Capital Clan Limited

Anti-Money Laundering

And

Counter-Terrorist Financing Policy

Version 1.0

CONTENTS

APPROVAL AND CONTROL

IMPLEMENTATION OF POLICY

This Policy shall be deemed effective as of 26/11/2024. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This document shall be subject to periodic reviews in accordance with changes in:

- Local and international legislation.
- Industry best practice.
- Internal changes in the business that impact the products available and relevant revenue streams.

The Board review and approve all changes before they are implemented. Minor changes are reflected by incrementing the version number as 1.1, 1.2, 1.3, etc.

Where significant changes to the document are made, these are reflected in a new version number as 1.0, 2.0, 3.0, etc.

This document was created by Carl Campbell, 26/11/24

1. INTRODUCTION

Operating under the name Capital Clan registered *Capital Clan Limited* of 71-73 Shelton Street, Covent Garden, London W1CH 9JQ and Capital Clan PTE. LTD *of 2 Venture Drive, #14 02 Vision Exchange, Singapore 608526.*

Money laundering and terrorist financing have been identified as a threat to the international financial services community. Global regulators have passed legislation designed to prevent money laundering and to combat terrorism. This legislation, together with regulations, rules, and industry guidance, forms the cornerstone of Anti-Money Laundering (AML)/ Counter-Terrorist Financing (CTF) obligations for firms and outline the offences and penalties for failing to comply.

Therefore, this Capital Clan AML and CTF Policy is designed to ensure that Capital Clan complies with the requirements and obligations set out in global legislation, regulations, rules, and Industry Guidance for the financial services sector, including the need to have adequate systems and controls in place to mitigate the risk of the firm being used to facilitate financial crime.

This AML Policy sets out the minimum standards which must be complied with by all Capital Clan employees, this policy covers the following:

- Establishing and maintaining risk-based customer due diligence, identification, verification KYC/B and EDD procedures, for those customers presenting higher risk, such as Politically Exposed Persons (PEPs).
- Establishing and maintaining risk-based systems and procedures to monitor ongoing customer activity.
- Procedures for reporting suspicious or unusual activity internally, to issuer and to the relevant law enforcement authorities as appropriate.
- The maintenance of appropriate records for the minimum prescribed periods.
- Training and awareness for all relevant employees.
- The provision of appropriate management information and reporting to senior management of Capital Clan to ensure compliance with the requirements.

1.1 Legislation And Jurisdiction

The requirements of UK and Malaysian legislation apply to Capital Clan globally. Principal requirements, obligations and penalties, are contained in the following Legal and Regulatory Framework:

- The Anti-Money Laundering and Countering Financing of Terrorism Act 2009
- The Criminal Proceeds (Recovery) Act 2009.
- Terrorism Suppression Act 2002 Counter-Terrorism Act 2008, Schedule 7.
- Financial Intelligence Unit (FIU).
- Guidance issued by the Joint Money Laundering Steering Group (JMLSG) on Prevention of Money Laundering/combating terrorist/financing.
- FIU Financial Crime Guide.
- The Financial Action Task Force (FATF) Mutual Evaluation.

Capital Clan, joint ventures, and all employees of Capital Clan shall strictly adhere to the policies and procedures outlined in this document.

1.2 The Board

Capital Clan Board is made up of individuals within Capital Clan who are empowered to make decisions regarding Capital Clan's business operations.

Capital Clan board is responsible for:

- The appointment of an MLRO who is responsible for the implementation, monitoring, and review of Capital Clan's AML and CTF controls.
- The regular (at least annual) review and approval of all Capital Clan Policies and procedures.
- The review of monthly and annual reports collated by Board members and MLRO.
- The implementation of any recommendations or findings that arise from reports.
- Performing annual reviews of MLRO's performance and conduct to ensure that the position is competently held.
- Ensuring that MLRO has sufficient resources to meet the requirements of their role.
- Implement a corporate culture enshrining a zero tolerance for financial crime.
- Ensure that all outsourced providers are screened for suitability before the onset of a business relationship.

The board is responsible for Capital Clan's approach to compliance and the implementation of adequate controls and resources.

1.3 Money Laundering Reporting Officer (MLRO)

To ensure compliance with relevant AML/AFT legislations, regulations, rules, and industry guidance, as well as oversee and implement the procedures reflected in the Policy, Capital Clan has appointed a Money Laundering Reporting Officer (MLRO) Carl Campbell CAMS.

MLRO is responsible for the following:

- The collection, analysis, and investigation of information on any suspicious activities escalated to them.
- The creation and provision of AML and CTF training to Capital Clan's employees.
- The development of policies outlining the controls and procedures implemented by Capital Clan to identify, prevent, and mitigate the occurrence and impact of Financial Crime.
- The annual review of Capital Clan's AML and CTF controls with findings presented to the board in a monthly meeting.
- The creation and presentation of Monthly Management Information regarding the activities of Capital Clan's customers.
- Further developing Capital Clan's internal controls used to identify suspicious activity.
- Keeping up to date with changes to industry best practice and any changes in applicable regulations and legislation.
- The handling of any complaints escalated to MLRO.
- The escalation of Suspicious Activity Reports (SARs) to FSP

The board will ensure that MLRO has a sufficient level of authority and independence within Capital Clan and that they have access to sufficient resources and information to carry out their responsibilities. This may include the appointment of an additional nominated officer to support the MLRO in their role.

1.4 Training

AML/CTF training would be imparted during induction of new employees and at least once a year to existing employees. MLRO will be responsible for the training to be imparted.

Participants of the training will be asked to respond to an AML/CTF questionnaire. Their understanding on AML/CTF will be evaluated based on their response to the questionnaire, a record of which will be maintained in Capital Clan files. A questionnaire has been created for the purpose.

In case a participant of the training is not able to pass the assessment, he/she will be asked to undergo the training and retake the assessment till he/she is able to pass.

1.5 Compliance Monitoring Team

Capital Clan's Compliance Monitoring Team's main objective is to conduct independent investigations of alerts and flags generated in the automatic screening systems applied to transaction monitoring and customer onboarding.

The Compliance Monitoring Team is also responsible for assisting MLRO in developing, implementing, maintaining, and enhancing the policies, procedures, and controls applied to the prevention of financial crime.

The responsibilities and day-to-day obligations of the Compliance Monitoring Team are:

- Monitoring of AML and CTF controls to verify the performance and adequacy.
- Investigate real-time transaction monitoring flags and alerts.
- Submission of suspicion reports to MLRO for review.
- Assess any flags of alerts pertaining to Know Your Customer (KYC) and Know Your Business (KYB) information.
- Communication with customers regarding updated KYC checks as required.
- Communication with customers regarding Enhanced Due Diligence (EDD) checks as required.
- Classify customers into the appropriate risk category in line with the documented risk category classification approach.

The Compliance Monitoring Team should make MLRO aware of any issues or doubt that they encounter whilst performing their duties.

1.6 All Employees

All employees of Capital Clan have responsibilities regarding AML and CTF imposed on them. A such all employees are required to follow the controls and procedures outlined in Capital Clan's policies.

Any employees found to be non-compliance may face disciplinary action which could include immediate dismissal.

All Capital Clan employees are obligated to be aware of and fully understand their responsibilities concerning the prevention of financial crime.

