Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Programme

Table of Contents

Introduction

Anti-money Laundering and Countering Financing of Terrorism Act 2009

The Act was passed by Parliament on 16 October 2009. The Act significantly changed New Zealand's existing AML/CFT regime (which consisted primarily of the Financial Transaction Reporting Act 1996) by aligning it with global standards as set by the Financial Action Task Force (FATF) and other international organisations such as the United Nations, Basel Committee and Wolfsburg Group.

Purpose of the Act:

- Detect and deter money laundering and the financing of terrorism;
- Maintain and enhance New Zealand's international reputation by adopting (where appropriate) the universal recommendations issued by FATF; and
- Contribute to the public confidence in the financial system.

Under the Act reporting entities have a range of responsibilities including:

- Developing and maintaining a risk assessment and a risk-based AML/CFT programme;
- Customer identification and identity verification ("Customer Due Diligence" or "CDD");
- Ongoing customer due diligence, including account transaction monitoring;
- Suspicious transaction reporting;
- Record keeping;
- Staff vetting and training; and
- Meeting audit and annual reporting requirements.

The obligations under the Act have been identified and Sections 3-14 of this programme document outline the processes and controls in place which enables Rockfort Markets to comply.

The most significant change to New Zealand's AML/CFT environment was the shift from a prescriptive reporting regime to that of a pro-active risk based management regime whereby reporting entities are considered best placed to identify our money laundering and terrorist financing risks in respect to our business operations.

What is Money Laundering?

Money laundering involves transforming money from crime ("dirty money") into money that:

- has the appearance of coming from a legitimate source; and
- makes the criminal origin of the money difficult to trace ("clean money").

Effective money laundering enables criminals to remove themselves from their criminal activities, making it harder to prosecute them, and confiscate their illegal proceeds.

There are three stages to laundering money:

1. **Placement**: placing cash proceeds from crime into the financial system. For example, depositing the "dirty money" into a bank or financial institution.
2. **Layering**: splitting the criminal funds into various deposit accounts or complex layers of transactions to disguise their origin and provide anonymity.

3. **Integration**: withdrawing the layered funds and bringing them back together in one account or multiple accounts so that they appear legitimate i.e. “clean money”.

Methods of Money Laundering

There are many ways to launder money, some of which are sophisticated and complicated. The most common examples include:

- Depositing cash at various institutions in amounts less than the amount that must be reported, and subsequently transferring the funds to a central account.
- Establishing shell companies or trusts by unverified beneficiaries.
- Moving funds via wire transfers to disguise their source and ownership.
- Buying foreign currency that can be transferred to offshore banks via international wire transfers.
- Purchasing high value assets with bulk cash i.e. gem stones, gold, luxury cars, boats and real estate in someone else’s name then selling them and depositing the funds.

More detail on the nature of money laundering and terrorism financing is included in the ‘*Best Practice Guidelines for Financial Institutions*’ released by the Financial Intelligence Unit of the New Zealand Police (“FIU”).

A copy of these guidelines is available at http://www.police.govt.nz/service/financial/guidelines.html.

The FIU has also published a National AML/CFT Risk Assessment and publishes quarterly reports highlighting money laundering and financing of terrorism (ML/FT) typologies and recent cases.

What is Terrorist Financing?

Terrorist financing refers to the use of funds (obtained from either legitimate or criminal activity) by designated terrorist entities, organisations or jurisdictions that are considered sympathetic to terrorist activity. Terrorist financing cares little about the source of funds, but it is what the funds are used for that defines its scope. Terrorists may use low value but high volume money from legitimate sources to fund their operations.

Reputation and Financial Risk

Public confidence in financial institutions can be severely undermined by adverse publicity as a result of inadvertent association with criminals involved with money laundering or terrorist financing. In addition, financial institutions may lay themselves open to direct or indirect financial loss either through negligence in screening undesirable or high risk customers or where the integrity of their own staff or agents has been undermined by association with criminals.

The Act also sets out increased civil liability and criminal offences for failure to comply with the Act.

Why Rockfort Markets Limited (Rockfort Markets) is captured under the Act

a. In terms of the AML/CFT Act, reporting entities are defined as being either a financial institution or a casino. Rockfort Markets’ business activities fall within the definition of a financial institution as defined by the Act and Rockfort Markets is therefore required to comply with the obligations under the Act.

AML/CFT Programme

Why an AML/CFT Programme is required

In accordance with sections 56 & 57 of the Act and the AML/CFT Programme Guideline, Rockfort Markets has established and implemented a compliance programme based on the risk assessment which includes adequate and effective internal procedures, policies and controls necessary to:

a) detect money laundering and the financing of terrorism;
b) manage and mitigate the risk of money laundering and financing of terrorism; and
c) designate an employee as an AML/CFT Compliance Officer.

This AML/CFT programme document sets out the internal policies, procedures and controls necessary to detect money laundering and financing of terrorism (ML/FT) and to manage and mitigate the risk of it occurring. Further details of the form of the programme together with key principles for AML/CFT compliance are included in the AML/CFT Policy.

The policies, procedures and controls implemented are robust to reasonably address the risks outlined in the risk assessment. The definitions used within the organisation are as follows:

Policies	Set out expectations, standards and behaviours
Procedures	More detailed than policies and set out day-to-day operations including processes and business rules
Controls	Actions that management set to ensure the business complies with policies and procedures to modify risk

This AML/CFT programme document has been approved by the Managing Director, and sets out Rockfort Markets' strategy to:

- Take a "risk based" approach for mitigating and managing AML/CFT risks taking into account:
  - The nature, size and complexity of the business;
  - The AML/CFT risks that Rockfort Markets may reasonably expect to face under the normal course of business;
- Achieve an optimal balance between compliance, customer impact and cost;
- Produce sound business intelligence on money laundering and terrorist financing activities occurring within Rockfort Markets;
- Encourage vigilance against the criminal use of the organisations business operations and payments systems;
- Implement adequate and effective preventative policies, procedures and controls; and
- Facilitate cooperation with the AML/CFT supervisor and law enforcement agencies.

