consult.
by momentum

Consult ("MC")
Risk Management and Compliance Programme (RMCP)

1. Definitions

1.1. **"AI" or "AIs"** means Accountable Institution in terms of FICA.

1.2. "**AML/CFT"** means Anti-money laundering and countering the financing of terrorism.

1.3. **"AML Requirements" -** Anti-Money laundering regulatory requirements include the following legislation:

1.3.1. Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FICA);

1.3.2. Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998) (POCA);

1.3.3. Prevention of Constitutional Democracy against Terrorism and Related Activities Act, 2004 (Act No. 32 of 2004) (POCDATARA);

1.3.4. The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended; and

1.3.5. The Drug Trafficking (Bailiwick of Guernsey) Law, 2000 as amended.

1.4. **"Business relationship"** A policy or Investment contract is a long-term business relationship that allows a client to transact with the insurer many times, for example, a recurring fixed-premium investment.

1.5. However, the take-on of each contract and subsequent trigger events, as described in the RMCP are considered a separate business relationship and therefore requires compliance.

1.6. Customer Due Diligence (CDD) is not required for subsequent transactions on a specific contract unless any client information has changed or become outdated.

1.7. **"Cash"** is defined in Section 1 of the FIC Act as:

1.7.1. Coin and paper money of the Republic or of another country that is designated as legal tender and that circulates as, and is customarily used and accepted as a medium of exchange in the country of issue; and

1.7.2. Traveller's cheques.

1.8. Cash, as defined in the FIC Act, does not include negotiable instruments, transfer of funds by means of bank cheque, bank draft, electronic funds transfer, wire transfer or other written order that does not involve the physical transfer of cash. These methods of transferring funds will not be covered by the CTR obligation under section 28 of the FIC Act.

1.9. **"CDD"** means Customer Due Diligence, and it refers to the knowledge that an AI has about its client and the institution's understanding of the business that the client is conducting with it.

1.10. **"Certified Copy"** for the purposes of this manual means a true copy of the original document which has been certified or commissioned.

1.11. **"Client"** who must be identified, established and verified means a:

1.11.1. Prospective client who intends on appointing MC or any one of its financial advisers as its broker on record;

1.11.2. Corporate clients such as companies and trusts;

1.11.3. Controlled and Non-Controlled Clients;

1.11.4. Policyholder or policy owner;

1.11.5. Life insured;

1.11.6. Premium payer;

1.11.7. Beneficiaries (only at claims stage, maturity or payout to beneficiary, beneficiaries on a Trust at new business);

1.11.8. Investment investor;

1.11.9. Cessionary (only if the cessionary is not a known bank);

1.11.10. A natural person acting on behalf of a client (please note that a client can refer to natural persons as well as legal persons); and

1.11.11. A client acting on behalf of another person.

1.12. **"Close associates"** are individuals who are closely connected to a prominent person, either socially or professionally. The term "close associate" is not intended to capture every person who has been associated with a prominent person. Examples of known close associates extracted from guidance provided by the FATF include the following types of relationships:

1.12.1. Known sexual partners outside the family unit (e.g. girlfriends, boyfriends, mistresses);

1.12.2. Prominent members of the same political party, civil organisation, labor or employee union as the prominent person;

1.12.3. Business partners or associates, especially those that share (beneficial) ownership of corporate vehicles with the prominent person, or who are otherwise connected (e.g., through joint membership of a company board); and

1.12.4. Any individual who has sole beneficial ownership of a corporate vehicle set up for the actual benefit of the prominent person.

1.13. **"Credible Vendors"** MC approved vendors that will provide third party electronic validation for natural and legal persons.

1.14. **"CTR"** refers to a cash threshold report submitted in terms of Section 28 of the FIC Act.

1.15. **"CRS"** refers to OECD Common Reporting Standards.

1.16. **"Copy"** includes making a photo copy and taking a digital photograph.

1.17. **"DPIP"** refers to Domestic Prominent Influential Person.

1.18. **"EDD"** refers to Enhanced Due Diligence.

1.19. **"Employee"** includes all levels of management, administrative staff, financial advisers, franchise principles, support staff, temporary employees, contractors, and any person directly or indirectly performing a function for or on behalf of MC.

1.20. **"FATCA"** refers to the Foreign Account Tax Compliance Act.

1.21. **"FATF"** refers to Financial Action Task Force.

1.22. **"FICA"** refers to the Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017).

1.23. **"FIC"** means the Financial Intelligence Centre, the government authority who ensures compliance with the Act and who MS reports to in terms of the Act.

1.24. **"FIC Guidance Note 7"** guidance on the implementation of various aspects of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), issued by the FIC on 2 October 2017.

1.25. **"FPPO"** refers to Foreign Prominent Public Officials.

1.26. **"GoAML"** refers to an integrated software solution implemented by the Centre as its preferred platform for registration, reporting, data collection, analysis and case management.

1.27. "KYC" means Know Your Client, in terms of the Financial Intelligence Centre Act (FICA).

1.28. **"ML/TF"** refers to Money Laundering and Terrorist Financing.

1.29. **"MLTFC Regulations"** refers to Money Laundering and Terrorist Financing Control Regulations issued under the FICA.

1.30. **"MLCO"** refers to the Money Laundering Compliance Officer.

1.31. **"MLRO"** means the Money Laundering Reporting Officer.

1.32. **"MMC"** means MMC Holdings Limited and all its subsidiaries.

1.33. **"MC" or "MC"** means MC (Pty) Ltd., AI/100831/.

1.34. **"MC Clients"** refers to any natural or legal person who has appointed MC or any of its representatives as its financial adviser / intermediary.

1.35. **"On-boarding staff"** refers to accountable employees responsible for taking on new financial advisers.

1.36. **"PEP"** refers to Politically Exposed Person.

1.37. **"PIP"** refers to Prominent Influential Person. It consists of DPIP, FPPO and Family members or Known Close Associates of DPIP & FPPO.

1.38. **"Product Providers"** refer to the financial institutions with whom MC has entered into an agreement with as listed in **Annexure A** and whose products and/or services are offered by one or more MC financial adviser.

1.39. **"Property"** in terms of POCDATARA means money or any other movable, immovable, corporeal or incorporeal thing, and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof.

1.40. **"Proceeds of unlawful activities"** means-

1.40.1. any property or any service, advantage, benefit or reward;

1.40.2. which was derived, received or retained-

- directly or indirectly;
- in South Africa or elsewhere; and
- at any time before or after the commencement of the POC Act; and

1.40.3. In connection with or as a result of any unlawful activity carried on by any person.

1.41. **"Prospective Client"** means a person who approaches the Business to enlist the Business' services, but that person has not yet appointed MC or any of its representatives as that person's financial adviser.

1.42. **"Representative"** as defined in Section 1 of the Financial Advisory and Intermediary Services Act 37 of 2002 (FAIS) means any person, including a person employed or mandated by such first-mentioned person, who renders a financial service to a client for or on behalf of a financial services provider, in terms of conditions of employment any other mandate, but excludes a person rendering clerical, technical, administrative, legal, account or other service in a subsidiary or subordinate capacity.

1.43. **"Retail investor"** refers to an individual who purchases securities for his or her own personal account rather than for an organization. Retail investors typically trade in much smaller amounts than institutional investors.

1.44. **"Tipping-Off"** refers to when an employee of MC discloses information to anyone outside the internal reporting chain as defined in this policy and in so doing the information given could prejudice an investigation into money laundering.

1.45. **"TTR"** refers to a Terrorist Transaction Report made in terms of section 28A of the FIC Act.

1.46. **"Transaction / single transaction"** a transaction carried out other than in the normal course of business for one of the parties. This includes:

1.46.1. Receiving an instruction or application that will result in a conclusion of a transaction or an alteration to the mandate or an addition of a product;

1.46.2. A trading instruction by a client to buy or sell securities or derivatives;

1.46.3. An amendment or variation of a trading instruction from a client;

1.46.4. Receiving an instruction or application that would create an inflow or outflow of funds; and

1.46.5. The closing of an account.

1.47. **"Shell Company"** means a company incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

1.48. **"STR"** refers to a suspicious transaction report made in terms of Section 29 of the FIC Act.

1.49. **"Unlawful activity"** means any conduct, which constitutes a crime or which contravenes any law whether such conduct occurred in the Republic or elsewhere**.**

2. Introduction

2.1. Combatting Money Laundering and Terrorist Financing is the responsibility of everyone**.**

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for the combating of money laundering, terrorist financing, and other related threats to the integrity of the international financial system.

South Africa is a member of the Financial Action Task Force (FATF) and as such have subscribed to the FATF Recommendations. The FATF Recommendations have been endorsed by over 180 countries, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism.

The South African government has demonstrated its commitment to combating money laundering and terrorist financing by implementing appropriate measures through the promulgation of FICA in order to introduce transparency in the South African financial system (based on robust customer due diligence measures). This will ensure that adequate information is captured in the records of financial and other institutions and to make the sharing of information that may support further investigation of money laundering and terrorist financing possible.

AIs' compliance with the regulatory requirements of FICA contributes to making it more difficult for criminals to hide their illicit proceeds in the formal financial sector and thereby profiting from their criminal activities and cutting off the resources available to terrorists.

FICA incorporates a risk-based approach to compliance elements such as customer due diligence (CDD) into the regulatory framework. A risk-based approach requires AIs to understand their exposure to money laundering and terrorist financing risks. By understanding and managing their money laundering and terrorist financing risks, AIs not only protect and maintain the integrity of their businesses but also contribute to the integrity of the South African financial system.

As a responsible corporate and global citizen; as well as an AI, MC takes its obligation to play its part in the combatting of money laundering and terrorist financing, and to contribute to the integrity of the South African financial system, very seriously.

To this end MC appreciates and is sincerely thankful for the co-operation and support provided by, and understanding of our financial advisers and their customers, in order to assist MC to fulfil its obligations in this regard.

Together we all contribute to the combatting of money laundering and terrorist financing, and thereby contributing to the integrity of the South African financial system, as well as the international financial system.

2.2. Amendments to FICA Changed the Regulatory Setting and Approach With Regard to ML/TF in South Africa.

The Financial Intelligence Centre Amendment Act changed the regulatory framework from a rules based environment to a principal based environment. Basically the regulator removed all the prescriptive requirements and exemptions, in order to allow AIs flexibility to implement an appropriate risk based approach unique to their business.

Previously, AIs were required to establish and verify the identity of a client in accordance with the MLTFC Regulations. The principle of client identification and verification is now expanded significantly with the introduction of the obligation to conduct CDD. As a result, the regulations and exemptions relating to client identification and verification have been amended significantly with most of the regulations having been repealed and exemptions having been withdrawn.

There is no longer a “one-size-fits-all” approach as the regulator recognized that this approach will not be appropriate. This is because different industries and/or sectors and businesses within those industries and/or sectors will be exposed to ML/TF risks in differing degrees based on the products and services provided by each business in those industries and/or sectors.

For example:

Generally the banking industry may be exposed to comparatively higher ML/TF risk than the insurance industry or asset management industry. Similarly the potential ML/TF risk that MC will be exposed to is comparatively lower than that for the insurer and/or investment product provider that MC supports. Banks, financial product providers, financial service providers and independent intermediaries are all AIs in terms of FICA.

MC would need to assess the potential ML/TF risk that the business relationship with its client may pose to its business.

When MC or any of its representatives introduces his/her client to a product provider, the last mentioned must assess the potential ML/TF risk that the client may pose to the business of the product provider. The product provider would need to consider the ML/TF risk indicators in its assessment of this business relationship.

In short, FICA requires MC to assess the ML/TF risk associated with each business relationship and/or transaction in respect of the unique circumstances and features of the products and/or services, offered by MC, and used by each particular client of MC.

2.3. The Impact of ML/TF Legislation on All

The AML Requirements are not intended to be unnecessarily intrusive and cumbersome. In fact, when considering the positioning made by regulators, AML requirements are intended to be an enhancement to already implemented prudent business practice; and should therefore seamlessly slot into existing processes.

Before engaging in a business relationship with a prospective client it is already practice to make enquiries regarding the identity of the client, usually via some type of application form requesting a range of personal information, to be used for business purposes. Consequently, AML requirements simply require an enhancement to this process by prescribing that:

a) some additional information/documents must be obtained from the client;
b) the organisation must understand the expected business pattern / conduct of the client;
c) some or all of the information collected must be verified;
d) the organisation must keep suitable records of the above-mentioned; and
e) the organisation must provide specified reports to the regulator.

In order to ensure that CDD are not unnecessarily intrusive and cumbersome MC will strive to, as far as practically possible, impose the least necessary burden on our clients in order to meet our

obligations in terms of AML Requirements. To this end, MC intends to over time roll-out and employ the use of:

a) appropriate technology;
b) government issued or controlled sources; and/or
c) reliable 3rd party vendors,

where MC is confident that it could adequately manage its ML/TF risks.