To ensure staff are appropriately prepared, Capital Clan's board ensures that sufficient resources are provided for all employees, and that where employees have any doubt, they should consult MLRO for guidance.

2. DEFINITION OF AML AND CTF

2.1. Money Laundering

Money laundering is the process of transforming the profits of crime and corruption into ostensibly 'legitimate' assets in a number of legal and regulatory systems. However, the term money laundering is sometimes used more generally to include misuse of the financial system.

The money laundering cycle can be broken down into three distinct stages; however, it is important to remember that money laundering is a single process. The stages of money laundering include the Placement Stage, Layering Stage and Integration Stage.

2.1.1 The Placement Stage

The placement stage represents the initial entry of the "dirty" cash or the proceeds of crime into the financial system. Generally, this stage serves two purposes:

(a) it relieves the criminal of holding and guarding large amounts of bulky of cash; and

(b) it places the money into the legitimate financial system. It is during the placement stage that money launderers are the most vulnerable of being caught.

This is since placing large amounts of money (cash) into the legitimate financial system may raise suspicions of officials.

The placement of the proceeds of crime can be done in a number of ways. For example, cash could be packed into a suitcase and smuggled to a country, or the launderer could use “smurfing” methods to avoid reporting threshold laws and avoid suspicion.

Some other common methods include:

- Loan Repayment - Repayment of loans or credit cards with illegal proceeds.
- Gambling - Purchase of gambling chips or placing bets on sporting events.
- Currency Smuggling - The physical movement of illegal currency or monetary instruments over the border.
- Currency exchanges - Purchasing foreign money with illegal funds through foreign currency exchange.
- Blending Funds - Using legitimate cash focused business to co-mingle dirty funds with the day's legitimate sales receipts.

To combat this and other international impediments to effective money laundering investigations, many like-minded countries have met to develop, coordinate, and share model legislation, multilateral agreements, trends and intelligence, and other information.

For example, international watchdogs such as the Financial Action Task Force (FATF) evolved out of these discussions.

2.1.2 The Layering Stage

After placement comes the layering stage (sometimes referred to as structuring). The layering stage is the most complex and often entails the international movement of the funds. The primary purpose of this stage is to separate the illicit money from its source. This is done by the sophisticated layering of financial transactions that obscure the audit trail and sever the link with the original crime.

During this stage, for example, the money launderers may begin by moving funds electronically from one country to another, then divide them into investments placed in advanced financial options or overseas markets; constantly moving them to elude detection; each time, exploiting loopholes or discrepancies in legislation and taking advantage of delays in judicial or police cooperation.

2.1.3 The Integration Stage

The final stage of the money laundering process is termed the integration stage. It is at the integration stage where the money may be returned to the criminal from what seem to be legitimate sources. Having been placed initially as cash and layered through a number of financial transactions, the criminal proceeds are now fully integrated into the financial system and can be used for any purpose.

There are many different ways in which the laundered money can be integrated back with the criminal; however, the major objective at this stage is to reunite the money with the criminal in a manner that does not draw attention and appears to result from a legitimate source. For example, the purchases of property, artwork, jewellery, or high-end automobiles are common ways for the launderer to enjoy their illegal profits without necessarily drawing attention to themselves.

2.2 Terrorist Financing and its 4-stage Process

Terrorism financing refers to activities that provides financing or financial support to individual terrorists or terrorist groups.

A government that maintains a list of designated terrorist organizations will also use laws to prevent money laundering being used to finance those organizations.

The terrorist financing 4-stage process involves:

- Collecting the funds intended for use in supporting the terrorist organisation from a variety of sources.
- Storing the funds, while determining and planning for their use.
- Moving the funds as and when required.
- Using the funds as needed to further the terrorist organisation's goals.

2.2.1 The Collection Stage

Typical sources of financial support for terrorist financing include:

- Direct donations by individuals and organisations.
- Use of charities and non-profit organisations.
- Criminal Activities.

2.2.2 The Storing Stage

The Storing of funds can be accomplished through means such as:

- Bank and other accounts
- Pre-paid cards
- Bulk cash storage.
- High value commodities such as oil, art/antiques, agricultural products, precious metals, and gems, and used vehicles'.
- Cryptocurrencies.

2.2.3 The Moving Stage

Well-known mechanisms for moving values include:

- Banking and financial sector.
- Remittance sector such as licensed Money Services Business.

- Informal value transfer systems (e.g., hawala) and foreign exchange houses
- Bulk cash smuggling.
- Smuggling high value commodities such as oil, art/antiques, agricultural products, precious metals, and gems, and used vehicles.
- Cryptocurrencies.

2.2.4 The Using Stage

Some examples of the use of funds in terrorism are:

Terrorist organisations: Weapons and materials.

- Administrative purposes and overheads.
- Media and messaging.
- Recruitment and training.
- Financial support for personnel and family.
- Communications equipment.
- Transportation.
- Bribing.
- Housing and planning and mission preparation to commit terrorist acts.

Foreign fighter:

- Travel services.
- Passport/visa costs.
- Outdoor/survival equipment.
- Weapons, and combat training.

Lone actors and small terrorist cells:

- Weapons and material.
- Vehicles (purchased or rented).
- Minimal financial means to provide for their own food.
- Shelter.
- Communications devices.
- Transport and any procurement requirements for terrorist plots.

2.3 Civil and Criminal Penalties

Government authorities of different countries and, in some cases, international organisations, may impose severe civil and criminal penalties against any person that violates the laws and regulations referred to in Section 1 of the Policy. Such civil and criminal legal penalties may include fines in the amount of up to hundreds of thousands or even millions of dollars, and the term of criminal punishment may be up to 14 (fourteen) years in prison. In addition, government authorities may confiscate any property involved in criminal violation of these laws and regulations, including companies, bank accounts, or any other assets that may be associated with criminal violations.

Under certain circumstances, companies may be deemed criminally responsible for the actions of their employees. In this regard, it is important for the employees of our Corporate Customers to have adequate knowledge in this sphere; it is also important that such Corporate Customers should ensure the compliance of their employees' actions with the said laws and regulations.

3. RISK METHODOLOGY

In developing and implementing controls Capital Clan must first identify and assess the AML and CTF that may arise during the provision of products and services. To understand its situation all products and services are broken down and assessed against a series of risk-based categories.

3.1 Risk Categories

The following risk categories are considered.

- 3.1.1 Customer Risk - The risk posed by Capital Clan's existing customer base.
    - Certain types of customers that may pose a higher risk are of significant importance. Customer risk also covers any risks posed by Capital Clan's products attracting potentially unwanted customers.
    - This risk category examines the potential flaws in any customer risk assessments that needs to take place before any agreement is put in place between Capital Clan and the customer.
- 3.1.2 Product Risk - The risk posed by the features of Capital Clan's products and services.
    - Specific risks need to address and mitigated as they are identified.
- 3.1.3 Transaction Risk - The risk that Capital Clan's products and services may be used for the purposes of financial crime.
    - Products may be used to perform transactions whose volume, value and/or purpose are criminal in their intent, resulting in the increase of Capital Clan's money laundering and terrorist financing risk.
- 3.1.4 Geographical Risk - The risk posed by the jurisdictions Capital Clan operates in and any customers who originate from there.
    - An increase in geography causes an increase in the risk of exposure to global sanctions, as well as other global aspects of money laundering.
    - This risk also covers jurisdictions outside of Capital Clan's operating area, which are areas potentially attracted to Capital Clan's products and services.
- 3.1.5 Business Risk - The risk that stems from Capital Clan's business operations.
    - This includes anything within Capital Clan's operating structure that may increase the risk of money laundering and can include employees participating in unlawful activity (knowingly or unknowingly) or being unaware of their employee responsibilities.
- 3.1.6 Distribution Risk – The risk arising from Capital Clan's distribution methods.
    - As this is likely provided by an expanded organisational framework, distribution presents several risks that must be addressed and mitigated.