This programme applies to all staff of Rockfort Markets who undertake customer due diligence. This AML/CFT programme document sets out in the following sections Rockfort Markets' action and response to the obligations within the Act and supporting guidelines and codes.

1. Appointment of AML/CFT Compliance Officer (s56(2)-(4))

Obligation	Rockfort Markets must designate an employee as an AML/CFT Compliance Officer to administer and manage its AML/CFT programme. The AML/CFT Compliance Officer must be appropriately trained and report to a senior manager of the Rockfort Markets. Senior manager is defined as: *"**senior manager** (and **senior management** correspondingly) means, —* *a) in relation to a Rockfort Markets that is a company, a director within the meaning of section 126 of the Companies Act 1993; and* *b) in relation to a Rockfort Markets that is not a company, a person who occupies a position comparable to that of a director (for example, a trustee or partner); and* c) *any other person who occupies a position within a Rockfort Markets that allows that person to exercise an influence over the management or administration of the Rockfort Markets (for example, a chief executive or a chief financial officer)"*
Actions Taken	The responsibility for the appointing the AML/CFT Compliance Officer. The role description is included in Appendix 1, together with other role responsibilities. As at the date of this Programme, Craig Beaumont has been appointed as the AML/CFT Compliance Officer and reports to the Managing Director, who is a senior manager for the purposes of the Act.

2. Staff Vetting (s57(a))

Obligation	There are procedures for vetting all senior managers, the AML/CFT Compliance Officer and all staff covered by AML/CFT obligations at the commencement of employment to ensure that they are appropriately qualified and have the requisite character to fulfil the requirements of the role.
Actions Taken	Rockfort Markets will complete criminal checks on all existing staff through the Ministry of Justice before staff's employment. It is likely that some future staff members will have already had such checks undertaken for example, job agency checks, immigration checks etc. All staff are also subject to screening against the PEP and sanctions watchlist (Verifi Identity Limited)
Control	If the candidate cannot meet our requirement, we will not issue the job offer.

3. Staff Training for staff with AML/CFT responsibilities (s57(b) (i – iii)

Obligation	There is formal AML/CFT training in place for all senior managers, AML/CFT Compliance Officer and all staff covered by AML/CFT obligations. Records are maintained of all

	staff that have undertaken AML/CFT training. There are internal communications to keep staff up to date with money laundering trends and alerts.
Actions Taken	All staff will be trained initially face-to-face by the AML/CFT Compliance Officer with the assistance of the company who finalised this policy. Further face-to-face training will be completed as required by the AML/CFT Compliance Officer. All staff will be required to undertake AML/CFT training as required by the AML/CFT Compliance Officer. This may include: • Staff reading and signing to indicate they understand key AML/CFT policies • Watching introductory videos • Periodic testing as required The AML/CFT Compliance Officer maintains a training register for staff. Completion of training is reported to management by the end of the month. AML/CFT Compliance Officer Training In addition to the training undertaken by all staff, the AML/CFT Compliance Officer will ensure that staff stay aware of developments in AML/CFT including: • Reviewing and incorporating relevant guidance • Relevant media articles and news coverage • Attendance of Supervisor roadshows • Attendance of relevant seminars, conferences and courses
Control	An assessment of the staffs that take the training will be processed by the compliance manager. If the staff cannot meet our requirement, that staff will be required to take a relevant training again until pass the assessment.

4. Customer Due Diligence

Rockfort Markets must conduct customer due diligence on:

- a customer (individual, company, trust, etc.);
- any beneficial owner of a customer; and
- any person acting on behalf of a customer.

The Amended Verification Code of Practice 2013 sets out the primary and secondary forms of customer identification documents and verification required. The supervisors expect us to meet the standard as a minimum or explain why they have chosen alternative verification practices. In addition, the Beneficial Ownership Guidelines published in December 2012 provide further guidance on identifying beneficial ownership and persons acting on behalf of customers.

Standard Customer Due Diligence (ss14-17, 57(c))

Rockfort Markets must conduct customer due diligence in the following circumstances:

- if Rockfort Markets establishes a business relationship with a new customer;
- if a customer seeks to conduct an occasional transaction through Rockfort Markets;
- if, in relation to an existing customer, and according to the level of risk involved,

- there has been a material change in the nature of purpose of the business relationship; and
- Rockfort Markets considers that it has insufficient information about the customer.

Rockfort Markets must also obtain –

- Information on the nature and purpose of the proposed business relationship between the customer and Rockfort Markets; and
- Sufficient information to determine whether the customer should be subject to enhanced customer due diligence.

Obligation	Rockfort Markets must obtain the following identity information: • the person's full name; • the person's date of birth; • if the person is not the customer, the person's relationship to the customer; • the person's address or registered office; • the person's company identifier or registration number; and • any information prescribed by regulations.
Actions Taken	Detail on how Standard CDD is undertaken in included in Appendix A. The application forms and client on-boarding checklist reflect the requirements of this policy.

Enhanced Customer Due Diligence (ss22-30, 57(c),(j))

Obligation	For enhanced due diligence Rockfort Market must, in addition to standard due diligence obtain the following additional information: • information relating to the source of the funds or the wealth of the customer; and • any additional information prescribed by regulations.
Actions Taken	The approach to Enhanced CDD is set out in Appendix A. The application forms and client on-boarding checklist reflect the requirements of this policy.

Politically Exposed Persons (PEPs) (s26)

Obligation	Rockfort Markets must, as soon as practicable after establishing a business relationship or conducting an occasional transaction, take reasonable steps to determine whether the customer or any beneficial owner is a politically exposed person. The Rockfort Markets must have senior manager approval for continuing the business relationship. Rockfort Markets must obtain information about the source and wealth of funds of the customer or beneficial owner and take reasonable steps to verify.
Actions Taken	Rockfort Markets screens all of its customers for PEP and sanctions purposes.