2.4. CDD is an Ongoing Process

Section 21C of FICA provides for ongoing CDD measures. These measures follow on from the obligation to understand the purpose and intended nature of a business relationship.

2.4.1 Ongoing CDD measures undertaken by the relevant product suppliers include:

the scrutiny of transactions undertaken throughout the course of a relationship, to ensure that the transactions being conducted in the course of a business relationship are consistent with an AI's knowledge of:

a) the client; and
b) the client's business and risk profile, including, where necessary, the source of funds.

2.4.2 Ongoing CDD measures undertaken by MC include:

a) ensuring that the information that an AI has about a client is still accurate and relevant, by obtaining updated verification documentation at least every two years.

The intensity and frequency of ongoing due diligence in respect of a given business relationship must be determined on the basis of MC's understanding of ML/TF risks associated with that relationship. This means that –

a) based on the type of client, e.g. trust, natural person etc.;
b) based on how the client conducts their affairs in relation to the business relationship with MC;
c) the type of product he/she subscribe for;
d) his/her political status; and
e) SOI / Wealth / SOF

Due to the nature of MC's business and the fact that clients may interact / transact with the relevant product providers directly without MC's knowledge, it may be necessary for MC to request additional supporting documentation before entering into a business relationship as expected by legislation. Ongoing monitoring at appropriate intervals may be based on certain trigger events such as regular checks against sanction lists.

3. Identification of MC

3.1. In terms of Schedule 1 of FICA, *MC* is an Accountable Institution (Schedule 1(12):

A person who carries on the business of a financial services provider requiring authorisation in terms of the Financial Advisory and Intermediary Services Act, 2002 (Act 37 of 2002), which is

registered at the Financial Intelligence Centre, with the FIC Organisational Identity Number: 24022 and Registration number: AI/100831/00012.

Under the provisions of Section 42A of FICAA, ***MC*** has appointed an-

Anti-Money Laundering Compliance Officer (MLCO):

Jacqueline Drotsky
268 West Avenue, Centurion, 0157
PO Box 7400, Centurion, 0046
Tel 087 742 7541
E-mail: Jackie.drotsky@momentum.co.za

Anti-Money Laundering Reporting Officer (MLRO):

Charlotte Archer
AML Operations Specialist
Momentum Metropolitan Holdings
268 West Avenue, Centurion, 0157
PO Box 7400, Centurion, 0046
Tel 012 673 7348
E-mail: charlotte.archer@mmiholdings.co.za

3.2. In terms of the Financial Advisory and Intermediary Services Act, 2002, (FAIS), MC is an authorised financial services provider and furnishes advice and intermediary services as a regular feature of its business. MC therefore acts as an intermediary between product providers and clients and is not a product provider in its own right.

4. Purpose of document

The Financial Intelligence Centre Amendment Act ("FICA: Act 1 of 2017") is formal legislation intended to combat money laundering activities by establishing a Financial Intelligence Centre ("FIC") and imposing certain duties on institutions and other persons, where such persons' or institutions services or products offered to clients may be used for money laundering purposes. These persons/institutions are in most instances clearly defined in the Act as "Accountable Institutions (AI)" but there are also some general duties imposed on other persons.

Apart from criminalising the act of money laundering, South African law also imposes a number of control measures that must be adhered to which are aimed to facilitate the prevention, detection and investigation of money laundering or terrorist financing activities.

These control measures introduced by FICA include requirements for institutions to establish and verify the identities of their clients, to keep certain records, to report certain information and to implement measures that will assist them in complying with the Act. To achieve this FICA further imposes on Accountable Institutions the requirement to implement a formal Anti-money laundering (AML) and Counter-Terrorist Financing (CTF) Risk Management and Compliance programme (RMCP).

This document is therefore prepared in compliance with Section 42 of FICA to advise employees on the specific duties of all employees, which flow from the requirements of the Act.

It is thus of paramount importance that all employees of MC understand and adhere to the contents of this document to avoid financial loss and reputational damage to MC and to avoid being held personally liable and accountable under the provisions of the Financial Intelligence Act.

5. Key elements to ensure compliance with FICA

5.1. Board Responsibility for Oversight of Compliance

The Board of MC has effective responsibility for compliance with FICA and the RMCP and references to compliance in this RMCP generally are to be taken as references to compliance with the RMCP. Reference in this RMCP to "the Board" must also be read as meaning the senior management of the business.

The Board and senior management of any business are responsible for managing the business effectively. In particular the Board must take responsibility for the RMCP on reviewing compliance and must consider the appropriateness and effectiveness of compliance and the review of compliance at appropriate intervals. In this regard approval of the RMCP by the Board of directors and senior management of the relevant AI will establish a formal yearly review process.

A financial services business or AI must also ensure that there are appropriate and effective policies, procedures and controls in place which provide for the Board to meet its obligations relating to compliance review, in particular the Board must:

a) Ensure that the compliance review policy takes into account the size, nature and complexity of the business and includes a requirement for sample testing of the effectiveness and adequacy of the policies, procedures and controls including where aspects of the due diligence process are undertaken via electronic methods and systems;
b) Consider whether it would be appropriate to maintain a separate audit function to assess the adequacy and effectiveness of the area of compliance;
c) Ensure that when a review of compliance is discussed by the Board at appropriate intervals the necessary action is taken to remedy any identified deficiencies;
d) Ensure that the financial services business in meeting its obligation, complies with the Regulations and applicable local law which is consistent with the FATF Recommendations; and
e) Provide adequate resources either from within the financial services business, within the group, or externally to ensure that the AML/CTF policies are adhered to.

5.2. Risk management

a) Undertake ML and TF risk assessments;
b) Establish and implement AML and TF risk frameworks within which to manage the AI's risks; and
c) Develop and implement risk rating models for various business relationships with the relevant supporting due diligence processes.

5.3. Governance and oversight

a) Implement appropriate AML and CTF policies;
b) Implement processes for ongoing review and governance of policies;

c) Implement governance structures roles and responsibilities, reporting frameworks and processes; and
d) Managing assurance and regulatory reviews.

5.4. People

a) Accountable persons to manage ML and TF risks;
b) Ensure the necessary AML and CTF skilled resources are employed; and
c) Implementation of appropriate AML and CTF training programs.

5.5. Process and technology

a) Implement simplified and enhanced CDD measures;
b) CDD programs to meet regulatory requirements whilst remaining customer centric;
c) Establish effective records management practices and processes with supporting systems; and
d) Source appropriate supporting AML/CTF technology solutions and systems.

6. Risk Management and Compliance Programme (RMCP)

The RMCP is a documented record of MC's control measures and efforts to comply with its obligations under FICA on a "risk sensitive" basis.

Below follows the minimum requirements of a RMCP and this document is therefore structured to address these minimum requirements:-

a) Document, maintain and implement a RMCP;
b) Incorporate all the elements in FICA that are linked to Client Due Diligent Measures (CDD);
c) Describe the application and implementation of measures of MC's Risk Based Approach that will as a minimum include:-
    - The end to end CDD process, i.e. from establishing a business relationship, on-boarding a client, on-boarding of financial advisers, ongoing monitoring of client behaviour, to termination of the relationship with recordkeeping of all relevant client detail and transaction information;
    - Ongoing CDD processes in dealing with High Risk clients or status changes in a client's risk profile from Low to High Risk;
    - Measures to deal with doubt about the veracity of previously obtained CDD information;
    - Measure to deal with suspicion formed of ML or TF activities formed post client on-boarding; and
    - Measures to prevent the entering into or maintaining a business relationships if MC cannot perform CDD and the manner in which MC will terminate an existing business relationship when unable to complete CDD requirements, etc.
d) Describe implemented governance processes for example related to executing reporting obligations, training programs, monitoring programs etc.

7. General MC Business practice

7.1. Dealing with cash transactions

a) No staff member/contractor or financial advisor acting on behalf of MC may deal in cash, they are not allowed to receive funds from a client or debtor when establishing a business relationship or facilitating a business transaction;
b) No staff member/contractor or financial advisor acting on behalf of MC may deposit cash or assist in depositing cash on behalf of any client to any product provider bank account; and
c) No staff member/contractor or financial advisor may suggest to a client to pay an amount in cash in to any product provider bank account.

8. Risk-Based Approach (RBA)

The **RBA** is the most cost-effective and proportionate way to manage **ML/TF** risks facing any **AI** and to ensure that measures to prevent or mitigate **ML/TF** are commensurate with the risks identified.

The Risk Based Approach requires an AI to understand its inherent and specific exposure to money laundering and terrorist financing risks and to establish a reasonable compliance and risk management programme to manage the risks of AML and TF, with the intent to protect and maintain the integrity of the South African financial system.

The **RBA** is not a "zero tolerance" approach as there may be instances where MC has taken all reasonable measures to identify and mitigate **ML/TF** risks, but it is still exploited for **ML/TF** purposes.

The **RBA** has, amongst others, the following advantages:

a) It recognises that ML/TF threat to MC varies across its client types (natural person, company, trust, etc.) product types and geographical location;
b) Resources are directed in accordance with priorities, so that the greatest risks receive the highest level of due diligence;
c) If applied correctly, it will improve the efficacy of measures to combat ML/TF while promoting financial inclusion without undermining AML/CFT objectives;
d) It allows MC to simplify the due diligence measures applied where they assess ML/TF risks to be lower; and
e) Instead of relying on rigid requirements in regulations and exemptions granted, MC will have greater discretion to determine the appropriate compliance steps to be taken in given instances based on the appropriate ML/TF risk indicators assessed.

The **RBA** is a systematic approach to risk management and involves:

a) risk identification and assessment – taking account of the client type (natural person, company, trust, etc.), product type (investment, short-term Insurance policy, etc.) and geographic location (where the client and/or intermediary is resident or incorporated, etc.) to identify the **ML/TF** risk to MC;
b) risk mitigation – applying appropriate and effective policies, procedures and controls to manage and mitigate the risks identified;
c) risk monitoring – monitoring the effective operation of the **MC's** policies, procedures and controls; and
d) policies, procedures and controls – having documented policies, procedures and controls to ensure accountability to the board and senior management.

9. ML/TF Risk Assessment

9.1. ML/TF Risk Exposure

ML/TF risks are threats and vulnerabilities which put **MC** at risk of being abused in order to facilitate **ML/TF** activities. These relate to the potential that clients, by using **MC's** services, can exploit **MC** to promote **ML/TF** activities. The nature of these **ML/TF** risks relate to a number of aspects such as:

a) the features of the intended target market of clients who are likely to use MC's services;
b) the geographic locations of MC's operations and of its clients;
c) the features of a particular product type; and
d) the features and complexity of the client type, etc.

Risk in the context of **ML/TF** can be thought of as the likelihood and impact of **ML/TF** activities that could materialise as a result of a combination of threats and vulnerabilities manifesting in an accountable institution.

Risk rating implies assigning different categories to the various **ML/TF** risk indicators (client types, product types and geographic locations) according to a risk scale and classifying the **ML/TF** risks pertaining to different relationships or client engagements in terms of the assigned categories. No two **AIs** are the same, therefore, the level of risk and the risk ratings attributed to particular business relationships or other engagements with clients may vary from one **AI** to another.

The **ML/TF** risk associated with a particular client engagement does not remain static. Factors underlying any given risk rating will inevitably change over time. It is therefore necessary that **AIs** re-evaluate the relevance of particular risk factors and the appropriateness of previous risk-ratings from time to time – ongoing **CDD**.

9.2. ML/TF Risk Rating Methodology

Momentum Metropolitan Holdings implemented a risk rating standard as described in a document entitled "*ORSA Standard Qualitative Risk Rating Methodology Momentum Metropolitan Holdings Ltd*" ("**Momentum Metropolitan** ORSA Standard"). MC, as a subsidiary of the Momentum Metropolitan Holdings Group of Companies, subscribes to this standard when applying its risk ratings to the financial advice process of its financial advisers.

Table 1 and *2* below depict the distribution of the risk exposures that reflect the outcome of this methodology.