3.2 Business Wide Risk Assessment (BWRA)

Capital Clan conducts annual Business Wide Risk Assessments (BWRA) to identify and assess the risks of money laundering and terrorist financing within its products and services. This assessment is documented and made part of Capital Clan's compliance policies and procedures.

The BWRA is an assessment of Capital Clan's activities within the approved policies and procedures and will be performed by MLRO. The BWRA also influences changes in policy and procedure where required.

If the BWRA finds that Capital Clan does not pay adequate attention to the provisions of the risk methodology, the AML and CTF controls, and/or other internal regulations concerning prevention of financial crime, the board will be immediately notified and an action plan to rectify the inadequacies put in place.

Any action plan addressing the gaps identified will be devised by MLRO and tracked to completion.

When considering the BWRA, risk items are identified with each having its risk impact to the business determined in two ways, either Inherent or Residual.

3.2.1 Inherent Risk

Inherent risk focuses on the natural risk that is present before any sort of control is implemented. An impact rating of High, Medium, or Low is achieved by considering the likelihood of any specific risk occurring and the severity of that risk if it were to occur. The combination of the ratings indicates an overall impact of the inherent risk and Capital Clan then applies appropriate controls based on the determined impact.

For High Likelihood events, the impact will be calculated as follows:

- Likelihood High and Severity High, the item will be High Impact.
- Likelihood High and Severity Medium, the item will be High Impact.
- Likelihood High and Severity Low, the item will be Medium Impact.

For Medium Likelihood events, the impact will be calculated as follows:

- Likelihood Medium and Severity High, the item will be High Impact.
- Likelihood Medium and Severity Medium, the item will be Medium Impact.
- Likelihood Medium and Severity Low, the item will be Medium Impact.

For Low Likelihood events, the impact will be calculated as follows:

- Likelihood Low and Severity High, the item will be Medium Impact.
- Likelihood Low and Severity Medium, the item will be Low Impact.
- Likelihood Low and Severity Low, the item will be Low Impact.

A risk matrix can also be used to visualise the impact scoring methodology:

	Severity		
Likelihood	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

3.2.2 Residual Risk

An effective control will reduce the inherent risk impact and create a lower risk impact. The residual risk is the risk that is left after all controls have been put in place. Where an effective control has been implemented to directly address the inherent risk, then the residual risk impact is considered a level lower than the inherent risk.

For example, High Impact risks are dropped to Medium, and Medium dropped to Low. Low Impact risks, although they have a control applied, remain Low Impact as a minimum standard and are not to be considered impossible.

Any implemented control should directly address the inherent risk and be signed off by the board.

3.3 SCHEDULE

As a minimum, Capital Clan will conduct a BWRA once a year. However, it may be necessary to conduct a BWRA because of a trigger event.

Trigger events can include, but are not limited to:

- When new products and services are introduced.
- When existing products and services change.
- When new customer demographics and geographies are considered.
- During changes in business structure.
- During regulatory changes.
- When a failing is identified in the way Capital Clan manage/control risks.

A BWRA could be triggered by anything that may affect Capital Clan's risk exposure.

MLRO will co-ordinate the assessment and will summarise the results in the annual review where the findings will also be presented to the board.

Priority will be given to areas where the risk is considered high, and controls will be tracked by MLRO to ensure they are implemented.

4. Customer Due Diligence (CDD)

Capital Clan has an obligation to identify and fully verify its customers without exception. For retail and corporate customers Capital Clan utilises KYC/B controls and third party software to identify and verify customers.

Capital Clan does not operate anonymous accounts or allows anonymous transfers of funds. Capital Clan applies KYC/B procedures in the following scenarios:

- Before establishing a customer or business relationship.
- During periodic reviews of customer data.
- During trigger events, related to the suspicion of financial crime being committed by a customer.
- Whenever significant changes to the CDD procedures of this policy are made.

During initial and renewed identification Capital Clan acts based on the perceived risk level of the given customers. Capital Clan classes all customers as either, high risk, medium risk, or low risk. The given risk level determines the level of scrutiny applies to a customer's application or account.

Prior to the completion of KYC/B, Capital Clan considers the inherent risk level of all customers to be medium risk, however, customers may be considered high depending on the preconceived circumstances.

A customer's risk level may be lowered by passing Capital Clan's CDD and/or EDD procedure which will determine whether the customer will be onboarded and the level of ongoing monitoring to be applied.

Capital Clan onboards customers who pass all KYC/B and EDD checks with a risk level of either low risk or medium risk.

Capital Clan does not engage with any customer with a residual risk of High. Certain high risk factors may not be lowered by completion of EDD, these include the following:

- The customer provides false information or refuses to complete KYC/B and/or EDD.
- The customer being identified as a PEP.
- The customer being identified as present on sanction lists.
- The customer falls outside of Capital Clan's risk appetite.
- The customer becomes the subject of an internal or external SAR.

All high risk customers and accounts are referred to the MLRO, who investigates such accounts and approves them only with board approval.

For clarity, any customer confirmed to be a PEP or present on an international sanctions list will also not be accepted.

Capital Clan uses ComplianceAssist to provide third-party software to collect and verify information during KYC/B procedures, this software allows us to set requirements where we can refresh and rescreen at set intervals – monthly, bi annually and yearly.

4.1 Know Your Customer (KYC)

In verifying the identity of retail customers Capital Clan requests the following information from the customer:

- Full Name (First, middle, and surname).
- Date of Birth.
- Residential Address.

- Nationality.
- Email Address.
- Contact Telephone Number.

Following collection of information Capital Clan verifies all provided information with the following methods:

- Proof of identity (passport, driver's license, national identity card).
- Proof of address (bank statement, utility bill); These must be dated within the last 3 months. Please note that a mobile statement/phone bill is not acceptable for this purpose.
- Confirmation of mobile number through activation code.
- Confirmation of email address with verification email and screening against internal records.
- Anti-Impersonation checks via the use of a photo of the customer taken live via the customer's device compared against the validated photo ID.
- Customer information is processed for PEP, adverse media, and sanction screening at point of application.

4.2 KNOW YOUR BUSINESS (KYB)

Before establishing a relationship with corporate customers, Capital Clan collects the following information:

- Incorporation details.
    - Legal Name.
    - Trading Name.
    - Registered Address.
    - Trading Address.
    - Website details.
    - Legal status.
    - Companies House registration number.
- Details of all directors and persons responsible for running the business.
    - Full Name (First, middle, and surname).
    - Date of Birth.
    - Residential Address.
    - Nationality.
    - Correspondence Email Address.
- Where applicable, details of Beneficial Owners (UBOs) with a holding of 20% or more. However, with entities who score High Risk in our Compliance Matrix, we will ask for all shareholding UBOs.
    - Full Name (First, middle, and surname).
    - Date of Birth.