	Rockfort Markets has a policy to not provide services for a PEP. In the event that a potential new customer is a suspected PEP, Rockfort Markets will refuse to open an account for that customer. Where an existing customer is positively identified as a PEP, Rockfort Markets will look to terminate the business relationship with the customer. Further detail is set out in Appendix A

Customer Identification Verification (s16, s20, s24)

Obligation	Verification of customer identity must be done on— • the basis of documents, data, or information issued by a reliable and independent source; or • any other basis applying to a specified situation, customer, product, service, business relationship, or transaction prescribed by regulations and code of practice.
Actions Taken	In Appendix A sets out how Rockfort Markets meets its customer due diligence obligations through operational procedures and controls in accordance with the Identity Verification Code of Practice.

Development of new products, services or technologies which favour anonymity (s30)

Obligation	Rockfort Markets must take any additional measures that may be needed to mitigate and manage the risk of new or developing technologies, or new or developing products, that might favour anonymity from being used in the commission of a money laundering offence or for the financing of terrorism.
Actions Taken	Deposits or withdrawals must be through regulated money transmitters or regulated financial institutions. The level of regulation must be, at a minimum, to the standard required by FATF and AML/CFT Standards of New Zealand. Management who will consult the AML/CFT Compliance Officer as to AML/CFT issues before any new platforms or products is offered by Rockfort Markets. They will ensure new products or platforms meet AML/CFT obligations and update the risk assessment as appropriate.

Countries Risk (s57(h))

Obligation	The countries assessment guideline released by the AML/CFT supervisors sets out the circumstances when it may be required to conduct a country AML/CFT risk assessment: • when you intend to form a designated business group and one of the members is resident overseas;

	• when you establish a business relationship or conduct an occasional transaction for a customer who is not a New Zealand resident; • when you have or propose to have a correspondent banking relationship with an overseas financial institution; • when you intend to rely on an overseas person to conduct customer due diligence on our behalf; • when we determine whether an overseas entity is a shell bank under the Act; and • when developing Rockfort Markets' risk assessment and AML/CFT programme.
Actions Taken	Rockfort Markets' clients will initially be predominantly New Zealand-based. Rockfort Markets is also likely to be referred clients from overseas. These jurisdictions, together with other relevant jurisdictions, have been considered in the written risk assessment. In the event that Rockfort Markets does need to consider other country risks, it would look to publicly available sources including: • Transparency International • Economic Freedom Index • Human Trafficking Index • State Stability Index • INCSR – ML and Narcotics • UN Drug Report • OECD, US Treasury and ATO tax havens • US State Dept. – countries designated terrorist safe havens, sponsors and for general levels of terrorist activity • FATF membership • FATF country warning lists In addition, it is worth noting: • Rockfort Markets does not rely on an overseas person to conduct customer due diligence on its behalf; • Rockfort Markets does not deal with shell banks. Rockfort Markets does not accept clients from mainland China.

Inability to conduct CDD (s37)

Obligation	If, in relation to a customer, Rockfort Markets is unable to conduct customer due diligence in accordance with the Act, the Rockfort Markets: (a) must not establish a business relationship with the customer; and (b) must terminate any existing business relationship with the customer; and (c) must not carry out an occasional transaction with or for the customer; and (d) must consider whether to make a suspicious transaction report.
Actions Taken	The consequences of an inability to conduct CDD are set out in the Appendix A. We will not do business with any customer who does not meet our CDD requirements. If the circumstances are suspicious, we will submit a suspicious transaction report.

False customer names and customer anonymity (s38)

Obligation	Rockfort Market must not provide customers with accounts held anonymously, or numbered accounts (being accounts which do not have a client name associated with them) for which customer identification is not performed. Rockfort Markets must not, without lawful justification or reasonable excuse, set up a facility for a customer under a false customer name.
Actions Taken	Appendix A sets out that anonymous accounts or accounts held in false names cannot be opened or maintained.

5. Ongoing Customer Due Diligence and Account Transaction Monitoring (s31)

Obligation	Rockfort Markets under the Act must conduct ongoing customer due diligence and undertake account monitoring to ensure that the business relationship and transactions are consistent with the Rockfort Markets' knowledge about the customer, the customer's business and risk profile. Accounts are examined and written findings kept in relation to: • Complex or unusually large transactions; and • Unusual patterns of transactions that have no apparent economic or visible lawful purpose; and • Other activity likely by its nature to be related to money laundering or financing of terrorism.

Actions Taken	The Account Monitoring and Suspicious Transaction Reporting Policy sets out how Rockfort Markets conducts ongoing customer due diligence and account monitoring. On-Going Customer due diligence is achieved through a number of channels. Through the Compliance Monitoring Programme, unusual activity is highlighted and investigated i.e. high value transfers inconsistent with initial CDD assessment. The following factors will be taken into account when conducting ongoing due diligence: • The type of customer due diligence conducted when the business relationship with the customer was established • The level of risk assessed when the customer was established • Whether the relationship with the customer has changed • Whether the ownership of the customer has changed • When the last review was completed for the customer. Rockfort Markets undertakes regular account monitoring to ensure that the business relationship and transactions are consistent with its knowledge about the customer, the customer's business and risk profile: • Is the transaction consistent with the knowledge we have about the customer and the customer's business? • Is the customer's account activity and transaction behaviour consistent with what we have been told will occur across the account and with account history? • Are there any grounds for reporting a suspicious transaction to the AML/CFT Compliance Officer? Transactions are monitored through the Compliance Monitoring Programme – which analyses transaction frequency and size by account – and "outliers" are compared versus the initial CDD assessment, and challenged if inconsistent with our expectations concerning the activity anticipated over the account in question. Examples of outliers include, but are not limited to: (a) frequent wires in an out of a client's account where such activity is abnormal for the account; (b) a request to wire money to an FATF sanctioned/blocked country; (c) several money orders received within a short span of time on a recently opened account; (d) multiple accounts under a single name or multiple names, with a large number of inter-account transfers; (e) high level of account activity with low level of securities transactions; (f) large wire transfers immediately followed by withdrawal by check or debit card; (g) customer appears to act as an agent for an undisclosed principal; (h) cash transactions involving a large dollar amount;

	(i) transactions that lack business sense or that are inconsistent with the Customer's investment strategy; (j) customer exhibits unusual concern for secrecy, particularly with respect to his or her identity, type of business, and assets; (k) customer's account indicates large or frequent wire transfers to unrelated third parties; (l) customer or beneficiary has a questionable background, including prior criminal charges or convictions; (m) customer has difficulty explaining the nature of his or her business, or lacks general knowledge of the industry; (n) customer is unconcerned with risks, commissions or other costs associated with trading; (o) as applicable, customer appears to be acting as an agent for another entity or individual but is evasive about the identity of the other entity or individual; (p) a customer is from, or has accounts in a country identified as a haven for bank secrecy, money laundering or narcotics production; and (q) a customer engages in transactions involving more than NZ$5,000 in currency or cash equivalents (in one transaction or a series of transactions in one or more days and in any number of accounts). The AML/CFT Compliance Officer will maintain a register of: • Complex or unusually large transactions; and • Unusual patterns of transactions that have no apparent economic or visible lawful purpose; and Other activity likely by its nature to be related to money laundering or financing of terrorism.