Table 1: Momentum Metropolitan ORSA Standard Qualitative Risk Rating Methodology

Likelihood		Impact				
		Insignificant	Minor	Moderate	Major	Severe
		1	2	3	4	5
Almost Certain	5	Medium Low	Medium High	Medium High	High	High
Likely	4	Low	Medium Low	Medium High	Medium High	High
Possible	3	Low	Medium Low	Medium Low	Medium High	Medium High
Unlikely	2	Low	Low	Medium Low	Medium Low	Medium High
Rare	1	Low	Low	Low	Low	Medium Low

Table 2: Momentum Metropolitan ORSA Standard Qualitative Risk Rating Methodology

Likelihood		Impact				
		Insignificant	Minor	Moderate	Major	Severe
		1	2	3	4	5
Almost Certain	1	5	10	15	20	25
Likely	4	4	8	12	16	20
Possible	3	3	6	9	12	15
Unlikely	2	2	4	6	8	10
Rare	1	1	2	3	4	5

The **Momentum Metropolitan** ORSA Standard is a five tier rating scale. **MC**, as previously stated, is a financial services provider, offering financial products from various product providers (regulated products and services, i.e. collective investment schemes, life insurance products, discretionary and non-discretionary investment products, short-term insurance products, health service benefits), and operates in the Republic of South Africa only.

MC has therefore concluded that the five tier rating scale would be the most appropriate risk rating methodology to implement in its environment.

The following **ML/TF** risk indicators have been considered and represent the components of the risk matrix that will be used to assess the **ML/TF** risk associated with a Single Transaction Risk Matrix") that are relevant to an engagement with a client:

a) Client type; and
b) Product type.

A risk matrix have been developed for the above-mentioned **ML/TF** risk indicators, in order to provide a reasonable basis for the assessment of these **ML/TF** risk indicators, which are discussed in more detail below.

9.3. ML/TF Risk Indicator Risk Matrixes

9.3.1. MC Product type Risk Matrix

The contribution of the product type offered by MC to the overall ML/TF risk exposure of the organisation is significant. This is a key risk indicator in the assessment of the overall ML/TF risk as some of the various products offered by MC may be potentially abused for ML/TF purposes as a result of the unique features of the particular product.

The following three tier ML/TF rating methodology have been developed and have been derived from the MC ML/TF Standard Qualitative Risk Rating Methodology discussed in 9.2. *Table 3* and *4* below depict the distribution of the risk exposures that reflect the outcome of Product type ML/TF Risk Matrix:

Table 3: MC Product type ML/TF Risk Matrix

		Impact				
		Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
Likelihood		**1**	**2**	**3**	**4**	**5**
Almost Certain	**5**	Medium Low	Medium High	Medium High	High	High
Likely	**4**	Low	Medium Low	Medium High	Medium High	High
Possible	**3**	Low	Medium Low	Medium Low	Medium High	Medium High
Unlikely	**2**	Low	Low	Medium Low	Medium Low	Medium High
Rare	**1**	Low	Low	Low	Low	Medium Low

Table 4: MC Product type ML/TF Risk Matrix

Likelihood		Impact				
		Insignificant	Minor	Moderate	Major	Severe
		1	2	3	4	5
Almost Certain	5	5	10	15	20	25
Likely	4	4	8	12	16	20
Possible	3	3	6	9	12	15
Unlikely	2	2	4	6	8	10
Rare	1	1	2	3	4	5

Table 5: MC Product type ML/TF Risk Matrix

Products	Client type = Low risk	Client type = Medium-Low risk	Client type = Medium-High risk	Client type = High risk
Pure Risk	Low	Medium Low	Medium High	High
Short term insurance (including Gap cover)	Low	Low	Medium Low	Medium High
Health Service Benefits	Low	Medium Low	Medium Low	Medium High
Fixed term investments (penalties for early withdrawal)	Low	Medium Low	Medium High	Medium High
Guaranteed products (no early withdrawal)	Low	Medium Low	Medium High	Medium High
Compulsory money products	Low	Medium Low	Medium Low	Medium High
Liquid Investments	Medium Low	Medium High	High	High
Call and savings Accounts	Medium Low	Medium High	High	High
Voluntary Annuities	Medium Low	Medium High	High	High
Endowments	Low	Medium Low	Medium High	High
Offshore investments	Low	Medium Low	Medium High	High

9.3.2. **Process to assess ML/TF risk relating to financial services rendered to the different client types:**

The contribution of the types of clients of MC to the overall **ML/TF** risk exposure of the organisation is significantly higher. This is a key risk indicator in the assessment of the overall **ML/TF** risk as a result of a business relationship entered into with the client.

The following five tier **ML/TF** rating methodology have been developed and have been derived from the **MC ML/TF** Standard Qualitative Risk Rating Methodology discussed in 9.2. *Table 6* and *7* below depict the distribution of the risk exposures that reflect the outcome of the **MC** Client **ML/TF** Risk Matrix:

Table 6: MC Client ML/TF Risk Matrix

Likelihood		Impact				
		Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
		1	**2**	**3**	**4**	**5**
Almost Certain	**5**	Medium Low	Medium High	Medium High	High	High
Likely	**4**	Low	Medium Low	Medium High	Medium High	High
Possible	**3**	Low	Medium Low	Medium Low	Medium High	Medium High
Unlikely	**2**	Low	Low	Medium Low	Medium Low	Medium High
Rare	**1**	Low	Low	Low	Low	Medium Low

Table 7: MC Client ML/TF Risk Matrix

		Impact				
		Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
		1	**2**	**3**	**4**	**5**
Almost Certain	**5**	5	10	15	20	25
Likely	**4**	4	8	12	16	20
Possible	**3**	3	6	9	12	15
Unlikely	**2**	2	4	6	8	10
Rare	**1**	1	2	3	4	5

Table 8 below indicates the outcome of the risk rating methodology applied to MC Legal status, Structure And Complexity of the client type.

Table 8: MC Client type ML/TF Risk Matrix

No.	Legal Structure and Complexity	Weighted Impact Assessment	Likelihood Assessment	Legal Structure and Complexity ML/TF Risk Rating Score	Legal Structure and Complexity ML/TF Risk Rating
1	Domestic natural person	2	2	4	Low
2	Foreign National natural person	2	3	6	Medium Low
1	Public Company - Listed on a recognised exchange	5	1	5	Medium Low
2	Public Company - Not listed on a recognised exchange	3	5	15	Medium High
3	Private Company - Unlisted	5	4	20	High
4	State-owned Company - Unlisted	5	4	20	High
5	Personal Liability Company - Unlisted	5	4	20	High
6	Non-Profit company - Unlisted	5	4	20	High
7	Closed Corporations (South Africa) - Unlisted	5	4	20	High
8	Partnerships - Unlisted	5	4	20	High
9	Trusts - Unlisted	5	4	20	High
10	Highly regulated South African entities - Collective Investments	1	1	1	Low

11	Other entities not mentioned above (i.e. stokvels, churches, clubs, schools, universities, municipalities, cooperatives (associations), etc.) - Unlisted	5	4	20	High

The factors identified that will influence the impact rating, and the weight that each factor will contribute in order to determine the overall impact rating for the legal structure and complexity, is indicated in *Table 9* below.

Table 9: ML/TF Risk Indicators Relating To the Legal Structure and Complexity (Factors Influencing Impact)

No.	Risk Indicator	Risk Indicator Description	Weighting of Indicator
1	Structure	This indicator considers the extent to which a specific legal entity structure could potentially be exploited for **ML/TF** purposes	**50.00%**
2	Complexity	This indicator considers the extent to which the potential complexity of a specific legal entity structure could potentially be exploited for **ML/TF** purposes	**50.00%**
			100.00%

The factors identified that will influence the impact rating, and the weight that each factor will contribute in order to determine the overall impact rating for the PIP status of the client, is indicated in *Table 10* below.

Table 10: ML/TF Risk Indicators Relating to the Prominent Influential Person status (Factors Influencing Impact)

No.	Risk Indicator	Risk Indicator Description	Weighting of Indicator
1	Political / Influential Status	This indicator considers whether a client or a prospective client, with whom it engages to establish a business relationship, or the beneficial owner of that client or prospective client, is either a foreign prominent public official ("FPPO") or a domestic prominent influential person ("DPIP") which requires additional vigilance and scrutiny as prescribed by law	**100.00%**

Table 11 below provides a summary of the **MC** Prominent Influential Person Status **ML/TF** Risk Register and only show the weighted average of the impact risk assessment the prominent influential person status of the client.

Table 11: MC Prominent Influential Person Status ML/TF Risk Register

No.	PIP Status	Weighted Impact Assessment	Likelihood Assessment	PIP Status ML/TF Risk Rating Score	PIP Status ML/TF Risk Rating
1	Domestic prominent influential person (DPIP) - South Africa {≤6 Months}	4	3	12	Medium High
2	Domestic prominent influential person (DPIP) - South Africa {>6 Months & preceding 12 Months}	3	3	9	High
3	Foreign prominent public official (FPPO) {Preceding 12 Months}	3	3	9	High
4	Not Applicable	1	1	1	Low

9.3.3. Process to assess ML/TF risk relating to geographic locations:

Should a client reside or be incorporated in a sanctioned country or a high-risk jurisdiction geographic location, the business CANNOT be accepted and must be declined. This is because these geographic locations either appear on the FATF High Risk and other monitored jurisdiction list and/or the geographic locations have sanctions or embargos imposed on them, and/or the geographic location do not subscribe to the combatting of ML/TF. Accepting business from in one of these geographic locations will expose MC to severe ML/TF risk. Should there be merit for an exception to be made such exception must be authorised on a MC executive level only.

The Treasury Department's Office of Foreign Assets Control (OFAC) administers and enforces economic sanctions imposed by the United States against foreign countries. Depending on the country, OFAC programs may freeze assets of embargoed countries, prohibit payment of funds to individuals and countries on the embargo list, or prohibit provision of services to countries subject to US sanctions. These sanctions may require obtaining OFAC approval before conducting research or other activities in or involving the sanctioned country. Some sanctions are more restrictive than others, and apply to the whole country, while others are specifically target on certain individuals or entities within a country. Currently, sanctioned countries include

the Balkans, Belarus, Burma, Cote D'Ivoire (Ivory Coast), Cuba, Democratic Republic of Congo, Iran, Iraq, Liberia, North Korea, Sudan, Syria, and Zimbabwe. The list of sanctioned countries is updated periodically and is available **here**.

OFAC can also designate persons and entities (including persons and entities in the United States) as Specially Designated Nationals ("**SDN list**"). OFAC designates persons and entities as SDNs for narcotics trafficking, weapons proliferation and other reasons. When entering into discussions with a proposed collaborator, it is critical to check the SDN list for the name of the person or entity with which you are dealing

The factors identified that will influence the impact rating, and the weight that each factor will contribute in order to determine the overall impact rating for the source of funds and/or wealth of the client, is indicated in *Table 12* below.

Table 12: ML/TF Risk Indicators Relating To the Source of Funds and/or Wealth (Factors Influencing Impact)

No.	Risk Indicator	Risk Indicator Description	Weighting of Indicator
1	Activity Generating Funds and/or Wealth	This indicator considers the extent to which a specific activity that may generate the client's funds or wealth could conceal the true nature of the origin of the funds and/or wealth of the client	**100.00%**

Table 13 below provides a summary of the **MC's** Source of Funds and/or Wealth **ML/TF** Risk Register and only show the weighted average of the impact risk assessment the source of funds and/or wealth of the client.

Table 13: MC Source of Wealth ML/TF Risk Register

No.	Source of Funds and/or Wealth	Weighted Impact Assessment	Likelihood Assessment	Source of Funds and/or Wealth ML/TF Risk Rating Score	Source of Funds and/or Wealth ML/TF Risk Rating
1	Donation	2.5	2	5	Medium Low
2	Funds Received as beneficiary in trust	3	3	9	Medium Low
3	Funds Received as beneficiary of a retirement fund	1	1	1	Low
4	Funds Received as beneficiary of an	1	2	2	Low

No.	Source of Funds and/or Wealth	Weighted Impact Assessment	Likelihood Assessment	Source of Funds and/or Wealth ML/TF Risk Rating Score	Source of Funds and/or Wealth ML/TF Risk Rating
	insurance policy				
5	Funds received from import/export business	5	5	25	High
6	Inheritance	1	1	1	Low
7	Investment activity (income and/or proceeds of sale)	4	2	8	Medium Low
8	Lotto	2	2	4	Low
9	Profits and/or income from business activities (if not salary)	4	4	16	Medium High
10	Salary	3	1	3	Low
11	Sale of fixed property (real estate)	4	2	8	Medium Low
12	Sale of movable assets (i.e. motor vehicle, furniture, stamp collection, jewellery, etc.)	5	3	15	Medium High
13	Savings	4	2	8	Medium Low

Table 14 below provides a summary of the **MC** World-Check Adverse Findings **ML/TF** Risk Register and only shows the risk assessment of the World-Check findings in respect of the client.

Table 14: **MC World-Check Adverse Findings ML/TF Risk Register**

No.	World-Check Findings	World-Check Adverse Findings ML/TF Risk Rating
1	No adverse findings	Low
2	Some findings noted – minor concerns	Medium Low
2	Some findings noted - moderate concerns	Medium High
3	Adverse findings	High

10. Risk Mitigation

10.1. Differentiation based on Risk Profile

The risk profiling exercise as mentioned above will result in 3 categories of client types within MC, being low risk, medium risk and high risk client types.