    - Residential Address.
    - Nationality.
    - Correspondence Email Address.
    - Ownership %.
- The ownership structure of the business.
- Relationship with any parent company or organisational structure.
    - Incorporation details.
    - Ownership %.
    - Operational Address.
    - Correspondence Email Address.
- Details of the services and products provided by the business.
- Details of the business's internal risk controls, for applicable services.

All collected information is verified by Capital Clan using the following methods:

- Incorporation details are verified against relevant registers (e.g. Companies House)
- Incorporation details are verified against provided articles of association/company memorandum.
- Director, UBO, and Persons Responsible are screened as per Capital Clan's KYC procures.
- UBO proof of ownership is verified using requested documents.
- The business is screened for sanction/adverse media.
- UBOs, Directors, and Persons Responsible are screened for PEP, sanctions, and adverse media.

4.2.1 Directors, UBOs, and/or Persons Responsible

In checking directors, UBOs and Persons Responsible Capital Clan applies the following procedure:

Regarding corporate customers, Capital Clan uses the same third-party KYC software used for retail customers to verify the information and documentation provided by director(s), UBOs, and/or persons responsible.

The information required for verification is:

- Government issued photo identity document (e.g. Passport) containing:
    - Full name.
    - Date of birth.
    - Photo.
- Confirmation of their ownership or control within the corporate customer's business activities.
- Residential address confirmation.

Capital Clan require evidence that they are fit and proper persons. Checks need to be made regarding the following:

- Honesty, integrity, and reputation, including ensuring that they have not been convicted of any criminal offence.

- Competence and capability, including ensuring they have the sufficient knowledge and awareness of the regulatory environment to carry out their duties.
- PEP, adverse media, and sanction checks.

4.3 Anticipated Use Questions

To fully understand a customer's intended use of Capital Clan products and services questions are asked during KYC/B.

These may include:

- Why are you using Capital Clan's services?
- How often do you intend to deposit funds into your account?
- What is your anticipated monthly usage?

Based on the customer's response to the question Capital Clan can anticipate their use of services. Where Capital Clan detects that a customer's behaviour deviates from their anticipated use then the risk level of the account is increased and is monitored for potential suspicious activity.

4.4 Preferred Customer Base

Capital Clan has a preferred customer base consisting of the following:

- Retail Shops including online, Professional Services Companies and Management Consultants - Low risk with an average monthly value of less than £20,000 per month with an average transaction less than £500.
- High end retail shops selling high end branded goods and services – Low risk with an average monthly value between £20,000 and £200,000 per month with an average transaction of £1,000.

For clarity Capital Clan's accepts customer who fall outside of its preferred customer base, however such customers have an Initial risk level of High risk which may only be lowered by successfully passing KYC/B and EDD.

4.5 Customer Risk Levels

Upon completion of the CDD process, customers will assigned as either Low, Medium, or High risk.

Capital Clan classifies a customer as Low risk where the customer has passed all CDD requirements and has been successfully onboarded without issue.

This would include:

- Successful photo ID, and address verification, this includes retail customers, directors, UBOs, and Responsible Individuals.
- Provided UK, Malaysian and Singapore based documentation.
- Has not raised any PEP, sanction, or adverse media flags.
- Relationship to the business has been established.
- Falls within scope of preferred customer base.

Low risk customers are considered Capital Clan's ideal customer base and fall under automated monitoring procedures which utilise the least amount of Capital Clan's resources and attention.

Medium risk retail customers would include:

- A customer who was provisionally flagged for PEP, sanction, or adverse media, but had since been identified as a false flag.
- A customer whose activity poses an elevated risk of financial crime, but this risk has been mitigated by Capital Clan's controls.
- A customer over the age of 65.
- An existing customer who has been previously investigated.

Medium risk business customers would include:

- A customer/Director/UBO/Responsible Individual was provisionally flagged for PEP, sanction, or adverse media, but had since been identified as a false flag.
- A Director/UBO/are identified as residing outside the NEW ZEALAND but found to be legitimate.
- The customer has more than five UBOs at point of onboarding, was investigated and found to be legitimate.
- The customer's activity is inconsistent with other customers but not considered suspicious.
- The customer's activity is inconsistent with expected activity as per the customer's declared turnover, but within an allowed 10% variance.
- The customer has been included in previous investigations but not found to be sufficient enough to indicate suspicious activity.
- The customer has a trading history of one year or less.

Medium risk customers are manually monitored alongside automated monitoring. Manual monitoring will continue as long as MLRO perceives there to be a higher risk than normal posed by the customer.

If the customer activity is considered to be in line with expectations, then the risk rating can be lowered upon MLRO approval.

High risk customers are those with a significant failing when passed through the CDD procedures or those who are found to be participating in suspicious activity.

High risk customers are those who:

- Are over the age of 65 and fail to perform additional verification.
- Are individuals using repeat or similar information to gain access to Capital Clan's services.
- Have been provisionally flagged for PEP, sanction, or adverse media, but an investigation has not been able to confirm the flag(s) as false.
- Provided KYC/B details that do not meet Capital Clan's requirements or standards.
- Participates in activity unacceptable to Capital Clan and is considered suspicious.
- Are currently part of an ongoing investigation relating to suspicious activity.
- Customers with UBOs who reside outside of our preferred economic areas that cannot be reviewed/ identified.
- Customers with more than five UBOs that cannot be reviewed/identified.
- Are considered a risk to Capital Clan as determined by MLRO for any justifiable reason in relation to the prevention of financial crime, money laundering and terrorist financing.

Capital Clan does not provide products and services to customers deemed High Risk. Potential customers identified as High risk are to undergo additional due diligence and investigation. If the risk

level cannot be mitigated, then the customer will be notified of their failure to pass the onboarding process.

Any existing customer flagged as High risk will have their services halted until an investigation can confirm the accuracy of the flag and mitigate the risk. Where the risk can be lowered, the customer is categorised as Medium. Where the risk cannot be lowered, Capital Clan will enact the termination procedure.

Customers who fall outside Capital Clan's risk appetite are:

- Customers under the age of 18.
- Customers who cannot be fully identified and verified.
- Customers who reside/operate out of Capital Clan's are of operations.
- Customers who operate in prohibited territories or industries.
- Customers identified as PEPs.
- Customers identified as present on sanctions lists.
- Customers whose residual risk is identified as High-risk.
- Any other individuals or entities deemed unsuitable by Capital Clan's board.

Capital Clan does not offer services to any entities or individuals who fall in any way outside of its risk appetite. Any customer who falls outside of the risk appetite are rejected during onboarding or, if within customer base, offboarded.

4.6 Enhanced Due Diligence (EDD)

Capital Clan applies EDD to customers with a risk level of Medium or High. The resulting risk level following completion of EDD may be lower than the initial level applied to the customer.

Capital Clan's EDD procedure requires customers to provide further information and evidence to verify their identity, circumstances, and anticipated use of Capital Clan's products and services, this consists of:

- Additional documents requested and verified by KYC/B Software.
- Questions relating to the customer's intended use of the offered products and services.
- Information to verify the customer's source of wealth funding the account.
- The determination on which level of ongoing monitoring is applied to the customer.
- Where required the investigation of the customer by MLRO.
- Where required the approval of the customer by Capital Clan's board.

4.6.1 Source of funds

Capital Clan may require customers to verify how they intend to fund their account. This is required so at to determine the likelihood of the account being used for criminal purposes.