6. Suspicious Activity Reporting (ss40-48, 57(d),(g))

Obligation	A suspicious activity report under section 40 must – ▪ Be in the prescribed form (if any); and ▪ Contain the details prescribed by regulations; and ▪ Contain a statement of the grounds on which Rockfort Markets holds the suspicions referred to in section 40(1)(b); and ▪ Be signed by a person authorised by Rockfort Markets to sign suspicious activityreports (unless the report is forwarded by email or another similar means of communication); and ▪ Be forwarded, in writing, to the Commissioner – ○ By way of secure electronic transmission by a means specified or provided by the Commissioner for this purpose; or ○ By another means (including, without limitation, by way of transmission by fax or email) that may be agreed from time to time between the Commissioner and the reporting entity concerned. However, if the urgency of the situation requires, a suspicious activity report may be made orally to any Police employee authorised for the purpose by the Commissioner,

	but in any such case the reporting entity must, as soon as practicable, but no later than 3 working days, forward to the Commissioner. There are procedures in place to ensure that transactions that have been identified as suspicious are reported to the Police FIU in the prescribed form no later than 3 working days after forming suspicion.
Actions Taken	The Account Monitoring and Suspicious activity Reporting Policy sets out how Rockfort Markets reports suspicious transactions. Staff are trained to be aware of red flags for transactions which include: • Unrealistic wealth compared to client profile • Defensive stance to questioning or reluctance to provide CDD information including proof of income • Buying and selling a security for no discernible purpose or in circumstances that appear unusual. • Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business that the investor operates. • Transfer of investments to apparently unrelated third parties with no explanation proffered. • Any transaction in which the nature, size or frequency appears unusual. • Payment by way of third party cheque or money transfers where there is a variation between the account holder, the signatory and the prospective investor. In the event that a staff member has suspicions about a transaction, they must provide details of the transaction, clearly setting out the grounds for suspicion, and immediately send it to the AML/CFT Compliance Officer for assessment as to whether the transaction is suspicious or unusual for reporting to the FIU. If the AML/CFT Compliance Officer considers it to be suspicious, they will, as soon as practicable, but no later than three working days after forming the suspicion, report the transaction or proposed transaction to the FIU through the GoAML portal (http://www.police.govt.nz/advice/businesses-and-organisations/fiu/goaml).

7. Prescribed Transaction Reporting

A prescribed transaction is a transaction, conducted through our business, that is:

Obligation	Rockfort Markets is obligated to report the following :

	– cash and bearer negotiable instruments that are exchanged for physical (NZ) currency), valued at NZ$10,000 or more
Actions Taken	Rockfort Markets compliance team monitors all transections manually. If compliance officer detects a transfer of cash and/or bearer negotiable instruments valued at NZ$10,000 or more he will report this to the FIU via Goaml.

8. Record Keeping

Customer identity and verification records (ss50, 57(h),(e))

Obligation	Rockfort Markets must keep those records used for the identification and verification to be readily identified at any time. Rockfort Markets must retain the records for at least 5 years after the end of that business relationship.
Actions Taken	Rockfort Markets records of all decisions made and retains customer due diligence records in an auditable manner. Notes on the risk-based decisions made at customer establishment are recorded: *Identity and Verification records* • A copy of the evidence used. • If it is not practicable to retain that evidence, any information as is reasonably necessary to enable that evidence to be obtained. *Rockfort Markets retains records as follows:* For records relating to the identity and verification of the identity of a person in relation to establishing a business relationship, daily information will be save a period of at least 5 years after the end of that business relationship. *Other Records* Rockfort Markets must keep the following records in addition to identity and verification records and transaction records: • Records that are relevant to the establishment of the business relationship • Any other records (for example, account files, business correspondence, and written findings) relating to, and obtained during the course of, a business relationship that are reasonably necessary to establish the nature and purpose of, and activities relating to, the business relationship. The records must be kept for a period of at least 5 years after the end of the business relationship.

Transaction Records (ss49,57(e),(g),(h))

Obligation	Rockfort Markets must keep transaction records that are reasonably necessary to enable that transaction to be reconstructed at any time. Rockfort Markets must retain the records for at least 5 years after completion of the transaction.
Actions Taken	As for Customer identity and verification records above.

Other Records (ss51, 57(e))

Obligation	Rockfort Markets must keep the following other records: • establishment of the business relationship • risk assessments, AML/CFT programmes, and audits; and • any other records relating to the nature and purpose of and activities relating to the business relationship
Actions Taken	Records in respect of establishment of the business relationship and any other records relating to the nature and purpose of and activities relating to the business relationship are as for the customer verification above. Records in respect of risk assessments, AML/CFT programmes, and audits are held by the AML/CFT Compliance Officer.

Destruction of Records (ss54, 57(e))

Obligation	Rockfort Markets must take all practicable steps to ensure that every record retained is destroyed as soon as practical after the expiry period.
Actions Taken	Rockfort Markets takes all practicable steps to ensure that every record retained by it under the Act, and every copy of that record, is destroyed as soon as practicable after the expiry of the period for which Rockfort Markets is required to retain that record except where there is a lawful reason for retaining that record. Further detail on record keeping and destruction will be detailed in document management procedures and processes.