Risk mitigation will be employed for each classification of client in the context of their risk profile in order to minimise the potential Money laundering and Terrorist Financing risks facing the company.

Even though MC will apply a standard due diligence process across all client types, certain client types risk rated as higher risk may trigger additional (enhanced) due diligence measures.

Before MC may enter into a relationship with a client, the client will be required to provide at a minimum the information and documentation as listed in the relevant FICA CDD checklist.

As mentioned in previous paragraphs, MC is a financial services provider who acts as the intermediary, facilitating transactions between various product providers and clients, via a franchise network of financial advisers. The financial advisers will take all reasonable steps to identify and verify their clients, however a lot of reliance is placed on the product provider to conduct ongoing CDD and to verify and validate their clients' information.

10.1.1. Additional Requirements

The client will as a standard, be subject to a **WorldCheck screening** to determine their status with regards to UNSEC security lists and possible status as FPPO and DPIP. However, as indicated on the table above a client will also be asked to confirm if he/she is a PIP as part of our normal process. The search must be done on all contract owners and related parties connected to a business relationship or transaction.

10.2. Clients qualifying for Enhanced CDD

Clients qualifying for Enhanced CDD (High Risk) clients pose a high to significant money laundering or terrorist financing risk to the company. Their risk rating stems from applying the risk rating methodology and risk matrices discussed in paragraph 9 above.

10.2.1. Enhanced Due Diligence Verification standard

The client will be required to provide at a minimum the following information as per the table below.

Natural Person	Legal Person
Full names	Full Name of Entity
ID Number/DOB	Registration Number
Residential/Physical Address	Current Physical Operating Address

Natural Person	Legal Person
Source of Funds/Wealth	Source of Funds/Wealth
Tax Number	Tax and VAT Numbers
Bank Details	Bank Details
Occupation and Industry	Industry
Countries of Affiliation (birth, nationality and residence)	Countries of Affiliation (registration and head office)
Mobile number/email address	Basic entity detail e.g. number of active Directors/Members/Trustees
PIP Status	DPIP status for each of the active Director/Member/Trustee/Founder of Trust/Trust beneficiary (Including Appointment & Resignation dates)
	Establish who may act on behalf of the entity
	Establish the Number of Managers
	Establish the Ultimate Beneficial Owner (UBO) of legal entity (Including shareholding %)
	Establish who is entitled to exercise 25% or more or the voting rights at general company meetings
	Obtain latest structure chart of entity

10.2.2. **Additional Requirements**

a) MC will follow a manual process of verification where a client will be required to provide copies of verification documents as per the CDD checklist;

b) Should any independent validation check done by the product provider highlight a discrepancy with the information provided to us by the client i.e. different address/full names/contact details etc. the product provider will be required to engage with the client to obtain further information to clarify the discrepancy;

c) The client will as a standard, be subject to a WorldCheck screening to determine their status with regards to UNSEC security lists and possible status as FPPO and DPIP. The search must be done on all contract owners and related parties connected to a business relationship or transaction;

d) Due to the high risk nature of the client, certain additional due diligence measures will need to be taken by the product provider; and

e) The business should not seek to de-risk by simply refusing to conduct business with high risk clients, but should apply their minds, on an on-going basis to the risk any one client

may pose to the business in the sphere of money laundering and terrorist financing, as well as reputational risk to the business and the group as a whole.

11. Compliance Monitoring

MC's compliance division conducts compliance monitoring in accordance with its annual monitoring plan which has been approved by Exco.

A monitoring exercise will typically include financial advisers' adherence to their obligations in terms of money laundering legislation and adherence to this policy. Identified compliance breaches are reported to the accountable manager and the breach is addressed with the financial adviser.

The financial adviser is provided with seven days to obtain the outstanding CDD verification documentation.

12. Establishing a Relationship with a Client

12.1. New Clients

MC cannot establish a business relationship with a client unless the following steps have been taken:

a) To establish and verify the identity of the client ("CDD");
b) If the client is acting on behalf of another person- establish and verify the identity of that other person along with the authority to act on their behalf. For example an estate late application; and
c) If another person is acting on behalf of the client- to establish and verify the identity of that other person along with the authority from the client to act on their behalf. For example a discretionary financial services provider, resolution appointing an authorised person to act on behalf of a company, trust etc.

12.1.1. Identification of Ultimate Beneficial Ownership

It is of paramount importance that the beneficial owner in respect of the legal person is identified.

Definition of 'beneficial owner' from the Glossary to the FATF Recommendations (24):-

Beneficial owner refers to the natural person(s) who ultimately owns or controls a client and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. To "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

AIs are to take reasonable measures in identifying the beneficial owner and measures to verify the identity of the beneficial owner, such that the AI is satisfied that it knows who the beneficial owner is.

For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the client.

Beneficial ownership is applied where the client is a legal entity, a corporate or trust arrangement.

An individual who ultimately owns or controls a client and/or the individual on whose behalf a transaction is conducted:

Direct and indirect ownership and/or control of specific percentage of shares or voting rights; or control over the management and their actions.

“Control” in this sense is to be distinguished from mere signature authority or legal title.

AIs need to:

a) Understand the substance and form of the legal person;
b) Understand the reason for the transaction and source of funds;
c) Identify individuals behind the institution, not only shareholding, but **control**; and
d) Ensure that individuals purporting to act on behalf of the entity are authorized to do so.

The lack of adequate, accurate and timely beneficial ownership information facilitates ML\TF by disguising:

a) The identity of known or suspected criminals;
b) The true purpose of an contract held by the legal entity; and
c) The source or use of funds or property associated with the legal entity.

Establishing the identity of the beneficial ownership helps to understand the client’s profile to properly assess the ML\TF risks associated with the business relationship, enables AIs to take appropriated steps to mitigate the risks and to collect and gather additional information about the beneficial owners to assist law enforcement efforts.

The standard Beneficial Owner Elimination process to determine who the natural person is who, independently or together with another person, has a controlling ownership interest in the legal person, will be as follows:

a) MC will consider 25 per cent or more of the shares with voting rights in a legal person as sufficient to exercise control of the legal person. The following will be used to determine the shares with voting rights: organogram, proof of shareholding; independent verification, CIPC etc.;
b) If the ownership interests do not indicate a beneficial owner, or if there is doubt as to whether the person with the controlling ownership interest is the beneficial owner, the AI must establish who the natural person is who exercises control of the legal person through other means, for example, persons exercising control through voting rights attaching to different classes of shares or through shareholders agreements; and
c) If no natural person can be identified who exercises control through other means, the accountable institution must determine who the natural person is who exercises control over the management of the legal person, including in the capacity of an executive officer, non-executive director, independent non-executive director, director or manager.

Once the AI has determined who the beneficial owner of a legal person is, the institution must take reasonable steps to verify that person's identity. MC will employ the requirements, as per the appropriate checklist to verify the details of the natural person. Once the relevant CDD documents have been received, MC will follow the third party validation process to verify the detail as correct and valid.

12.1.2. **Establishing the source of wealth/income of the client**

AIs are not required to verify the information about the client's source of income/wealth, but will have to include this information in its client profile which will be used as the basis for enhanced system based ongoing monitoring. A question will be asked on the forms and verbally. The CDD checklists have been enhanced as to obtain clarity of the source of funds.

When determining the source of wealth, an AI should look at the activities that have generated the total net worth of the client (that is, the activities that produced the client's funds and property).

When determining the source of funds, an AI should consider the origin and the means of transfer for funds that are involved in the transaction (for example, occupation, business activities, proceeds of sale, corporate dividends).

An AI must establish the source of wealth of a client that includes the nature of the client's business, occupation and source funds which the client intends to fund the contract.

MC will determine if/what the client's status is:

a) Is Employed (an employee);
b) Is Unemployed;
c) Is Self Employed (employer); and
d) Its core business activities and turn-over.

MC is required to reasonably establish the source of wealth/income and source of funds of a client as to satisfy MC of the reasonability of establishing a business relationship or single transaction relative to the source of funds/wealth. In this instance MC will only require supporting documentation showing the source of income and wealth if a client is a confirmed PEP/DPIP/FPPO/high risk client.

12.1.3. **Establishing and verifying the source of funds related to a transaction**

Identification of source of funds for specific transactions is required when an MC concludes the establishment of a business relationship with a client.

This process is required to enable MC to **establish the identity** of the **contribution/ premium payer** on a contract or on a specific transaction, e.g. an ad hoc incoming payment or a single premium investment and is based on the principle that from where/from whom the funds are received (bank account number/s and bank account holder/s) on all transactions is an imperative anti-money-laundering principle.

The identity of a premium payer/contributor needs to be established regardless of whether the case is exempt from other CDD requirements. In a case of an entity a simplified CDD will be required together with a resolution confirming who may act on behalf of the company.

Note: AI's are obligated to keep record of all bank accounts that are involved in transactions concluded by clients in the course of the business relationship and any single transaction during the full life span of a contract where financial transactions are processed. This includes accounts from where ad hoc/single payments are received and accounts to which withdrawals are paid.

12.1.4. **Process:**

Before a MC financial adviser may enter into a business relationship with a client, the financial adviser must verify the client's banking details by obtaining the required verification documentation as per the CDD checklist.

If the contribution/premium payer is different from the contract owner/holder MC must apply the full CDD process to the contribution payer as well. For example, if the policy holder is an individual, but the contribution/premium payer is a legal entity such as a trust or company, the necessary CDD process and documents required as per the specific checklist will also be required for the contribution payer

a) Identification of an Authorised Representatives of a legal person, trust or natural person

Each natural person that is authorised to transact on behalf of the legal entity must be identified and verified in accordance with the FICA KYC rules and MC's CDD checklists. In addition to the identification and verification requirement to identify each natural person so authorised by the legal person/ trust or natural person, proof of authority must also be obtained.

The legal person may provide the authority in the following manner:

- Power of attorney (in exceptional circumstances and to be approved by Compliance);
- Letter of Authority/ Letter of Executorship;
- Written mandate;
- Resolution duly executed by authorised signatories; and
- Court order authorising the third party to conduct business on behalf of another person.

b) Identification of a sanctioned person or entity in terms of UNSC resolutions

It is vital for an AI to screen its clients to enable an AI to determine whether these clients are sanctioned persons or entities.

MC will screen its clients by submitting client data on the (Office of Foreign Assets Control (OFAC) Sanctions List Search application: https://sanctionssearch.ofac.treas.gov/.

This Sanctions List Search application ("Sanctions List Search") is designed to facilitate the use of the Specially Designated Nationals and Blocked Persons list ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the List of Persons Identified as Blocked Solely Pursuant to E.O. 13599, the Non-SDN Iran Sanctions Act List, the Part 561 list, the Sectoral Sanctions Identifications List

and the Non-SDN Palestinian Legislative Council List. Given the number of lists that now reside in the Sanctions List Search tool, MC pays close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. Sanctions List Search has a slider-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. Sanctions List Search will detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating.

Due to the fact that the use of Sanctions List Search is not a substitute for undertaking appropriate due diligence, MC will use the application on a temporary basis only, until a solution is implemented whereby appropriate due diligence can be undertaken.

If a client and does not appear on any of the lists, MC will proceed with the on-boarding process but if a new client appears on a list, MC will not proceed with the on-boarding process.

MC is prohibited to continue the relationship with a sanctioned person/entity. Due to the nature of MC's business and its contractual relationships with various product providers, screening will not take place prior to entering into a relationship, but monthly on all existing clients.

If an existing client appears on a list, MC has an obligation to follow the Reporting on Property associated with Terrorist and Related activities and financial sanctions pursuant to Resolutions of the United Nations Security Council (Section 28A) process. The matter will also be escalated in accordance with MC's management process so that an exit process can be initiated.

MC may not:

- alert the client of the status as sanctioned person/entity;
- acquire, collect or use property of such persons/entity – strictly prohibited;
- transact or process transactions for sanctioned persons/entity; or
- render or provide any financial services to the person or entity – except in instance where Minister of Finance has permitted certain financial services or dealings with the property.

c) Identification of Domestic Prominent Influential Person and Foreign Prominent Public Officials

MC must establish if the client falls within this category of clients by screening them against World Check and various other compulsory lists identified by the FIC. The table below shows examples of individuals who are or have in the past been entrusted with prominent public functions in a particular country:

- Domestic Prominent Influential Person ("DPIP");

- Foreign Prominent Public Officials (“FPPO”); and
- Family members or Known Close Associates of DPIP & FPPO.