Capital Clan finds the following sources of wealth to be acceptable:

- Savings from salary (basic and/or bonus) detailing:
    - Salary per annum.
    - Employer's name and address.
    - Nature of business.

- Bank statements clearly showing receipt of last three most recent regular salary payments from named employer.
- Payslips from the last three months (including bonus payments, where appropriate) clearly showing named employer and amount received.
- Letter from employer confirming salary, on letter-headed paper clearly showing appointment held, registered address of company, nature of business and confirming that the customer is not a shareholder (this evidence can only be provided where the customer is not a shareholder).
- Audited personal tax statement of customer from regulated accountant clearly showing amount of income received and accompanied by updated proof of accountant's regulated status.

- Sale of investments/liquidation of the investment portfolio detailing:
  - Description of shares/units/deposits.
  - Name of seller.
  - Time period held.
  - Total sale/liquidation amount.
  - Date funds received.
  - Investment/savings certificates, contract notes, surrender statements or equivalent clearly showing date and amount of surrender/liquidation/maturity.
  - Bank statement clearly showing receipt of funds and name of investment company.
  - Letter detailing receipt of funds from a regulated accountant on letterheaded paper and accompanied by updated proof of accountant's regulated status.
- Sale of property detailing:
  - Sold property address.
  - Date of sale.
  - Total sale amount.
  - Letter from a licensed solicitor or regulated accountant, stating property address, date of sale, proceeds received, and name of purchaser.
  - Copy of sale contract as well as proof of receipt of funds (e.g. bank statement) clearly showing receipt of funds and name of purchaser.
- Company sale detailing:
  - Name and nature of Capital Clan.
  - Date of sale.
  - Total amount.
  - Client's share.
  - Copies of media coverage (if applicable).

- Letter detailing company sale signed by a licensed solicitor or regulated accountant on letter-headed paper and accompanied by updated proof of accountant's or solicitor's regulated status.
- Copy of contract of sale, plus bank statement showing proceeds received.

- Inheritance detailing:
  - Name of deceased.
  - Date of death.
  - Relationship to client.
  - Date received.
  - Total amount.
  - Solicitor's details.
  - Evidence that the customer is the inheritor.
  - Grant of Probate (with a copy of the Will) clearly showing the amount of inheritance.
  - Signed letter from a licensed solicitor or estate trustees on letter-headed paper clearly indicating the amount of inheritance, accompanied by updated proof of solicitor's regulated status.
  - The Will (if absolute amount is not clearly shown, other documentary evidence shall be required to support this).
- Divorce settlement detailing:
  - Date received.
  - Total amount received.
  - Name of divorced partner.
  - Copy of court order clearly indicating the amount of settlement.
  - Letter detailing divorce settlement as well as clearly indicating the amount of settlement and signed by a licensed solicitor on letter-headed paper accompanied by updated proof of solicitor's regulated status.
- Company profits detailing:
  - Name and address of company.
  - Nature of company.
  - Amount of annual profit.
  - Copy of latest audited company accounts.
  - Documentary evidence of the nature of business activity and turnover, e.g. a letter from a regulated accountant accompanied by updated proof of accountant's regulated status.

4.6.2 Prohibited Territories

Capital Clan has developed a list of territories deemed outside of its risk appetite which are considered prohibited.

Therefore, Capital Clan will not authorise transactions, enter into an agreement with customers, or partake in any business activity relating to the following territories deemed outside of Capital Clan's risk appetite:

- Afghanistan
- Albania
- Bahamas
- Barbados
- Belarus
- Botswana
- Burkina Faso
- Cambodia
- Cayman Islands
- Central African Republic
- Congo
- Crimea
- Cuba
- Ethiopia
- Ghana
- Iran
- Iraq
- Jamaica
- Lebanon
- Liberia
- Libya
- Mali
- Mauritius
- Morocco
- Myanmar
- Nicaragua
- North Korea
- Panama
- Republic of Guinea
- Russian Federation
- Senegal
- Somalia
- South Sudan
- Syria
- Sudan
- Trinidad and Tobago
- Uganda
- Ukraine
- Venezuela
- Yemen
- Zimbabwe

4.6.3 High Risk Territories

Capital Clan has also assigned a number of territories as High Risk. Although these territories do not pose any immediate financial crime risk, they are territories identified as having deficiencies in their internal counter money laundering and/or terrorist financing controls.

Because of a this, all transaction authorizations done within these territories will be monitored for unusual or suspicious activity. Additionally, any business relationship entered into with a corporate customer with ties to these territories will be reviewed as part of a business risk assessment. This must be approved by MLRO and Railsr before being initiated.

These territories are:

- American Samoa
- Anguilla
- Antigua and Barbuda
- Aruba
- Azerbaijan
- Azores
- Bahrain
- Belize

- Bermuda
- Bissau
- Bolivia
- Bosnia-Herzegovina
- Brazil
- British Virgin Islands
- Brunei Darussalam
- Burundi
- China
- Comoros
- Cook Islands
- Democratic Republic of the Congo
- Dominica
- Dominican Republic
- Ecuador
- Egypt
- Fiji
- Gaza Strip
- Gibraltar
- Guam
- Guatemala
- Jersey, Guernsey and Isle of Man
- Guinea
- Hati
- Kenya
- Lao
- Liechtenstein
- Madeira
- Maldives
- Marshall Islands
- Meno Sala
- Montserrat
- Namibia
- Nauru
- Nigeria
- Palau
- Pakistan
- Philippines
- Saint Helena, Ascension, and Trista
- Saint Pierre and Miquelon
- Samoa
- Seychelles
- St Kitts and Nevis
- St Maarten
- Tahiti
- Tonga
- Tunisia
- Turkey
- Turks and Caicos Islands
- Uruguay
- Vanuatu
- Virgin Islands
- Western Sahara.

4.6.4 Prohibited Industries

Similarly, to prohibited territories, Capital Clan has established a list of industries where it will not operate.

Therefore, Capital Clan will not engage with any business found or suspected to be involved with the following activities:

- Unregulated financial services.
- Pyramid or Ponzi schemes (multi-level marketing programs).
- Hawala.

- Un-licensed FX brokering.
- Binary options.
- Debt restructuring, credit repair, debt settlement, providing credit, debt collections.
- Gambling.
- Get rich quick schemes.
- Activities aimed at circumventing security controls (software, hardware).
- Unregulated pharmaceuticals or food supplements.
- Piracy or illegal streaming.
- Counterfeiting of goods and violation of intellectual property.
- Items that violate someone's privacy.
- Firearms and weapons.
- Dual use goods (software, technology, documents, and diagrams).
- Sale or trade of human organs.
- Unlicensed charities.
- Shell companies.
- Companies formed of Bearer Shares.
- Remittances funded in cash.
- Cheque handling and depositing.
- Cash handling and cash transfer services.
- Shell banks.
- Adult services connected to human trafficking; intermediation of prostitution; production, visual broadcasting of pornography or striptease clubs (the approach does not include literature, toys, DVD's, educational or scientific material or dating sites).
- Fourth party payment and multi-layered Money Service Business arrangements.
- Transactions for goods subject to export prohibition and restrictions.
- Transactions with living animals (except for horse riding and dog training).
- Political and religious organisations engaged in hate speech.
- Sanctioned entities.