9. Assurance (s59(1))

Obligation	A reporting entity must review its risk assessment and AML/CFT programme to— • ensure the risk assessment and AML/CFT programme remain current; and • identify any deficiencies in the effectiveness of the risk assessment and the AML/CFT programme; and • make any changes to the risk assessment or AML/CFT programme identified
Actions Taken	**Ensuring the Risk Assessment and AML/CFT Programme remain current**

	A description of how Rockfort Markets ensures that its risk assessment is up to date is set out in the written risk assessment. Other than changes to the AML/CFT Programme which flow from changes to the risk assessment, the following circumstances may require an update of the AML/CFT Programme: • Industry guidance or updated obligations with respect to AML/CFT Programmes; • New / emerging money-laundering/financing of terrorism trends which may dictate a change to controls or procedures in the Programme; • Internal feedback / reporting / observations regarding the efficacy of the AML/CFT Programme; and • External opinion / feedback (e.g. from Rockfort Markets' Supervisor or independent auditor). It is the responsibility of the AML/CFT Compliance Officer to ensure that they are up to date with the above. The risk assessment and AML/CFT Programme will be reviewed at every year at the time of the annual report. **Internal Assurance and Reporting** The AML/CFT Compliance Officer prepares a monthly report to management on AML/CFT compliance including. • Number of STR's submitted • Staff training • Issues / findings from Internal Assurance / Regulators / Audit • Any media items of interest **Audit** Where there are any deficiencies identified in an audit of the AML/CFT risk assessment or programme, those deficiencies are escalated to the Board with the AML/CFT Compliance Officer having responsibility for addressing those deficiencies.

10. Independent Audit (s59(2)-(7))

Obligation	Rockfort Markets must ensure its risk assessment and AML/CFT programme are audited every 2 years or at any other time at the request of the relevant AML/CFT supervisor. The audit must be carried out by an independent person appointed by the Rockfort Markets who is appropriately qualified to conduct the audit
Actions Taken	The AML/CFT Compliance Officer will co-ordinate the appointment of an independent auditor in accordance with the Audit Guidelines released by the Supervisors. The Managing Director will approve the appointment. Where there are any deficiencies identified in an audit of the AML/CFT risk assessment or programme, those deficiencies are escalated to the Director(s)

	with the AML/CFT Compliance Officer having responsibility for addressing those deficiencies.

11. Reporting (s60)

Obligation	Rockfort Markets must prepare an annual report to the AML/CFT supervisor on its risk assessment and AML/CFT programme. An annual report must— • be in the prescribed form; and • take into account the results and implications of the audit; and • contain any information prescribed by regulations. Rockfort Markets must provide the annual report to its AML/CFT supervisor at a time required by the AML/CFT supervisor.
Actions Taken	**Annual Report** The completion of the annual report requires information to be obtained from various sources i.e. • AML/CFT risk assessment • AML/CFT programme • Product and Services Register • Data warehouse / systems While the AML/CFT Compliance Office will maintain overall responsibility for ensuring the report is collated, approved and submitted, including the following information: • Each products and service offered: ▪ Average monthly number of transactions over most recent financial year ▪ Average monthly NZD value of transactions over most recent financial year • Number of Customers under following customer types: ▪ Individuals ordinarily resident in New Zealand ▪ Overseas residents (nor ordinarily resident in NZ) ▪ New Zealand entities (including companies, partnerships, trusts, charities and incorporated/unincorporated entities) ▪ Overseas entities (including companies, partnerships, trusts, charities and incorporated/unincorporated entities) ▪ Overseas Government bodies ▪ Politically Exposed Persons • Methods for delivery of services (i.e. Channels). Require both percentage by customer usage for new customers (during recent financial year) and for existing customers (during the most recent financial year): ▪ Face to face (over the counter, other than intermediaries) ▪ Non face to face (includes electronic, telephone, via post and all other types of remote access – other than intermediaries) ▪ Domestic intermediaries / agents/third party referral (excludes employees acting as advisors working outside main offices)

	▪ Overseas intermediaries (excludes employees acting as advisors working outside main offices) • Country risk as categorised in your risk assessment for: ▪ Correspondent banking relationships (cross border only) ▪ Other respondents ▪ Relationships where there is a written agreement for delivery of products and services ▪ Other relationships for delivery of products and services The annual report will be approved by the Board prior to submission to the Supervisor.

Appendix 1 – Roles & Responsibilities

Board	• Approve the AML/CFT programme and policy. • Receive regular AML/CFT compliance reports. • Receive and approve Programme review/changes. • Approve the annual report prior to submission to the supervisor. • Establish and maintain the formal position of AML/CFT Compliance Officer.
Management	Management is responsible for reducing the risk on Rockfort Markets and any subsidiaries, third parties or agents from becoming associated with money laundering and terrorist financing. • Ensure that business is conducted in conformity with high ethical and professional standards and that the laws and regulations pertaining to AML/CFT are adhered to. • Ensure documented AML/CFT programme, policies, procedures and resources have been communicated and are in place across all business units providing financial products and services. • That the AML/CFT programme is to remain current, robust and effective for identifying, monitoring and assessing the risks and key controls of money laundering and terrorist financing. • Promote embedding and adherence with AML/CFT programme, policies, procedures and training awareness so that all staff, wherever located, are informed of and have access to Rockfort Markets's supporting policies and procedures • Undertake an annual review of the risk assessment, AML/CFT programme, policies and procedures.

Staff	• All employees and representatives of Rockfort Markets are responsible for assisting in Rockfort Markets' efforts to uncover and report any activity that constitutes, indicates or raises suspicions of money laundering or terrorist financing.
	• All relevant employees are responsible for the day to day compliance of money laundering and terrorist financing risks including risk assessment of Rockfort Markets' customers, products, services and systems.
	• All relevant employees must follow approved policies, business procedures and controls to verify the identity of new customers and be confident they are who they claim to be. This includes the accurate input of all customer identification data into the system.
	• All relevant employees must report suspicious transactions to the AML/CFT Compliance Officer.
	• When dealing directly or indirectly with customer's employees must not reveal any suspicion or indicate that a suspicious activity report will be lodged other than to:
	  ○ AML/CFT Compliance Officer
	  ○ Managing Director
	• Employees must follow the retention requirements for customer identification and transaction records.