Domestic Prominent Influential Person (“DPIP”)	Foreign Prominent Public Officials (“FPPO”)	Family members or Known Close Associates of DPIP & FPPO
• President or deputy president. • Government minister or deputy minister. • Premier of a province. • Director-Generals and Chief Financial Officers of government departments. • Member of an executive council of provinces. • Executive mayors and municipal managers • Chief Executive Officers and Chief Financial Officers of state entities like Eskom, Telkom, PRASA, etc. • Judges. • Senior officials of companies that receive certain tenders from government. • A member of a royal family or senior traditional leader.	• Head of state or head of a country or government. • Member of a foreign royal family. • Government minister or equivalent senior politician. • Leader of a political party. • Senior judicial officer. • Senior executive of state-owned companies. • High ranking member of the military/police etc.	• Spouse or civil/life partner. • Previous spouse or civil/life partner. • Children and step children and their spouses or civil/life partners. • Parents. • Siblings and step siblings and their spouses or civil/life partners. • Prominent members of the same political party, civil organisation, labour or employee union as the prominent person. • Business partners or associates who share beneficial ownership of corporate vehicles with the prominent person, or who are otherwise connected e.g. through joint membership of a company board. • Known sexual partners outside the family unit (e.g. girlfriends, mistresses and boyfriends). • Any individual who has sole beneficial ownership of a corporate vehicle set up for the actual benefit of the prominent person

The above persons are often susceptible to corruption and bribery and in turn can use their position and influence to launder the proceeds from corrupt activities. Such persons may also use their families or close associates to conceal funds or assets that may have been misappropriated as a result of abuse of their official position or from bribery and corruption. In addition, these persons may also seek to use their influence to gain control of legal entities for similar purposes.

In terms of the FATF standards, and the FIC Amendment Act it is therefore noted that these persons should automatically be classified as a high-risk clients with an **exception of DPIP who must still be risk rated**. Once it has been established that a client or the beneficial owner of that client falls within one of the above categories MC will additionally be required to conduct enhanced due diligence measures on an annual basis.

An individual who holds or who is acting in a position **for a period exceeding 6 months** or has held the position **at any time in the preceding 12 months** in the Republic, are considered a domestic prominent influential person.

Before MC is able to enter into any business relationship with these persons the following **High Risk Client On-boarding measures** are to be implemented:

PEP/DPIP/FPPO/ High Risk Client On-Boarding Procedure: New clients		
Step	**Name**	**Description**
1	Client Identification	Identify the ultimate client and associated beneficial owner(s) (if not a natural person)
2	Reasonably Established PEP / DPIP / FPPO	If established a PEP/DPIP/FPPO, authorisation must be obtained from an accountable senior manager at the product provider before concluding a transaction or establishing a business relationship. The following precautionary procedures must be followed: • Clients PIP status must be captured and updated on a relevant database; • The domestic prominent official must be added to an enhanced ongoing monitoring list; and • The relevant ongoing monitoring activities must be implemented and managed
3	Enhanced Due Diligence	Once supporting documentation has been received, MC should be in a position to understand the objective and reasoning for entering into a business relationship with the client
4	Senior Management & Compliance Approval	PIP status will be indicated on the relevant application form and submitted to the product provider - if senior manager and compliance are comfortable with the level of risk involved, both parties will sign off
5	PEP/DPIP/FPPO Status	The PEP/DPIP/FPPO status will be captured and updated on a relevant database for ongoing monitoring purposes

In the event that an existing client is flagged on the monthly World Check screening as being one of the above mentioned persons and wasn't initially designated as being one

of them when the relationship was entered into, the General Manager will be responsible for on-boarding the respective person and requesting the necessary enhanced due diligence documentation.

d) Identification of a refugee/ asylum seeker

During the establishment of a relationship or during the course of the relationship, MC may rely on the permit issued under Section 22 & 24 of the Refugees Act as an alternative to identify the person should the client not be in possession of official identification documentation. This document will indicate the names of the refugee, date of birth, thumb print and a bar coded number (used for tracking). The refugee permit has an expiry date and we may not accept expired documents as proof of identity. There is no unique identification number on the permit.

However, the relevant product provider may set additional requirements to establish the validity of the permit.

Current process: This monitoring list is entrusted to the AML Operations Specialist within GFS who implements additional monitoring and analytics upon any movements on a contract or client, which has been identified as a PEP/PIP.

The preferred official identification documentation is as follows:

- Refugee identity document (only valid for two (2) years); and
- United Nations certified travel document.

e) Completion of the CDD Checklist

Based on the risk ratings, the financial advisers and On-boarding staff will be responsible for identifying and collecting all the necessary documentation.

12.1.5. **Complete Due Diligence**

Due to the nature of MC's business and the fact that it does not "own" the client, but merely act as intermediary to facilitate transactions between product providers and clients, MC will apply a standard CDD process on all clients.

The table below shows the minimum information to be collected and verified in respect of every natural and legal person for reporting purposes:

The client will as a standard, be subject to a **Sanctions List Search** to determine their status with regards to sanction lists.

Financial Advisers must obtain current, up to date verification documents from their clients **every two years.**

MC will apply Enhanced Due Diligence Verification standards on high risk clients.

Due to the high risk nature of the client, certain additional due diligence measures will need to be taken as follows:

- High risk clients will need to have their details reviewed and verification documentation updated **annually.**

a) Certification for EDD Purposes

CDD documentation will not need to be certified. MC will follow a manual process of verification where a client will be required to provide **copies of verification documents** as per the CDD checklist.

However, should there be any unforeseen need or regulatory requirement, documents will be dated and certified within the last three months by a regulated financial institution located in an equivalent jurisdiction like:

- an embassy;
- a consulate;
- a notary;
- an independent solicitor; and
- barrister /licensed lawyer.

Persons certifying the document(s) must provide the following:

- full name;
- an original signature;
- the date of certification;
- address and stamp of relevant authority/company as proof of authority; and
- statement confirming the following: **'I hereby certify that this is a true copy of the original'.**

b) Certification by MC Employees

MC employees who are commissioners of oath or are suitably qualified and who have sighted the client's original documents may certify copies of the originals.
The MC employee certifying the document(s) must provide the following:

- full names;
- employee number and designation;
- an original signature;
- the date of certification;
- address and stamp of relevant authority/company as proof of authority; and
- statement confirming the following: **'I hereby certify that this is a true copy of the original'.**

c) Clarity

The documents must be legible. The photograph of the copy of an identity document must be clear enough to distinguish the features of the client. This means that the following features must be clear:

- Eyes;
- Ears;

- Nose;
- Mouth; and
- Outline of chin.

d) Contents of the document

Identity documents to verify a Natural Person must have the following:

- Full names;
- Surname;
- ID number (13 digit and 10 digit);
- Date of birth;
- Nationality; and
- Last date of issue.

Passport:

- Full names;
- Surname;
- Gender;
- Birth date;
- Birth place (Town or country);
- Issue date;
- Expiry date;
- Issuing authority/Issuing country; and
- Passport number.

Birth certificates will only be acceptable for minors younger than 16 years.

Address documents must adhere to the following:

- Monthly issued document cannot be older than three months (current); and
- If a yearly issued document is used, it must not be older than a year.

The document must show the physical address or ERF number or portion number and township name. In the case of a letter, confirm that the township name matches that as stated in the application. Refer to **CDD checklist** for accepted proof of residential addresses.

MC advisers may, in exceptional circumstances only, where a client cannot provide verification of their physical address or where the client does not have any residential address verification documents in their own name, complete the declaration of financial adviser section on the CDD checklist, declaring that she/he has visited the client at their residential address.

e) Non Face to Face Clients

Accountable institution must take reasonable steps to confirm the existence of the client and to verify the identity of the natural person/s involved according to the risk associated with the client after applying their information to the MC risk matrix. There will be specific

and adequate measures in place to address the risk involved with non-face-to-face clients that are specific to the business risk framework.

Examples of enhanced customer due diligence procedures for Non-face-to-face Clients:

- Request of additional documentation that complements those required for face-to-face transactions;
- Utilising third party verification/E-verification processes;
- Where a third party vendor can verify the client's detail in respect of identification and verification of physical address, PEP/POI statuses; and
- Verification of bank account details preventing the use of unknown accounts etc.

There must be specific and adequate measures in place to address the higher risk involved with non- face-to-face clients that is specific to the business risk framework.

Examples of enhanced CDD measures include (but are not limited to):

- Obtaining additional information on the client;
- Obtaining additional information on the intended nature of the business relationship, and on the reasons for intended or performed transactions;
- Obtaining information on the source of funds or source of wealth of the customer; and
- Conducting enhanced monitoring of the business relationship, potentially by increasing the number and timing of controls applied, and identifying patterns of transactions that warrant additional scrutiny.

Scanned and emailed copies of documents may be relevant in instances when client information is obtained in a non-face-to-face situation. In such cases, where enhanced customer due diligence procedure could apply, it implies that documents that are certified as true copies of originals may be accepted, but MC would have to take additional steps to confirm that the said documents are in fact those of the client in question.

An independent verification check performed by a credible vendor to confirm the client's particulars as mentioned above would be deemed as an acceptable form of verification.

f) Face-to-face Verification

In cases when client information is received in a face-to-face situation, the relevant documents will be sighted as part of the verification process. The said MC financial adviser that sighted the client's original documents would then take a copy of the originals and where necessary certify them as per paragraph (e) above.

g) Secondary means of verification if client's identity document has been lost or stolen

Cases in which a person is unable to produce an official identity document - an official identity document refers to the following:

For South African citizens:

- A Client's green South African bar coded ID document;
- South African Smart Card ID (both sides to be provided);
- Valid South African passport;
- Valid South African driver's license;
- For Foreign Nationals;
- United Nations certified travel document/passport;
- Refugee document (valid for 2 years only);
- Valid passport; and
- Valid travel document.

(No temporary identity documents will be accepted).

12.2. **Existing Clients**

Reviews of existing records by financial advisers will take place every two years and in accordance with section 21 C of the FIC Act to ensure that MC has up- to date information about its clients.

Continuous due diligence and account monitoring

The requirement includes the scrutiny of transactions undertaken throughout the course of a relationship, to ensure that the transactions being conducted are consistent with the financial adviser's knowledge of the customer, and the customer's business and risk profile, including, the source of funds.

It further requires MC to ensure that the information that it has about a client is still accurate and relevant.

Financial Advisers will review the client's information when any change (trigger event at appropriate intervals) is made to a client's status which includes but not limited to the following:

a) A request to change the bank details;
b) Change of premium payer/contribution payer;
c) Third party payments;
d) Fund withdrawal requests received;
e) Cancellation of contract where CDD has not previously been implemented;
f) Changes to residential address;
g) Specific contract alteration requests e.g. increase in premiums;
h) Ad hoc/Voluntary payments received;
i) Changes in contract ownership;
j) Transfer of ownership;
k) Add/change beneficiary of ownership;
l) Cessions;
m) Cool-of;
n) Refund;
o) Sec 14/37 transfers;
p) Unit transfers (Wealth);
q) Commutations;
r) Tax information changes ;
s) Additional investments;

t) Change in client personal information; and

u) Alterations such as:

- regular contribution changes (excluding CPI/% growth changes);
- switching (depending on product);
- change / add product;
- Death claim; and
- Change beneficiary (but only to determine possible PEP/POI relationship as full CDD will apply on beneficiary once the benefit transfers to them).

It is important to note that the financial adviser may not be aware of the above in the event where the client deals directly with the relevant product provider. MC Financial Advisers must therefore take reasonable steps to ensure that the information which they have for their clients are valid and current.

If none of the above listed trigger events occur, or MC is unaware of the occurrence of the particular trigger event MC will review client's details **every two years** as stipulated above.

The below procedure will have to be performed in the event of clients qualifying for Enhanced CDD (High Risk). An annual EDD process is tabled below.

Annual Enhanced Due Diligence Procedure: For Existing DPIP/FPPO/ Clients qualifying for Enhanced CDD (High Risk)		
Step	**Name**	**Description**
1	Senior Management & Compliance signoff	Relationship Manager/accountable representative should follow an annual review process for DPIP / FPPOs / clients qualifying for Enhanced CDD and to get a Senior Management and Compliance approval and sign off. The review process is to be followed for all existing DPIP/FPPOs/ clients qualifying for Enhanced CDD on an annual basis;
2	Review of documentation	FDM/accountable representative to request enhanced due diligence to determine if collected information is consistent with the information currently on record for the DPIP/FPPOs / clients qualifying for Enhanced CDD and
3	Monitoring of Activities	Monitoring of activities to ensure consistency with documentation on record and profile of DPIP/FPPOs / High Risk Clients. If any transaction appears suspicious, to report to MC's Money Laundering Reporting Officer.