4.7 Periodic and Event Driven Reviews

In order to make sure the due diligence information held regarding customer verification is up to date, Capital Clan will review and update the information every three years unless flagged as an ongoing medium or high risk customer, where it will be done more frequently.

SARs raised against a customer may also trigger an update request for KYC information, as will events that change the personal details stored against the account such as name and address.

Periodic KYC renewals, will be done on the following schedule using third-party KYC/B software:

- Low Risk Customers are reviewed every three years.

- Medium Risk Customers are reviewed annually.
- High Risk Customers are reviewed when discovered and if their risk category cannot be lowered through EDD then the relationship will be terminated.

The MLRO shall be involved in the process of EDD with customers who are categorized as high risk, or in cases where an increase of AML risk has been identified.

Renewed PEP and Sanction assessments will also be applied to all retail customers and corporate UBOs daily.

4.8 CUSTOMER FAIR TREATMENT

Capital Clan is committed to treating all customers who its products and services fairly, this includes providing appropriate resources, support, and communications to its customers.

Capital Clan understands that individuals within its customer base may have, or develop, vulnerable characteristics. Vulnerability impacts a customer's use of Capital Clan's services as it increases the risk of misuse by the customer or financial crime occurring via third party influence.

Throughout their relationship with Capital Clan customers may develop a wide variety of vulnerable characteristic which affect how they use the offered products and services. Where Capital Clan becomes aware that a customer has develop vulnerable characteristics then the customer is investigated by the MLRO.

The MLRO, with the approval of the board, then determines the allocation of resources to ensure that the customer fully understand and safely use Capital Clan's services.

Capital Clan uses age as a potential marker of vulnerability, all customers under the age of eighteen (18) fall outside of Capital Clan's risk appetite and are not onboarded as customers.

All customers over the age of Sixty-Five (65) have a default residual risk of medium, and those over the age of Seventy-Five (75) are classed as high risk. Such customers are at a higher risk of being targets or tools of financial crime. As such the Capital Clan requires such customers to provide the following additional information:

- For customers identified as over sixty-five years old, customers are required to undergo EDD as well as provide an additional photograph of the customer holding their proof of identity in line with Capital Clan's CDD requirements.

Where a customer becomes a vulnerable customer through the course of a business relationship, (e.g., the customer turns seventy years old) then the above outlined additional step will be taken during the next periodic or event driven KYC/B review.

If the customer refuses or is unable to provide the additional information, then the account is disabled, and the relationship terminated in line with Capital Clan's termination procedure.

Capital Clan also recognises customer vulnerability is not only related to age and knows anyone can find themselves in vulnerable circumstances at any time. This is due to several reasons, most notably in Capital Clan's consideration, financial circumstance.

To ensure it is correctly identifying and protecting vulnerable customers, Capital Clan:

- Understands the needs its target demographic and existing customer base.
- Makes sure employees have the right skills and capability to recognise and respond to the needs of vulnerable customers.
- Responds to customer needs through product design, customer service options and communication techniques.

- Monitors and assess whether they are meeting and responding to the needs of their customers with characteristics of vulnerability and make improvements where this is not happening.

Therefore, within its capacity as a financial service provider, Capital Clan deals with vulnerable customers and applies fair treatment by:

- Striving to ensure customers can be confident they are being delt with fairly.
- Ensuring products and services are sold to meet the needs of Capital Clan's identified customer demographics.
- Giving customers clear information regarding updates to the products.
- Not giving customers financial advice, as Capital Clan is not able to appropriately do so.
- Providing products that perform as the customers have been led to expect and have associated customer service at a standard they have been led to expect.

4.9 Approach to PEPs

Due to their position and influence, it is realised that many PEPs are in situations that can potentially be abused for the purpose of laundering illicit funds or other offences such as corruption or bribery. However, these recommendations should not be interpreted as all PEPs are involved in criminal activity.

PEPs are outside the risk appetite of Capital Clan. However, for sake of clarity and in order to ensure PEPs are not onboarded, the definition of a PEP is outlined below.

PEPs are defined as individuals entrusted with prominent public functions, including:

- Members of the administrative, management or supervisory bodies of state-owned enterprises, government corporations, government business enterprises, government-linked companies, or public enterprises.
- Members of courts of auditors or of the boards of central banks.
- Members of Goalcourts, of constitutional courts or of other high level judicial bodies.
- Members of NEW ZEALAND Parliament.
- Members of the governing bodies of political parties.
- Heads of State, heads of government, ministers and deputy or assistant ministers.
- High ranking military officials.

In some instances, a family member of a PEP may also be identified, which includes:

- The spouse or civil partner of a PEP.
- Children of a PEP and/or the spouses or civil partners of a PEP's children.
- Parents of a PEP.

PEP classification remains for a period of twelve months after the person ceases to hold the public function or longer if the PEP continues to pose a risk of money laundering and terrorist financing.

In accordance with regulatory obligations, all customers are reviewed using third-party KYC/B software to identify the presence of PEPs. Where information identified via KYC/B software suggests that a potential or existing customer could be a PEP, this should immediately be reported to MLRO for investigation and confirmation.

In confirmed cases the potential customer will be notified of a failure to complete the application. For confirmed cases relating to existing customers, the customer will be notified, and the termination process enacted.

4.10 Approach to Sanctions

International Financial Sanctions are imposed by national governments or International Bodies such as OFSI (Office of Financial Sanctions Implementation), UK HM Treasury (United Kingdom, Her Majesty's Treasury), the Office of Foreign Assets and Control (OFAC, US Treasury) and more. Engaging in business activities with sanctioned individuals and entities are prohibited and Capital Clan has an obligation to freeze the assets of any confirmed sanction match and report any transactions to the authorities.

For clarity, Capital Clan will not set up accounts for customers listed on any financial sanctions lists or carry out any transactions or business activity with them. This is because it is a criminal offence to make funds or financial services available to individuals or entities on sanctions lists.

Capital Clan is required to screen its customers and employees, filter its transactions, and prevent activity with sanction targets immediately once identified. Capital Clan does not whitelist any individuals, including their own employees. All customers and employees will undergo initial and ongoing sanction checks.

To minimize the customer risk, Capital Clan applies screening checks before establishing any business relationship, and daily thereafter regarding whether the members of its customer base are included in relevant watch or sanction lists accessed by the third-party KYC/B software.

In the event of a sanctions flag for new customers, the account opening process will be put on hold pending further investigation. In case of a flag, the case will be referred to MLRO to decide on the next course of action.

To determine if the flag is a false positive, MLRO must do a review to confirm whether the customer is confirmed to be on a sanctions list. After completing the review, MLRO will decide on whether to establish a relationship with the customer if the outcome of the investigation identifies the flag as false.

For a new flag on an existing customer, then the customer's account will be put on hold pending further review. The case will be escalated to MLRO for immediate review. If the flag is found to be a false positive, then the account's hold will be released, and the customer contacted regarding service disruption.

Should it be confirmed positive, the case will be presented to the authorities, and the board.

Where a potential associate is confirmed to be on a sanctions list the onboarding processes is stopped immediately. Capital Clan will report the event to the authorities, and the board immediately.