	• Rockfort Markets shall provide continuing education and training of all employees. All employees must complete AML/CFT training at least once every 2 years. • Staff vetting procedures pertinent to money laundering and terrorist financing risks must be in place for directors, senior management, staff and prospective staff in positions to facilitate money laundering. • If any employee believes that they or their business unit or activities cannot meet the requirements of this programme and the associated internal AML/CFT compliance policies and procedures, this must be formally communicated (and as soon as practical) to the AML/CFT Compliance Officer. • All identified breaches of Rockfort Markets's internal AML/CFT policies and procedures by employees will be documented and reported to the AML/CFT Compliance Officer. • Employees will need to be aware that disciplinary action may follow from non-compliance with the AML/CFT programme.
AML/CFT Compliance Officer	• In undertaking his/her duties the AML/CFT Compliance Officer has full and unfettered access to all Rockfort Markets staff, systems and documents pertaining to the investigation of money laundering or terrorist financing incidents. • Principle duties of the AML/CFT Compliance Officer are to: i) Produce sound customer and financial intelligence that leads and monitors effective detection and reporting of suspicious transactions; and ii) develop and maintain Rockfort Markets' AML/CFT policies, compliance programme and associated procedures. • Responsibilities include: ▪ Determine whether the information or other matters contained in the suspicious activity reports received or generated give rise to knowledge or suspicion that a customer is engaged in money laundering or terrorist financing. ▪ Ensure that all Suspicious activity Reports (STRs) which are submitted to law enforcement agencies by Rockfort Markets are formally signed-off by the AML/CFT Compliance Officer and reported to the NZ Police Financial Intelligence Unit within 3 working days. ▪ Ensure compliance with all applicable money laundering and terrorist financing laws and regulations. The AML/CFT Compliance Officer will identify, assess, monitor and report on the anti-money laundering compliance risks for Rockfort Markets. ▪ Liaison with Police and relevant authorities, on current money laundering investigations, STRs and Rockfort Markets' AML/CFT practices. ▪ Liaison with Rockfort Markets' AML/CFT supervisor, the Department of Internal Affairs. ▪ Assists or directs Rockfort Markets entities or units with AML/CFT compliance-related issues. ▪ Initiates money laundering awareness and drives ongoing training within Rockfort Markets based on the function or

	position staff hold (i.e. front line staff / back office support staff). ▪ Develop a risk assessment model to ensure structured risk assessments are performed under the auspices of the AML/CFT programme. Data based risk analysis is undertaken to i) identify the specific products, services, customers, entities, channels and geographic locations that may be more vulnerable or have been historically targeted by criminals; and ii) to develop or refine appropriate and effective AML/CFT policies and procedures. ▪ Ensure employee due diligence is undertaken for all new and relevant staff. ▪ Provide periodic reporting on AML/CFT risks, incidents and trends to the Board.
Human Resources (as carried out by the AML/CFT Compliance Officer and/or Managing Director)	Rockfort Markets will continue to maintain screening procedures when hiring all new employees to ensure high standards: • Ensure employee vetting (credit and criminal checks) is undertaken as part of the internal and external recruitment process, including contractors and details recorded. • Undertake any additional vetting of existing employees as required. • Record retention and retrieval obligations will also apply to staff identification documentation and / or information held on the payroll system.

Appendix 2 – Non-applicable obligations

Designated Business Group (s32)

Obligation	A reporting entity that is a member of a designated business group may rely on another member of the group to conduct customer due diligence procedures and share certain elements of the AML/CFT programme under the Act subject to certain conditions, including AML/CFT supervisor approval. The AML/CFT supervisors have published Designated Business Group ("**DBG**") - Formation and Scope Guidelines. A member of a DBG can rely on another member to carry out some obligations on their behalf. These include: • customer due diligence; • parts of an AML/CFT programme - such as record keeping, account monitoring and ongoing CDD; • annual reporting; • risk assessments; and • suspicious activity reporting. Importantly, all members of a DBG must agree in writing to comply with certain privacy principles in the Privacy Act 1993. These are Principles 5-11 in section 6 of the Privacy Act and cover storage, access and accuracy of personal information held and limits on its use and disclosure.

Simplified Customer Due Diligence (ss18-21, 57(c)-(j))

Obligation	The Act lists customers that reduced CDD measures can be taken in respect of (e.g. publicly listed companies and government departments). Other types of customers can be included on this list through regulation.

Third Parties or Agents (s32-34)

Obligation	A reporting entity may authorise a person to be its agent and rely on that agent to conduct customer due diligence procedures and obtain information required for customer due diligence under the Act (section 34) and regulations. A reporting entity may rely on another person (who is not an agent) to conduct the customer due diligence procedures under the Act and regulations subject to certain conditions.

Correspondent Banking (s29)

Obligation	A financial institution (the correspondent) that has, or proposes to have correspondent banking relationship with a respondent financial institution (the respondent) must according to the level of risk conduct enhanced customer due diligence in accordance with the conditions under the Act.

Shell banks (s39)

Obligation	A reporting entity must not establish or continue business relationship or allow an occasional transaction through a shell bank. A shell bank is an entity that is formed and authorised to carry on banking business in a country but does not have a physical presence in that country.

Wire Transfers – Identification (s27) and verification (s28)

Obligation	A reporting entity that is an ordering institution must identify and verify (according to the level of risk) the originator of a wire transfer that is over the applicable threshold value as per the conditions of the Act for international and domestic wire transfers. A reporting entity that is an ordering institution must identify the originator of a wire transfer that is over the applicable threshold value by obtaining the following information: • the originator's full name; and • the originator's account number or other identifying information that may be prescribed and allows the transaction to be traced back to the originator; and • one of the following: (i) the originator's address: (ii) the originator's national identity number: (iii) the originator's customer identification number: (iv) the originator's place and date of birth; and • any information prescribed by regulations. However, if the wire transfer is a domestic wire transfer, a reporting entity that is an ordering institution may identify the originator by obtaining the originator's account number or other identifying information that may be prescribed and allows the transaction to be traced back to the originator. The ordering institution must, according to the level of risk involved, — • verify the originator's identity so that the reporting entity is satisfied that the information provided under section 27 is current and correct; and • verify any other information prescribed by regulations. Verification of the originator's identity must be carried out before the wire transfer is ordered.