The below diagram shows **MC's ongoing monitoring process** driven by the above trigger events at appropriate intervals:

a) A trigger event will happen and client will be taken through the process of risk rating since client's circumstances could have changed over time;

b) The risk matrix tool will then provide the client's new risk rating;

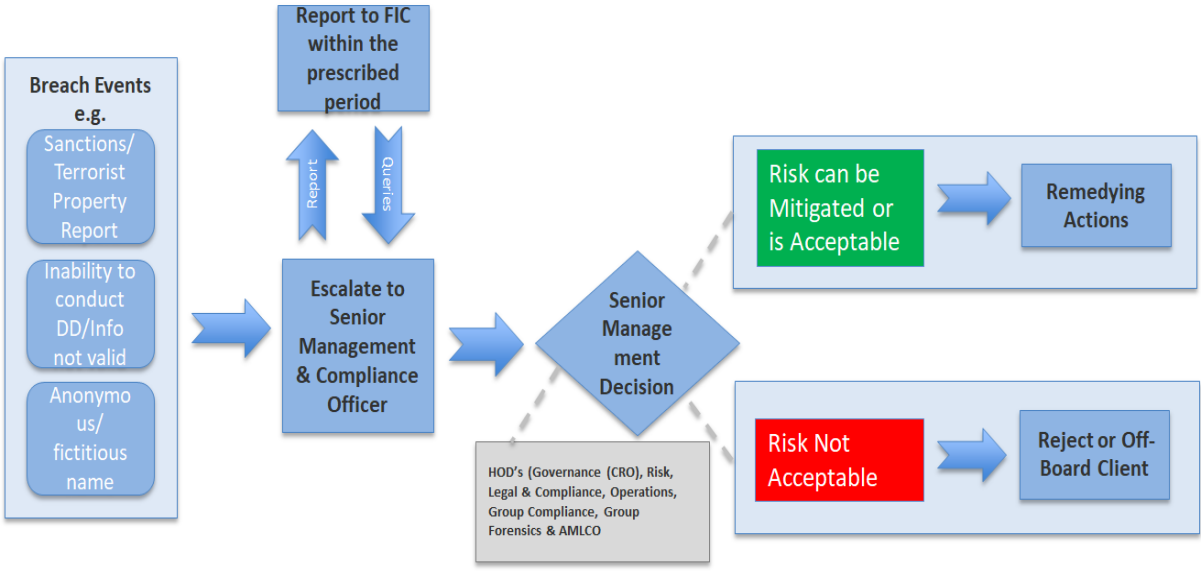
c) If the client's risk rating did not change MC will continue to process the trigger event;

d) If the client's risk rating has increased i.e. from medium risk rating to high risk rating, the client will be requested to provide additional documentation necessary to conduct EDD as per CDD checklist;

e) If the additional documentation is acceptable, MC will proceed with processing the trigger event; and

f) If the additional documentation received is unacceptable to perform EDD, the matter will be escalated to senior management through a breach management process for further consideration.

The below diagram shows **MC's Breach Management Process**:



12.3. Prohibited Business Relationships

MC must refuse to enter into a relationship or refuse to terminate a relationship, if MC cannot form a reasonable belief that it knows the true identity of the client and/or the ultimate beneficial owner and/ or the nature of any underlying business.

In particular, MC is prohibited from entering into/ maintain business relationships with individuals or entities known or suspected to be terrorist or a criminal organisation or member of such or listed on any sanction lists;

A detailed step by step process for new clients take on process is documented **on Annexure B.**

12.4. MC Sources of business

It must be noted that MC sources clients via its financial advisers.

MC (MC) is registered as an authorised FSP in terms of the FAIS Act and an Accountable Institution in terms of FICA. MC financial advisers are representatives of MC (Pty) Ltd, under FSP5503. MC contracts with financial advisers via a franchise house /financial adviser agreement. As required in terms of FAIS, MC financial advisers have professional indemnity insurance in place.

A proper due diligence process is undertaken by the Operations Department and Agreements Department respectively when financial advisers are on boarded before issuing broker codes. The financial advisers are also monitored on an on-going basis. If there are any persistent or

unresolved non-compliance issues which may result in a code being suspended and/or subsequently blocked. Furthermore a suspicious transaction/activity will be logged with the FIC through the relevant reporting officer. A take on process for advisers is attached hereto marked as **Annexure C.**

13. Record Keeping

Record keeping is an essential and required process which successfully enables AI's to combat money laundering and terror financing. The records of client identities and transaction activities are of paramount importance as these records can be used as documentary evidence which can assists law enforcement authorities in the detection, investigation, prosecution and the repossession of criminal funds where illegal flow of funds is concerned.

IMPORTANT NOTE: Exemption 4: Previously an AI could rely on a certificate issued in terms of the regulations to FICA, i.e. Exemption 4, which allowed a secondary AI to reasonably rely on a principal AI to the effect that the necessary CDD process was executed and that the relevant Identification and verification documentation was held by the principal AI. This regulation has been revoked and MMC will no longer accept or rely on such certificates. In this regard all interaction with clients, whether directly or through a person acting on behalf of a client would require that the MMC AI obtain all relevant CDD documentation. Therefore in those cases where a MMC AI does not have CCD information and documentation on record, a full CDD process will be required for all investment instructions, new business, ad hoc investments etc.

13.1. Duty to Keep Records

The duty to keep records arises whenever we establish a business relationship or conclude a single transaction with such a client. FICA requires MC to keep records of the following:

a) Copies of proof of identification documentation;
b) Copies of proof of residential documentation;
c) Copies proof of source of funding .e.g. bank statement;
d) Documentation which prove nature of business relationship or occupation; and
e) Verification document and any other information collected about the client e.g. all information linked to a transaction e.g. dates, values, parties involved, bank accounts etc.

13.2. Period for which records must be kept

An AI has an obligation to retain records for the following period:

a) Records relating to establishment of the business relationship must be kept for at least five years from date of termination of business relationship;
b) Records relating to all transaction must be kept for at least five years from the date which the transaction was concluded;
c) Records relating to a transaction or activity which gave rise to reporting a suspicious activity or transaction to FIC must be retained for at least five years from the date which an suspicious activity or transaction was reported to the FIC;
d) Records which an AI have in their possession which is connected to an ongoing investigation must be kept until such time that relevant law enforcement authority has confirmed that the case has been closed; and
e) Records not being used for the intention for which it was collected must be immediately destroyed.

No person may delete or destroy any record pertaining to a client in respect of their identity or verification of identity or in respect of the relationship unless written authorisation has been obtained from Momentum Metropolitan Group Forensic Services.

13.3. Records may be kept by way of storing original documents or copies of original documents, scanned versions of originals in electronic format in an effort to reduce the density of such records and may be kept in:

a) Internal networks;
b) Physical storage devices;
c) Cloud storage;
d) Fintech capabilities;
e) Electronic document repository; and
f) The records must be stored in a safe and secure location which is tamper free.

13.4. MC must keep a record of all documentation relating to a client in the following manner:

13.4.1. Electronic and hard-copy storage

a) All documents are scanned onto MC's Financial Planning system (Elite Wealth); and
b) MC may make use of a commercial third party who provides storage services for hard-copy documentation, provided that MC has free access to the files, or MC financial advisers may store all original documents in their offices, provided that such documents are kept safe from destruction and unauthorised access. All documents must be backed-up on Elite Wealth.

13.4.2. Electronic storage

a) All documents are scanned onto Elite Wealth;
b) Electronically retained records can be reproduced in a legible format. These electronic records are secured by unique User IDs, passwords etc.;
c) The AI must inform clients of its intention to retain the client's records with a specific third party and must seek the clients consent in sharing their personal information with this third party; and
d) AI must safeguard and ensure that there are controls in place such as firewalls that will safeguard against anyone tampering with the electronic data. Other preventative measures are as follows, user logs, network logs, password controlled access, levels of authority etc.

13.5. Regardless of the manner in which records are kept, MC must ensure that the following principles are met:

a) It has easy free access to the records and will have the records readily available to the FIC and relevant supervisory body as and when it's needed;
b) The liability remains with MC should the third party fail to comply with the provisions of this Act;
c) MC provides the FIC and supervisory bodies with the full particulars of the third party;
d) Electronically retained records can be reproduced in a legible format;

e) MC will inform clients of its intention to retain the client's records with a specific third party and will seek the clients consent in sharing their personal information with this third party; and

f) MC will safeguard and ensure that there are controls in place such as firewalls that will safeguard against anyone tampering with the electronic data.

13.6. MC will store the records in a detailed manner which will enable easy identification of such records.

These records will be stored in the following manner:

a) The client's identity number;
b) The reference number on the policy or the contract number;
c) The reference number of the business correspondence;
d) Relevant dates of issuing or expiring; and
e) Details of the issuer or writer, etc.

13.7. MC will take reasonable steps to maintain the correctness of particulars of clients, which are susceptible to change.

13.8. Based on the risk based approach it is recommended that MC should verify particulars of clients, at any stage when MC interacts with the client.

13.9. MC will ensure that records are tamper proof and that there are safeguards in place to prevent the unauthorised access to information stored electronically through electronic alerts via KRIS.

13.10. MC as part of Momentum Metropolitan Holdings will implement group-wide policies on record-keeping which may include centralised storage of records.

13.11. If MC make use of commercial third party services, or intra-group centralised data storage to retain their records to conduct regular assessments of its service providers and to test the controls and business processes so as to provide assurance to the relevant supervisory body that the accountable institution can access and retrieve data and/or documents as envisaged under the FIC Act.

IMPORTANT NOTE: MC remains responsible for compliance with its obligations in terms of the FIC Act regardless of their internal arrangements relating to the manner in which those obligations are met.

MC may rely on the services of a third party or the relevant product provider to perform activities relating to the establishing, verifying and validation of clients' CDD documents to establish and verify the identity of their clients, and for record-keeping purposes as required in terms of the FIC Act and the Regulations to the FIC Act. However, MC remains liable for compliance failures associated with and/or caused by such arrangement.

14. Reporting Obligations and FIC Interventions

The registration and deregistration of accountable and reportable institutions according to schedule 1, 2 and 3 of FICA is intra-group centralized to Momentum Metropolitan Group

Forensics Service (GFS). As part of a complex structure MC's reporting to the FIC is also centralised to Momentum Metropolitan GFS.

Each respective AI is responsible for the identification, investigation and upon confirmation of a suspicion in a case of suspicious transaction.

14.1. Inability to conduct customer due diligence (Section 21E)

MC must consider submitting a section 29 report to the FIC should they be unable to-

a) Establish and verify the identity of the client and other relevant persons, in terms of their RMCP;
b) Obtain information about the business relationship with the client in terms of their RMCP; and
c) Conduct on going due diligence on the client in terms of its RMCP.

14.2. Accountable Institutions, Reporting Institutions and persons subject to obligations to advise the FIC of client related detail (Section 27).

Natural and Juristic clients

a) Upon receipt of a Section 27 request from the FIC, via the FIC's go-AML system, that contains the information for the individuals/companies that the enquiry relates to;
b) The MLRO will request the Momentum Metropolitan Business Intelligence unit to trace any matches or potential matches to existing MC clients;
c) A template is populated with the information as received from the FIC;
   - Name and Surname;
   - ID;
   - Registration number; and
   - Date of Birth.
d) This information is then submitted as part of an automated process to look for matches across various platforms within Momentum Metropolitan.

The results are interrogated as follows:

Natural client:

a) ID number matches are obtained from the ID number match list; and
b) Name matches
   - If an ID number was recorded on the line of business system, but it does not match the FIC ID number then discard the record;
   - If a date of birth was recorded on the line of business system, but it does not match the FIC date of birth then discard the record;
   - If the date of birth is the same as the FIC date of birth or no date of birth was obtained from the line of business system, then do a name match; and
   - For name matches there must be a high probability for the name match, i.e. exact or near exact name match (first/second name and surname).

Juristic client:

a) Company registration number matches are obtained from the company registration number match list; and
b) Name matches-
   - If an a valid company registration number was recorded on the line of business system, but it does not match the FIC company registration number then discard the record;
   - Where the company registration number was not returned from the line of business system, or it is a default value e.g. 1111/111111/11, then name matches are done; and
   - There must be a high probability for the name match, i.e. exact or near exact name match.

Bank accounts:

a) Bank account numbers are not yet part of the existing automated process, but queries are processed on an ad-hoc basis; and
b) The account number provided by the FIC is "run" against the Momentum Metropolitan financial systems (FACS) to establish if Momentum Metropolitan has every used such an account number, for any type of transaction or reason.

Once the interrogation process has been finalized, the MLRO compiles a feedback report to the FIC and submits the report via the FIC go-AML system. The MLRO also stores hardcopies of all reports submitted in files for a minimum or 5 years.