All confirmed sanction flags will be reported to:

NCA in the UK - Suspicious Activity Reports (SARs) and Prescribed

Transactions Reports (PTRs)

4.11 Approach to Adverse Media

Adverse Media Screening, also known as media monitoring or negative news screening, is undertaken as part of the KYC/B process. It is the process in which a customer, or prospective customer, is screened against negative information and publicly available data sources. This allows Capital Clan to identify and prevent potential risk events before they arise.

This includes searches against social media and online news providers for all customers during the normal KYC/B process. All customers are screened for adverse media at point of application, but where a customer is flagged as medium risk, this search will be done weekly to monitor for any changes in the

customer's public information. Where possible adverse media screening includes checking customer reviews for relevant findings.

Goaluses the latest technology to screen users of our services from Adverse Media. After verifying the users I.D, ShuftiPro automatically sweeps the lastest media databases for Adverse Media. If there are any true hits, our KYC team will be alerted and prompted to screen and check all hits.

4.12 Dormant Account Procedure

Dormant accounts are accounts that:

- Are initially inactive accounts where an account has been created but an initial transaction has not been made in 3 months.
- Are semi active accounts which have transacted but have been identified by Capital Clan as being continuously inactive for a period of three months.

Dormant accounts are suspended and investigated by MLRO, depending on the customer's response Capital Clan will:

- If satisfied with the customer's response Capital Clan will reactivate the account.
- Where unsatisfied Capital Clan will increase the customer's risk rating to Medium and require the customer to undergo EDD before the account is reactivated.
- Where there is no response, or where the customer refuses to undergo EDD, then the customer is offboarded.

Capital Clan carries out periodic reviews of all accounts to detect inactivity and are subsequently made dormant. The dormant account may be reactivated or closed via a written request from the customer, in such cases the customer must provide the following documentation and information for verification:

- Address.
- Contact details.
- Source of funds bank account details.
- Copies of any registration documentation given during CDD.

Customers who refuse to cooperate or who provide inadequate or false information are investigated by MLRO or Nominated Officer, a SAR is raised depending on the outcome of the investigation. Where the customer requests the account to be closed then Capital Clan offboards the customer. A customer that closes their account must pass Capital Clan's CDD checks again before the account can be reopened.

Upon successful completion of CDD, the customer's account is reactivated.

All accounts that are nominated as dormant, or dormant accounts that have been reactivated, are subject to ongoing monitoring to avoid unauthorised transactions from the account. Dormant accounts are monitored to ensure that only the original customer is using the account. The accounts are also monitored to ensure that Capital Clan employees do not engage in criminal activities using the dormant account.

Low activity accounts are accounts whose transaction volumes and value fall significantly under expected amounts in a three-month period. Any accounts found to be low activity are investigated by MLRO; the risk level of such accounts is elevated until the account successfully passes EDD.

4.13 Request for Information (RFI)

Capital Clan is required to share customer information when requested by relevant law enforcement authorities. MLRO is responsible for manging requests for information, and applies the following procedure:

- Capital Clan ensures that all employees are aware that MLRO is responsible for receiving and responding to requests from law enforcement agencies.
- Where any requests arise, employees direct all queries to MLRO immediately, employees do not engage in any discussions with the agencies themselves.
- MLRO verifies the legitimacy of the request and if the authorities have the appropriate court/legal documentation to validate the request. If not given this is requested before proceeding.
    - This includes searching for the requesting officer on the appropriate website/database.
- MLRO will assess whether the requesting third-party needs the information this includes confirming:
    - The exact information being requested.
    - The reason why the information is requested.
    - The consequences of not providing information.
- MLRO should consider the minimum information to satisfy the request.

Where requests for information involve specific accounts, Capital Clan will investigate any such accounts. Requests for information and any following investigations are recorded by MLRO and presented to the board as part of monthly management information packs.

5. Monitoring, Reporting and Record Keeping

Capital Clan implements monitoring procedures to detect any unusual or suspicious behaviour regarding its customers' financial activities. Capital Clan is required to perform monitoring of all transactions undertaken within its products and services and performs automated monitoring in real time and manual analysis post transaction.

There is no clear definition as to what activity can be called suspicious, but the techniques Capital Clan applies are used to monitor financial transactions and customer behaviour in search for patterns attempting to conceal the true intent of the funds.

These patterns can include various risk categories such as unusual activity patterns, significant volumes, high amounts, risky jurisdictions, and activity aimed at avoiding suspicion.

Capital Clan applies a number of monitoring techniques such as:

- Automated monitoring, which are alerts raised based on specific scenarios designed to identify suspicious transactions. The responsibility of addressing the alerts lies with the Compliance Monitoring Team. These alerts are addressed immediately.
- Manual analysis, which is undertaken every working day against the previous day's (or multiple days in the event of a weekend or holiday) transaction activity. Customer behaviour is reviewed to identify new patterns or activity that may be suspicious or indicate updates required to the alert scenarios applied to automated monitoring. Any customers flagged as Medium risk or higher are to undergo individual manual analysis and review until their risk category can be lowered.
- Additional review or monitoring may be undertaken in the event of a trigger event or if any employee comes across an event that might raise suspicion.
- Retrospective analysis of all previous account activity in the context of the current suspicious activity.

If during any of the above processes an employee identifies a suspicious transaction, then the SAR procedure will be followed.

5.1 Suspicious Activity

The definition of suspicious activity as well as the types of suspicious transactions which may be used for financial crime, money laundering and terrorist financing are almost unlimited. However, Capital Clan maintains adequate information and knows enough about its customers' expected activities to recognise that a transaction or a series of transactions is unusual or suspicious.

A suspicious transaction will often be one which is inconsistent with a customer's known or expected behaviour, or the expected behaviour of Capital Clan customers as a whole.

Examples of what might constitute suspicious activity are listed below. The relevant list is not exhaustive, nor does it include all types of activity that may be considered, nevertheless it sets a base level framework Capital Clan, and its employees can use in recognising the main instances of suspicious activity.

The detection of any of the transactions contained in the below list prompts further investigation and clarification on the circumstances surrounding the particular transaction.

Examples of suspicious activity are:

- Transactions with no discernible purpose or appear unnecessarily complex.
- Transactions which are inconsistent with Capital Clan customers' known activities.

- Transactions which are the same as or just below Capital Clan transaction limits.
- Transactions which are made to or from foreign (outside of issuance area) jurisdictions.
- Transactions whose nature, size or frequency appear to be unusual with regards to customer expectations.
- Transactions are flagged for investigation and a customer is reluctant/unable to provide supporting information/documents requested by Capital Clan within relation to the investigation of the flagged transaction.
- A customer requests to close their account following the request of supporting information/documents by Capital Clan.
- Transactions are flagged for investigation and a customer provides falsified information/documents within relation to the investigation of the flagged transaction.
- A customer tries repeated attempts to make transactions that exceed Capital Clan's transaction limits.

5.2 TRANSACTION MONITORING SYSTEM

In order to distinguish suspicious activity from legitimate activity, customer transactions are monitored by the Compliance Monitoring Team to reduce money laundering, layering and maintain fraud prevention via a fully automated, real-time monitoring.

Capital Clan has implemented a set of various flags and triggers to identify unusual transaction behaviour. These rules and the logic behind these flags are regularly reviewed in order to ensure that they continue to identify all possible suspicious or unusual transactions that could take place. For a full list of our rules, our MLRO is the owners and nominated person of these rules.