Transportation of cash in or out of NZ (ss106 - 107)

Obligation	A person must not move cash in or out of New Zealand if the total amount is more than the applicable threshold value unless the reporting conditions to Customs under the conditions of the Act are met.

Appendix A

Material change in the nature or purpose of the business relationship

As part of Rockfort Markets' customer due diligence obligations under the Act[1], Rockfort Markets must obtain information on the nature and purpose of the proposed business relationship between the customer and Rockfort Markets.

Rockfort Markets has determined that '**nature**' refers to the customer, products, etc. and '**purpose**' relates to the uses that the customer intends to put the products to.

Questions to help determine the nature and purpose of the relationship will be included in our client application forms and our on-boarding checklists.

To determine whether a **Material Change** has taken place, we should consider:

- Staff interactions and knowing the customer
- Unusual patterns of transaction behaviour
- When customer applies for new products and/or services
- A change to the customer's details e.g. change of address, bank account,
- A change in customer domiciled country as not all overseas laws are relevant to Rockfort Markets business etc.

A Material Change includes, without limitation:

- Where there is a dramatic increase in the volume or value of transactions in a customer account.
- Where a dormant account is reactivated
- Changes in name, address, phone number or residential address.
- Where there has been a material change, we must ensure that we have identified and verified the existing customer to the standard set out in this policy. Where the identity documents collected previously are not reasonably capable of establishing the identity of that person, new copies of verification documents in accordance with this policy are required.

The ultimate determination of when an existing customer must be identified and verified will rest with the AML/CFT Compliance Officer.

Identification and Verification

Rockfort Markets will not do business with anyone who does not meet our required level of client identification and verification requirements.

Where the customer is not able to meet the prescribed client identification requirements, the Compliance Officer should give consideration of whether alternative forms of identification may be acceptable in the particular circumstances.

Standard Due Diligence (SDD)

The minimum identification and verification documents which must be obtained for a customer are set out in Appendix B. These minimum standards are amended only by the AML/CFT Compliance Officer.

Where our staff are unable to determine the legitimacy of any presented document, staff should contact the AML/CFT Compliance Officer for clarification.

For each document, we must either:

- have a staff sight the original and retain a verified copy; or
- be provided a certified copy of the document by a trusted referee; or
- be provided a verified copy by an agent of Rockfort Markets (see Procedures for Introduced Business below); or
- have the document electronically verified.

As some of our clients are overseas, copies of international identification provided by a customer resident overseas must be verified.

The trusted referee must not be:

- related to the customer; for example, a trusted referee cannot be their parent, child, brother, sister, aunt, uncle or cousin
- the spouse or partner of the customer
- a person who lives at the same address as the customer
- a person involved in the transaction or business requiring the certification.

Certification by a trusted referee or verification by an agent must:

- include a statement to the effect that the documents provided are a true copy and represent the identity of the named individual;
- include the name, occupation and signature of the employee or trusted referee and the date of certification/verification (Note: If completed by a trusted referee, the trusted referee must specify their capacity to act as a trusted referee from the selection above); and
- have been carried out in the three months preceding the presentation of the copied documents in the case of an agent or trusted referee.

Enhanced Due Diligence (EDD)

Where Rockfort Markets considers that a customer presents a higher level of risk to money laundering or terrorist financing activities the following information is required to be obtained in addition standard customer due diligence information:

- Information relating to the source of the funds or the wealth of the customer.

The following customer types are considered to be higher risk:

- Trusts or another vehicle for holding personal assets
- Foreign politically exposed person (PEPs) from central watch list
- Non-resident customer from a country that has insufficient anti-money laundering and countering financing of terrorism systems or measures in place
- If the customer comes from a country known to deal in drugs, is very corrupt or has links with terrorism or embargoed countries
- Company with nominee shareholders or shares in bearer form.

If staff are unsure if enhanced customer due diligence applies, contact our AML/CFT Compliance Officer.

Politically Exposed Persons (PEP)

A politically exposed person is an individual who holds, or has held at any time in the preceding 12 months, in any overseas country the prominent public function and any immediate family member of the individual (i.e. spouse, partner, child etc.).As soon as practicable after establishing a business relationship or conducting an occasional transaction, you must take reasonable steps to determine whether the customer or any beneficial owner is a politically exposed person. Determining whether a customer is a politically exposed person will be undertaken through the PEP screening process provided by Verify Identity Limited. http://www.verifidentity.com/ If it is determined that a customer or beneficial owner is a politically exposed person with whom a business relationship is going to be established, if it is a new customer, Rockfort Markets will not approve the client application, for an existing customer, Rockfort Markets will terminate the client's agreement.

Examples of prominent public functions include head of a country, government minister, senior politician, senior Judge, governor of a central bank, ambassador, high commissioner, high-ranking member of the armed forces, or senior position in a State enterprise.

Electronic Identity Verification

Electronic Identity Verification (EIV) for name and date of birth is acceptable via an approved Rockfort Markets service provider.

- verify the customer's name from either:
  - a single independent electronic source that is able to verify an individual's identity to a high level of confidence; or
  - at least two independent and reliable matching electronic sources.
- the customer's date of birth is verified from at least one reliable and independent electronic source.
- the customer's details are checked against customer records to ensure that no other person or entity has presented the same identity information or documents.
- a risk assessment of the proposed process and reliability of data sources has been completed; and
- documentation of any additional methods that will be used to supplement electronic identity verification or otherwise mitigate any deficiencies in the verification process.

The AML/CFT Compliance Officer will confirm whether or not the sources proposed by the business are acceptable. We have engaged Verifi Identity Limited and GBG to provide EIV services to Rockfort Markets after having met these criteria.

Acting on Behalf

Identification must be collected and verified for each person Acting on Behalf of a customer.

If a person Acting on Behalf is unable to provide the information required that person will not be able to undertake any transactions in respect of that customer.

This will include any introducing brokers who have a power of attorney to operate a client's account.