14.3. Reporting on Property associated with Terrorist and Related activities and financial sanctions pursuant to Resolutions of the United Nations Security Council (Section 28A).

MC is a financial services provider and does not hold and can therefore not be in possession or have under its control property owned or controlled by or on behalf of, or at the direction of report:

a) Any entity which has committed, or attempted to commit, or facilitated the commission of the financing of terrorism or related activities;
b) A specific entity identified with in a notice by the President; and
c) A sanctioned person or entity identified on the UNSC sanctions list.

The MLRO will implement various checks in an attempt to establish the true identity of the client:

Check: Client's complete portfolio for irregularities, e.g.-

a) Changing/updating of personal information often, especially bank account details;
b) Unexplained ad-hocs & withdrawals, if known to MC;
c) Attempts for 3rd party payments, if known to MC; and
d) Incomplete KYC/CDD documents etc. stored on Elite Wealth.

Check: Electronic Systems and Media

a) TransUnion: ITC details (Full names/Address/Contact details/Occupation etc.);
b) Experian: ITC details ((Full names/Address/Contact details/Occupation etc.);
c) Google: Fraud/corruption & general search;

d) World Check: Searches for clients on https://sanctionssearch.ofac.treas.gov/. If the client is in any way high risk/politically exposed their information will come up on this search and details will be provided regarding why they are high risk/politically exposed; and
e) Windeed: Provides details of companies that the client is/was a member of.

Once the MLRO has finalised the investigation and has managed to reach a conclusion, the MLRO, will be in a position to provide comments on KR1S and make an educated decision in determining if the client is a terrorist or assisting in terrorist funding.

If the client or entity has been identified as a terrorist or is assisting in terrorist funding, the MLRO is to immediately freeze all assets in the name of the client and immediately inform the FIC of the client's status.

Business must be informed that NO withdrawals are permitted from any contracts in the name of the client.

A warning message will be placed on system informing business that NO withdrawals are permitted without referring the contract to the MLRO.

The MLRO keeps record of all cases which are reported to the FIC. These contracts are to be monitored monthly, to ensure that no unauthorised payments are processed.

14.4. DPIP/FPPO

The application form will include fields where a client can declare if he/she is a DPIP or a FPPO. The electronic verification to determine if a client is DPIP or a FPPO would be over and above the client declaration.

14.4.1. DPIP/FPPO Business Rule Principles

Natural party

Natural party <u>has</u> provided an RSA ID number:

Search criteria A:

a) 85 % full name (full name = first name, second name + surname) plus 100% date of birth and World check country = South Africa;
b) 85 % full name (full name = first name, second name + surname) plus 100% Year of birth and World check country = South Africa. Date of birth populated as 1962/00/00;
c) No date of birth or year of birth populated on World check. Derive a year of birth by using the variable "WORLDCHECK AGE DATE (AS OF DATE)" and "World check age". Allow for a difference of 1 year either side. (-1,0,1) and World check country = South Africa; and
d) Included in the above criteria is the match against the gender of the client and the gender as defined on WorldCheck.

Natural party <u>has not</u> provided a RSA ID e.g. Passport number:

Search criteria B:

a) 85 % full name (full name = first name, second name + surname) plus 100% date of birth and World check country = All countries;
b) 85 % full name (full name = first name, second name + surname) plus 100% Year of birth and WorldCheck country = All countries. Date of birth populated as 1962/00/00;
c) No date of birth or year of birth populated on World check. Derive a year of birth by using the variable “WORLDCHECK AGE DATE (AS OF DATE)” and “ WorldCheck age”. Allow for a difference of 1 year either side. (-1,0,1) and World check country = All countries; and
d) Included in the above is the match against the gender of the client and the gender as defined on WorldCheck.

Overarching principles

a) Once a PEP / PIP always a PEP / PIP /POI;
b) If any one of the directors or members of a Juristic is a PEP then the Juristic will be classified as a PEP / PIP; and
c) The results of the individual directors / members of the juristic must be linked to the Juristic, meaning the Juristic = no match, but for individual members a match could be found.

Outcome from the World check search

a) No match found - no rows returned. The business process may continue on the “happy path”;
b) One or many rows returned – These transactions must follow an “unhappy path” to enable further investigation;
c) A KR1S front end application will be provided to enable business to extract the relevant data from the WorldCheck data base; and
d) Business must arrange access to TransUnion ITC data base or the like to enable further investigations.

United Nations Sanctions List

The sanctions matched criteria will include the same logic as per the Pep / Pip /Poi conditions listed above.

Outcome from the Sanction list search:

a) No match found - no rows returned. Business process to continue on the “happy Path”;
b) One or many rows returned – The business process is to be routed to the GFS AML team who would investigate further;
c) GFS investigates, updates the CDD data base with the positive or negative result and reroute the transaction to line of business;
d) A positive result will be blocked on CDD and only GFS and selected parties will have access to this data; and
e) The positive match on the Sanctions list could result in the “Freeze” of the contract or decline of the new business application.

14.5. Reporting of Suspicious and Unusual transactions: STRs (Section 29)

The FIC Act applies to any person who carries on a business, is in charge of a business, manages a business or is employed by a business.

Any person associated with MC as the owner, a manager or employee of MC, is subject to the obligation to report suspicious or unusual transactions and activities to the Centre:-

The obligation to report in terms of section 29 of the FIC Act arises when a person knows of certain facts, or in circumstances in which a person ought reasonably to have known or suspected that certain facts exist. This means that a person associated with a business, as described above, must report his or her knowledge or suspicion to the Centre whenever:

a) he or she becomes aware of something; or
b) circumstances arise in which a person can reasonably be expected to be aware of something; or
c) circumstances arise in which a person can reasonably be expected to suspect something.

Section 29(1) of the FIC Act describes the "something" referred to above. This can relate to situations concerning the business itself; or concerning transactions or potential transactions to which the business is a party; or concerning an activity which may lead to the business being abused by money launderers.

The "something" also relates to:

a) the proceeds of unlawful activity;
b) unlawful activity;
c) facilitating the transfer of proceeds of unlawful activity;
d) has no apparent business or lawful purpose;
e) may be relevant to the investigation of an evasion or attempted evasion of a duty to pay tax evasion or attempted tax evasion;
f) an offence relating to the financing of terrorist and related activities;
g) the contravention of a prohibition under section 26B of the FIC Act; and / or
h) any structuring of a transaction or activity which is conducted for the purpose of avoiding giving rise to a reporting duty under the FIC Act;

It is important to note that section 29 of the FIC Act refers to reports being made in connection with suspicions concerning the proceeds of unlawful activities and money laundering, terrorist financing, and financial sanctions offences as opposed to criminal activity in general. The FIC Act therefore does not require reports to be made on suspected crimes or unlawful conduct by a person (apart from money laundering, terror financing and financial sanction activities).

Examples of deemed Suspicious Transaction:-

a) New business or existing business relationship, where the proper identification of client/s cannot be established or information related to the identification and verification process is suspicious;
b) Where a staff member dealing with a transaction actually knows, or believes that there is a reasonable possibility that the client's/clients' name/s is/are false;
c) Where the client transfers ownership or cedes a contract to a party outside the borders of the RSA, or to a non-resident, or to a non-citizen;

d) Application for a policy from a potential client in a distant place where a comparable contract could be provided “closer to home”;
e) Application for business outside the policyholder’s normal pattern of business;
f) Any transaction or suspicious transaction that involves an undisclosed party;
g) Early termination of a product, especially at a loss caused by front-end loading of costs, or where cash was tendered and/or the refund is to a third party;
h) The transfer of the benefit of a product to an apparently unrelated third party (e.g. outright cessions);
i) Requests for a large purchase of a lump-sum contract where the policyholder’s history shows small, regular payment contracts;
j) Attempts to use third-party funding to purchase a policy;
k) The applicant shows no concern for the performance of the policy but much concern for the early cancellation of the contract;
l) The applicant attempts to use cash to complete a proposed transaction when other payment instruments would normally be used in this type of business transaction;
m) The applicant requests to make a lump-sum payment by a wire transfer or in foreign currency;
n) The applicant appears to have policies with several institutions; and
o) The applicant purchases policies in amounts considered beyond the client’s apparent.

A person who files a report in terms of section 29 of the FIC Act, should evaluate matters concerning both the reporter’s internal business and the business of the client, or potential client in question and the transactions involving the business, in relation to what seems appropriate and is within normal practices in the particular line of business of that person or entity type, and bring to bear on these factors such as the knowledge the reporter may have of the client. This should involve an application of the person’s knowledge of the customer’s business, financial history, background and behaviour.

A particular category of transactions that are reportable under section 29(1) of the FIC Act are transactions which a person knows or suspects to have no apparent business or lawful purpose. This refers to situations where customers enter into transactions that appear unusual in a business context or where it is not clear that the purpose of the transaction(s) is lawful. In order to identify situations where customers wish to engage in these unusual transactions a person would have to have some background information as to the purpose of a transaction and evaluate this against several factors such as the size and complexity of the transaction as well as the person’s knowledge of the customer’s business, financial history, background and behaviour.

Process:

Once a suspicious transaction has been identified, the staff member must complete an Anti-Money Laundering Report (see STR template below).

a) This report must be presented to the MLCO of their Business Unit;
b) The facts must be discussed and the matter reviewed;
c) Where appropriate, additional information must be provided relating to the client or transaction if it is relevant to the matter under consideration;
d) If a staff member suspects the Head of the Business Unit, to be involved with the suspicious activity under consideration, the MLCO should be contacted immediately;
e) Suspicions must not be discussed with anyone other than direct management, the Business Unit MLCO and the Momentum Metropolitan Group MLCO. It is of vital

importance, regardless of whether the suspicions are proven true or not, that no mention of these suspicions be made to the client;

f) Any discussion of this nature would risk a tipping-off offence;
g) Staff should at all times neither confirm nor deny the existence of a report to the client or to a third party;
h) Any correspondence that could indicate the existence of a report should not be placed in the client's file;
i) Once the report has been finalised, it must be presented to the Momentum Metropolitan Group MLRO, who in turn will acknowledge its receipt in writing or ratification;
j) The staff member will then receive guidance from the MLRO on how to proceed with the client in question;
k) In particular, if the client demands that subsequent transactions be executed, the situation must be discussed with the Momentum Metropolitan Group MLRO before any action is taken;
l) In certain cases, the Momentum Metropolitan MLCO may decide to allow transactions to continue in order not to raise the client's suspicions. Regardless, the Momentum Metropolitan Group MLCO should be kept informed of all subsequent dealings with the client;
m) The process is handled exclusively by the Momentum Metropolitan Group MLCO;
n) The Momentum Metropolitan Group MLCO must judge, based on the staff member's report and all available information (including additional enquiries), whether or not the transaction has remained suspicious;
o) If the Momentum Metropolitan Group MLCO judges that the transaction has remained suspicious, the MLRO will make an official report to the FIC via the go-AML system;
p) All reports made to the FIC must be stored manually and electronically by the MMC Group MLRO;
q) The initiating staff member will receive an acknowledgment of the receipt of report, from the Group MLRO confirming that their personal legal obligations in terms of this policy have been met;
r) Once the report has been submitted, the FIC will respond to the submitted report by issuing an "Approval or Rejection" report;
s) If the report is approved, the Approval report must be stored electronically and manually;
t) If the report was rejected, the MLRO must investigate the reason for the failure and correct the report within 48 hours (2 business days) before re-submitting the report for approval;
u) The MLRO must store all responses received on CTR submitted as hardcopies and electronically; and
v) The MLRO only has 14 business days to ensure that all reports are downloaded and stored, before the FIC moves the response to an archived status, after which the report can no longer be accessed or downloaded.

The MLRO must store all reports submitted and responses received from the FIC for a minimum or 5 STR Reporting Template

Details of client being reported:

a) Full name;
b) Address (registered if required);
c) Postal: Physical;
d) Telephone numbers (as appropriate);
e) Home;

f) Work;
g) Cell;
h) Email;
i) Identity /passport / company registration No;
j) Income Tax Number;
k) Name of organization client represents or works for;
l) Capacity;
m) Bank account details (If applicable);
n) Nature of Suspicion;
o) Reasons for Suspicion;
p) Manager Referred To;
q) Name;
r) Position;
s) Contact details;
t) Manager's Comments;
u) Attach any copy of supporting documentation to this report, including-
- Name of Staff Member making this Report;
- Contact details;
- Date handed to MLRO and
- Signature.

Provide clear and concise information.

Who? –the subject, its associates and relationships

What? –the transaction or activity

When? –date of detection, date of occurrence, span of time

Where? –location of the client and where the transaction occurred

How? –describe how the activity/transaction was completed or attempted

Why? –results of your investigation into why the activity/transaction is reported/suspicious

14.6. Reporting on the transfer of money to and from the Republic of South Africa (Section 31)

MC does not deal with clients' funds and will therefore not transfer funds to and from the Republic.