Real-time transaction monitoring is applied in one of two processes:

- Prevention, where real time blocks are applied to suspicious transactions before they are processed.
- Detection, where real time flags after the event where transactions are considered unusual but do not meet a requirement to be prevented from occurring.

Capital Clan's transaction monitoring system is also capable of quarantining any attempted transaction that appears suspicious in nature. Following the quarantining of any suspicious transaction, an investigation will take place.

Transaction monitoring is conducted on a risk-based approach. Depending on the risk posed by the specific transaction, the intensity of the checks as well as the measures taken for mitigating the risks may vary from:

- Requesting additional documentation/information to ascertain the nature of the transaction.
- To a possible block of the account or termination of the customer relationship.

Capital Clan applies increased transaction monitoring for customers that are flagged as medium risk. All transactions of such customers are manually reviewed by the Compliance Monitoring Team (and by the MLRO if necessary). Customers flagged as High risk are unable to transact until their risk rating can be lowered.

Capital Clan's MLRO is obliged to raise an Internal SAR as soon as practicable if they consider that there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering, or that terrorist property exists. Having made such a report, the director or employee concerned will have met his or her legal obligations under the regulations.

Different requirements for reporting suspicious transactions may depend on the nature and amount of a transaction and the risk profile of the customer.

The MLRO also has access to the results of transaction monitoring. Results are regularly reviewed by MLRO who in turn provides Management Information reports to the board as required.

The board will consider the appropriateness and effectiveness of Capital Clan's monitoring processes as part of its ongoing review of Capital Clan's business risk assessments and associated policies, procedures, and controls.

Where Capital Clan identifies weaknesses within its monitoring, it is ensured that the weaknesses are rectified in a timely manner.

The MLRO test and monitors the information our third party provider inputs into the database for both monitoring and screening.

5.3 Investigation

Transaction flags are investigated for legitimacy, and, in turn, it is decided if a SAR is required.

Since transaction monitoring is conducted on a risk-based approach, the MLRO and/or the Compliance Monitoring Team may request additional information depending on the nature of the transaction itself and overall transaction history of the customer.

The Compliance Monitoring Team can request the following supporting information/documents:

- Details of the nature of the transaction if it is not self-evident.
- Information and documents proving the customer's source of wealth and ownership over the method used to fund the Capital Clan account.
- Renewed KYC/B documents to reverify the customer's identity.
- Documents supporting the transaction with the merchant, including documents certifying the actual provision of goods or services (contracts, invoices, quotations etc.).

All communications, reviews, decisions regarding flagged transactions and SARs are documented and monitored by the MLRO.

5.4 Internal SAR Procedure

Where any employee has a suspicion regarding customer behaviour, they should report to MLRO immediately. Once an event is escalated to the MLRO then the following procedure is followed:

- MLRO collects information from the employee with suspicions.
- MLRO investigates the behaviour of the suspicious account.
- MLRO validates whether the activity is false.
- Where false the event is reported to the board in monthly MI and recorded, the monitoring level for the suspicious account is increased until renewed KYC/B is performed.
- Where the event is confirmed to be suspicious then MLRO immediately informs the board, collects information, prepares a SAR, and follows the External SAR procedure.

5.5 External SAR Procedure

As a financial service provider, Capital Clan is obliged to have external procedures in place to detect, report and disclose activities or financial transactions which do not fit with the normal course of business. Disclosures are made by submitting a SAR to the NCA.

The MLRO will receive any internal SAR reports or concerns relating to any suspected or actual financial crime and will record, investigate, and report this to NCA where necessary. The MLRO is responsible for all communications with FIU and any law enforcement agencies concerning the reporting of suspicious activity.

For reference, external SARs submitted to the NCA go through a web based portal.

All SARs are stored securely and is strictly confidential, accessible only by the MLRO and a designated other of the MLRO's choosing. All notifications made will be handled with strict confidentiality.

All customer activity is subject to ongoing monitoring, therefore:

- When suspicious activity is identified, the employee immediately notifies the MLRO in writing and in person where possible.
- The MLRO immediately reviews the details of the suspicious activity and seeks further information where necessary to determine whether financial crime is suspected.
- The relevant customer's account is internally flagged, and where necessary blocked, whilst the compliance investigation is underway.
- Any employee who is contacted by the relevant customer must not speak to them and pass them on to the MLRO immediately.
- If financial crime is not suspected, the reasons will be documented, identifying why no further action needs to be taken and, if appropriate, the customer's account will be unblocked.
- If financial crime is suspected, the customer relationship will be terminated.
- The MLRO incorporates any lessons learnt into future employee training, policies or processes as required.

5.6 Record Keeping

Reports and other data which may lead to identify clients' personal details shall be stored in the proper manner to prevent unauthorized persons from using the data.

Data shall be kept for at least five years after the completion of the transactions or five years following the end of a relationship between Capital Clan and the customer. In accordance with the principles of completeness, accuracy, and confidentiality, Capital Clan will keep the suspicious transaction reports and transaction records for at least five years from the date of the generation.

All documents and information related to the subject matter of commenced transactions shall be kept for at least five years after the completion of the transactions. Results of transactions analysis shall be kept for five years after the completion of the transactions.

All internal and external reports and board decisions are stored electronically as per Capital Clan's information security procedures.

6. OFFBOARDING PROCEDURE

Capital Clan offboards any customer found to have a residual risk of high or who falls outside of Capital Clan's risk appetite.

During offboarding, all funds are to be removed from the customer's Capital Clan ledger and returned to the original source. Once the customer's account has been reduced to zero balance and all products and services have been restricted, then the account is considered closed.

A customer may request to have their account closed with no resistance from Capital Clan. However, there are defined circumstances where it will be necessary to escalate issues to the board regarding the offboarding of a customer:

- A new/existing customer has been identified as being on a sanctions list.
- A new/existing customer has been identified as being a PEP.
- New legislation has been identified that may impact on Capital Clan's risk appetite.
- An event has occurred in which an existing customer has been found to be linked to financial crime, money laundering or terrorist financing.

Capital Clan will also choose to offboard customers if there has been a breach in customer terms and conditions such as:

- The use of Capital Clan's products and services in connection with industries that are prohibited.
- The use of Capital Clan's products and services for illegal purposes.
- Where Capital Clan's products and services have been used by anyone other than the onboarded customer.

When offboarding a customer regarding the above events, the following procedure needs to be followed:

- MLRO will escalate the matter to the board for them to decide on whether a customer is offboarded.
- The reason for offboarding will be fully documented.
- If not in breach of any legal requirements, a notice period will be agreed to ensure that all pending financial services are completed and settled.
- The offboarding notification that is communicated to the customer provides a clear period of time for the customer to find an alternative financial services provider.
- At the end of which the notice period, the account will be closed, and funds returned to the last known funding source of the customer (unless prohibited by law from doing so).
- Capital Clan will ensure removal of the customer details from any relevant database where it does not impact the need to retain information for AML and CTF purposes.
- Legal and regulatory issues encountered with the customer's offboarding are addressed systemically and, to avoid repetition of these problems with other customers, recorded and applied to the offboarding strategy or any other policy and/or procedure.

Should there be a conflict between the MLRO and the board regarding the offboarding of a customer, the MLRO's judgment should take precedence when offboarding a customer due to regulatory concerns or breach in compliance controls.

Details of any individuals who have been offboarded for breaching terms and conditions will be stored so as to identify them should they try and create a new account.