Beneficial Owners including Effective Controllers

As a part of customer due diligence you are required to identify, and according to the level of risk take reasonable steps to verify the identity of the "beneficial owner". A beneficial owner is someone who either:

- Owns a prescribed share of more than 25% of the customer
- Exercises effective control over the customer
- Transacts on behalf of customers (requirement to identify and verify the other person).

We must identify and verify the beneficial owner as we would enquire from an individual person by obtaining the reliable and independent documents (refer Appendix B):

- Full name
- Date of birth
- Residential address.

Exceptions

Where the customer is not able to meet the prescribed client identification requirements, staffs should contact the AML/CFT Compliance Officer for consideration of whether alternative forms of identification may be acceptable in the circumstances.

The AML/CFT Compliance Officer will make the final decision on the granting of any exceptions. Any requests will be documented in the Identification Verification Exception Register maintained by the AML/CFT Manager together with the reason for any decision.

Procedures for Introduced Business / Agents

For introduced business, identification requirements for introducing brokers are the same as for direct customers. Customers introduced by introducing brokers are still to be identified as for any other customer – Rockfort Markets does not rely on the introducing brokers or agents to undertake any aspect of CDD.

The ultimate responsibility for knowing Rockfort Markets' customers always lies with Rockfort Markets.

Ongoing Customer Due Diligence

Under our business relationship with a customer, it is a requirement to conduct ongoing customer due diligence in order to determine that customer behaviour is in line with the customer profile. The customer

profile is established when customer due diligence is conducted at the outset of the business relationship with the customer. The level of customer risk is assessed in line with the customer profile.

The following factors should be taken into account when conducting ongoing due diligence:

- the type of customer due diligence conducted, and the information held when the business relationship with the customer was established;
- the level of risk assessed when the customer was established.
- has the relationship with the customer changed?
- has the ownership of the customer changed?
- has the level of customer risk changed?
- when was the last review completed on the customer?

Record Keeping

Customer Identity and Verification

We must keep records of all decisions made and retain customer due diligence records in an auditable manner. It is important we record quality notes on the risk based decisions made at customer establishment:

Identity and Verification records

- A copy of the evidence used.
- If it is not practicable to retain the copy of the evidence, we will retain any information reasonably necessary relates to the particular evidence.

Rockfort Markets must retain the records as follows:

- For records relating to the identity and verification of the identity of a person in relation to establishing a business relationship, a period of at least **five** years after the end of that business relationship

Other Records

Rockfort Markets must keep the following records in addition to identity and verification records and transaction records:

- Records that are relevant to the establishment of the business relationship
- Any other records (for example, account files, business correspondence, etc) relating to, and obtained during the course of, a business relationship that are reasonably necessary to establish the nature and purpose of, and activities relating to, the business relationship.

The records must be kept for a period of at least five years after the end of the business relationship.

Record Destruction

Rockfort Markets must take all practicable steps to ensure that every record retained by it under the Act, and every copy of that record, is destroyed practicable after the expiry of the period for which Rockfort Markets is required to retain that record except where there is a lawful reason for retaining that record.

Further detail on record keeping and destruction will be detailed in management procedures and processes document.

Appendix B: Identification & Verification Requirements by Customer Type

Individual Customers / Natural Persons

Name and Date of Birth

In order to conduct documentary verification of a customer's name and date of birth, the following is required:

EITHER:

One form of the following primary photographic identification:

- New Zealand passport
- New Zealand certificate of identity
- New Zealand refugee travel document
- New Zealand firearms licence
- Overseas passport or a similar document issued for the purpose of international travel which:
  - contains the name, date of birth, a photograph and the signature of the person in whose name the document is issued; and
  - is issued by a foreign government, the United Nations or an agency of the United Nations
- a national identity card issued for the purpose of identification that:
  - contains the name, date of birth and a photograph of the person in whose name the document is issued, and their signature or other biometric measure included where relevant; and
  - is issued by a foreign government, the United Nations or an agency of the United Nations.

OR

One form of the following primary non-photographic identification:

- New Zealand full birth certificate
- Certificate of New Zealand citizenship
- A citizenship certificate issued by a foreign government
- A birth certificate issued by a foreign government, the United Nations or an agency of the United Nations,
- in combination with a secondary or supporting form of photographic identification:
- New Zealand driver licence
- 18+ Card
- Valid and current international driving permit

Residential address:

In order to conduct documentary verification of a customer's residential address, the following is required:

- NZ Driver's Licence (if address is included on licence)
- Citizenship card or passport (if address is included on document)
- A recent bank statement that includes the customer's residential address and is less than 6 months old
- A recent utility bill that includes the customer's residential address and is less than 6 months old

Enhanced Due Diligence - Source of Funds/Wealth Verification

The Act requires that Rockfort Markets takes reasonable steps, according to the level of risk involved, to verify the information in respect of source of funds/wealth for customers requiring Enhanced Customer Due Diligence. The AML/CFT Compliance Officer should be consulted around the application of this requirement.

Source of funds / wealth

- Payslips
- Bank statements
- IRD statements
- Audited financial statements
- Documents confirming the source such as a sale of a house, sale of shares, a bequest under an estate or a win from gambling activities.

Printed documents must be dated within 6 months of opening the Facility.

Legal Entities

Private Companies

Customer's Identity	Verification Documents
Full name of the company	Document: Certificate of Incorporation. Requirement: A copy of the Certificate of Incorporation must be maintained. The details in the certificate must be verified by a Companies Office search carried out by the business.
Full address of the company's registered office and principal place of business	For NZ companies, a Companies Office online search carried out by the business (www.business.govt.nz/companies). Prove of address must be provided. For other countries, an extract from the relevant register.
Registration number of the company	Document: Certificate of Incorporation Requirement: A copy of the Certificate of Incorporation must be maintained. The details in the certificate must be verified by a Companies Office search carried out by the business.
Names of the directors of the company	A Companies Office online search carried out by the business.
Natural persons to verify	• Who owns a prescribed threshold of more than 25% of the customer • Who has authority to act on the account (i.e. signing authority) • Who exercises effective control over the customer • Transacts on behalf of others (requirement to identify and verify the other person) Verification is as per 'Natural persons'.