or method of delivery or new technology ("the project manager") at design stage or prior to the introduction of the new service, delivery method or technology. He will be required to advise on the ML/TF risk factors which are to be considered having regard to:
2. the target market (customer type);
3. the service features;
4. foreign jurisdictional features / offerings;
5. any electronic access to / the delivery method of the service.
6. The AML/CTF Compliance Officer/ Head of Compliance will, in consultation with the project manager undertake the risk assessment and formulate the controls and systems to manage any ML/TF risks.
7. The AML/CTF Compliance Officer/ Head of Compliance will review the AML/CTF Program, policies and procedures to ensure that any new ML/TF risks are identified in the AML/CTF Program and amendments to the AML/CTF Program are made. All amendments will be overseen by senior management and will require Board approval.
8. The AML/CTF Compliance Officer/ Head of Compliance will formulate staff awareness and training programs in respect of the change to ML/TF risks and will oversee the delivery of training programs.
9. The AML/CTF Compliance Officer/ Head of Compliance will retain all records relevant to the risk assessment, addendums to the AML/CTF Program and the training programs.
10. The AML/CTF Compliance Officer/ Head of Compliance, under the direction of the Board, will ensure that any government or FATF findings concerning the approach to money laundering and terrorism financing prevention in particular countries or jurisdictions, is assessed and appropriate amendments made to the AML/CTF Program. Furthermore, all compliance procedures will be made and communicated to all representatives.

EXTERNAL AUTHORITIES

CLM will co-operate with all external authorities. CLM will comply with any directions or notices received from such bodies and will actively search and retain records of any guidance issued or released in respect of perceived ML/TF risks.

PRIVACY

Customer identification and verification procedures will be carried out having regard to the Privacy Act 1988. CLM's Privacy Policy and Disclosure Document/s (e.g. the Financial Services Guide and Product Disclosure Statements) will be amended to include the following disclosure:

(i) that personal information may be collected because CLM is obliged by Law to collect certain information (for example, the Anti Money Laundering Counter Terrorism Financing Act 2006 requires CLM to collect information and verify the identity of its clients / customers. This is often referred to as "know your customer" information);
(ii) that information may be collected from other persons or organizations and a listing of those sources including agents, brokers, publicly available information and documents; and
(iii) that where required by Law, the client or customer's personal information may be disclosed to other parties.