14.7. Reporting procedures and furnishing of additional information (Section 32)

Requests for information in terms of section 32 of the FIC Act provide the FIC with a mechanism to obtain additional information concerning a report submitted by an AI, including the grounds for the report.

Process

a) An AI receives a Section 32 request on the go-AML Message Board in the name of the AI. It may also be addressed to an AI in different manners and it is therefore imperative

that employees are aware of their responsibilities in terms of the Momentum Metropolitan Dawn Raid Policy;

Dawn+Raid+Guidanc e+Note.pdf

b) The MLCO/MLRO must without delay provide the requested detail and documents to the FIC by submitting an Additional Information File (AIF) or an Additional Information File Transaction Report (AIFT) report;
c) All information must be provided as per the Section 32 request within the given time frame;
d) All AIF/AIFT reports submitted to the FIC must be stored manually and electronically;
e) This includes the Rejection/Accepted reports received from the FIC, after a report has been submitted;
f) All requests received from the FIC contains a reference code, this is the only reference code which must be used when providing feedback to the FIC on a specific request; and
g) All Rejected reports must be corrected and resubmitted, within 48 hours of been rejected, until the report has been accepted.

14.8. Intervention by the Centre (Section 34)

The FIC may direct the **AI, reporting institution or person in writing not to proceed with a specific action as detailed in the Section 34 request.** This can include, but is not limited to the carrying out of a specified transaction or proposed transaction for a period not longer than 10 days. For the purposes of calculating the period of 10 days, Saturdays, Sundays and proclaimed public holidays are excluded.

This intervention enables the FIC to make the necessary inquiries concerning the transaction and if the Centre considers it appropriate, to inform and advise an investigating authority or the National Director of Public Prosecutions regarding the transaction.

Process

a) An AI will receive a Section 34 request, on the go-AML Message Board, in the name of the AI. It may also be addressed to an AI in different manners and it is therefore imperative that employees are aware of their responsibilities in terms of the Momentum Metropolitan Dawn Raid Policy.

Dawn+Raid+Guidanc e+Note.pdf

b) The MLCO/MLRO must without delay act upon the instruction received from the FIC
c) An alert needs to be placed on the said transaction/client/contract/entity;
d) Line of business must be informed of the Section 34 request received on a transaction/client/entity/contract/policy;
e) Line of business must provide ongoing monitoring of the transaction/client/contract entity to ensure that no unauthorised movements are processed;
f) The MLCO/MLRO must report any additional relevant information with regards to any change in client behaviour or any further information received or established;

g) Once the said 10 days have expired, without further instruction from the FIC, it is suggested that the MLCO/MLRO enquire further instruction from the FIC, via the AI's go-AML Message Board, to ensure that no unauthorized transactions are processed;
h) All requests received from the FIC contains a reference code, this is the only reference code which must be used when providing feedback to the FIC on a specific request; and
i) All communication and reports submitted to the FIC must be stored manually and electronically.

14.9. Monitoring Orders (Section 35)

Section 35 of the FIC Act is only applicable to AI's and relates to **monitoring orders granted by a judge** designated by the Minister of Justice for the purposes of the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992).

Process

a) An AI will receive a Section 35 request, on the go-AML Message Board, in the name of the AI;
b) Employees must on receipt of the request from the FIC refer the request to the AML Compliance Officer before the end of that business day. The request may also be addressed to an AI in different manners and it is therefore imperative that employees are aware of their responsibilities in terms of the Momentum Metropolitan Dawn Raid Policy;

Dawn+Raid+Guidanc
e+Note.pdf

c) The MLCO/MLRO must without delay act upon the instruction/s received from the FIC;
d) An alert needs to be placed on the said transaction/client/contract/entity;
e) Line of business must be informed of the Section 35 request received on a transaction/client/entity/contract/policy;
f) Line of business must provide ongoing monitoring of the transaction/client/contract entity to ensure that no unauthorised movements are processed;
g) The MLCO/MLRO must report any additional relevant information with regards to any change in client behaviour or any further information received or established;
h) Monitoring and reporting of the transaction/client/contract entity needs to be adhered to as per the prescriptions of the Section 35 request, weekly, monthly etc.;
i) The MLCO/MLRO must report the requested information as per the instruction received;
j) This can be done by means of Word or Excel documents which can be attached to the Additional Information File (AIF) or an Additional Information File Transaction Report (AIFT) report;
k) All requests received from the FIC contains a reference code, this is the only reference code which must be used when providing feedback to the FIC on a specific request; and
l) All communication and reports submitted to the FIC must be stored manually and electronically.

14.10. Power of access by authorised representatives to records in respect of reports required to be submitted to the FIC

The FIC may request information from an AI or-

a) A specified person or entity is or has been a client of an AI or person;

b) A specified person acting or has acted on behalf of any client of an AI or person;
c) A client of an AI or person is acting or has acted for a specified person;
d) A reference number etc. specified by the FIC was allocated by an AI to a person with whom an AI has had a business relationship; and
e) The type and status of a business relationship with a client of an AI.

Process

a) If a person claiming to be a representative of the FIC insists on access to any records held by MC, MC staff must refer the request for information to the MC Compliance Officer or the Momentum Metropolitan Group Anti-Money Laundering Compliance Officer (MLCO) for further attention. The request may also be addressed to an AI in different manners and it is therefore imperative that employees are aware of their responsibilities in terms of the Momentum Metropolitan Dawn Raid Policy;

Dawn+Raid+Guidanc e+Note.pdf

b) If the FIC should ask an AI for access to AI's records, they must never inform any other person of this request or of the nature of the records sought by the FIC, except to inform the MLCO. (If an employee does it may be regarded as 'tipping off' which is a criminal offence);
c) The MLCO will ensure that the representative from the FIC has written authority to represent the FIC and a warrant to gain access to the records;
d) In the event that a printout of the electronic records of MC is made and provided to a representative of the FIC (or the police), the MLCO will certify that the printout is an extract copy of MC's electronic records; and
e) The MLCO will keep a record of all requests for information from the FIC, manually and electronically.

14.11. Confidential information

All staff must satisfy any legal obligation to report knowledge or suspicions relating to the proceeds of unlawful activities or money laundering i.e. in the required format and within the time frames required. Where a suspicious activity report has been filed or otherwise reported to the MCLO and MLRO, staff must not notify any person of any matters relating thereto i.e. besides the MLCO and MLRO or specifically authorised MC officials. All reports submitted remain confidential and each staff member is protected. MC and its employees can rely on the protection provided by Section 38 of FICA and Section 7A of POCA.

Under no circumstances must the person suspected of money laundering be alerted to the report or must the matter be discussed with anyone except the MLRO and management. MC has introduced training to minimize the risk of a staff member tipping off a client or any other person with whom they come into contact, **FICA makes tipping-off an offence.** A person found guilty of tipping-off and acting negligently constitutes a fine of up to R10 million and/or 15 years imprisonment.

15. Training

In terms of Section 43, AIs must provide training to employees involved in transactions to which FICA applies to enable them to comply with the provisions of FICA and the RMCP. The format of

training is not prescribed. Formal training and FICA awareness training are both recognised. Both methods are designed to raise the level of awareness of employees regarding their obligations under FICA. A record of training attended and training material must be kept as proof.

Any training programme should educate employees on the following compliance obligations:

a) Establishing and verifying the identity of clients;
b) The duty to keep records;
c) The reporting duties and access to information; and
d) The risk management and compliance program.

The on-going training programme should further enable employees to:

a) correctly identify different types of clients in accordance with the FIC Act;
b) understand the duty to keep records correctly as per the AI's internal procedures; and
c) correctly identify and report different reportable transactions in accordance with the FIC Act.

MC employees should not be allowed to deal with clients if they have not received training on the FIC Act and RMCP.
MC on-going awareness training is provided via InConsultation across all MC staff and contractors. All FICA related information and training is stored electronically on Elite Wealth and is accessible to all MC staff and contractors.

Our awareness training programme includes assessments of employees and the record of training attended is kept. A training manual and records and reports are stored on InConsultation.

16. Non-Compliance

Any contravention of the rules contained in this manual or of the FIC Act will be dealt with in accordance to the disciplinary procedures as set out in the financial adviser and franchise house agreements. Any person convicted of an offence in terms of Chapter 4 of FICA may be liable to imprisonment for a period of not more than 15 years or a fine or not more than R 100 000 000.
Please refer to table below for further information pertaining to the offences and penalties associated with the FIC Act. MC observes the right to recover any penalty imposed upon it by a regulator due to the negligence of an employee from that employee.

The table below shows Penalties for Non-Compliances

Compliance Duty		Section	Regulations	Directives, Guidance Notes & Public Compliance Communications (PCCs)		Exemptions	Administrative Sanction	Criminal Sanction
Customer Due Diligence		20A, 21, 21A to 21H	N/A	GN 7		No exemptions	Natural Person = R10 million Legal Person = R50 million	N/A
Record Keeping		22, 22A, 23 & 24	20	PPC 02		No exemptions	Natural Person = R10 million Legal Person = R50 million	N/A
Reporting	**CTR**	28	22, 22B, 22C & 24	Directive 03/2014	GN 5B	No exemptions	Natural Person = R10 million Legal Person = R50 million	15 years or R100 million
	TPR	28A	22, 22A, 23B, 23C & 24		GN 6			
	STR	29	22, 23, 23A & 24		GN 4A		N/A	
	Cash Conveyance reporting	30	Not in operation					
	IFTR	31	Not in operation					
Risk Management & Compliance Programme		42	N/A	GN 7		No exemptions	Natural Person = R10 million Legal Person = R50 million	N/A
Training		43	N/A	GN 7 & PCC 18		No exemptions	Natural Person = R10 million Legal Person = R50 million	N/A
Governance of AML & CFT		42A	N/A	GN 7		No exemptions	Natural Person = R10 million Legal Person = R50 million	N/A
Registration		43B	27A	Directive 02/2014 & PCC 5C		No exemptions	Natural Person = R10 million Legal Person = R50 million	N/A

17. Client onboarding requirements

Before a MC financial adviser may enter into a business relationship with a client, the default documents as per the relevant FICA CDD checklist must be obtained.

Due to the nature of MC's business and its contractual agreements with various product providers, MC will require the documents listed on the FICA CDD checklist as a minimum requirement.

External product providers may require additional documents or information, in which case the adviser will be obliged to obtain and provide such information to the relevant product provider before an application for new business will be processed.

The FICA checklists are stored on InConsultation. All MC staff and contractors have access to the system.

The following FICA CDD checklists are utilized by MC:

a) Natural persons (RSA citizens);
b) Private companies;
c) Listed companies;
d) Close corporations;
e) Trusts;
f) Other legal persons; which include but are not limited to-

- Schools;
- Churches;
- Stokvels;
- Municipalities;
- Clubs;
- Non-profit organisations;
- Public Sector Entities/Government Departments;
- Semi-Public Entities;
- Deceased Estates;
- Insolvent Estates;
- Liquidators; and
- Curators.

g) Partnerships; and
h) Foreign companies.

18. Protection of personal information

MC will-

Collect personal information about its clients to offer them the best service. MC will not share this information outside of Momentum Metropolitan Holdings, its associated groups or agents, without the client's explicit consent. In order to provide the client with an effective service, we may be required to share this information with our administrators or agents who perform certain services for us (e.g. mail houses who post your statements on our behalf), members of Momentum Metropolitan Holdings, the client's financial adviser or broker, as well as with any regulatory bodies as the law requires. We may share the client's information with foreign regulatory bodies if required.

The client's information is used for administrative, operational, audit, marketing, research, legal and record keeping purposes. We will take all reasonable steps necessary to secure the integrity of any personal information which we hold about our clients and to safeguard it against unauthorized access. If our clients don't consent to us using their personal information, there may be delays or some instructions might not be carried out. Clients can have access to their information at any time and ask us to correct any information we have in our possession. Clients may write to us to obtain a copy of this information. We keep relevant documents for a period of five years or more as required by the law. If the client consents to us retaining their personal information for periods of longer than five years, we will restrict access to their information. It will only be processed for storage or for purposes of proof (with their consent).

MC, its holding company and all other entities that form part of the Momentum Metropolitan Holdings group of companies are required to collect relevant information from each client to ensure their identification and classification for tax purposes is correct according to the IGA, and report on these clients to the South African Revenue Services ("SARS") where necessary. The Intergovernmental Agreement ("the IGA") entered into between the Governments of South Africa and the United States of America was designed to improve international tax compliance and to implement the Foreign Account Tax Compliance Act ("FATCA"), and equivalent IGAs between the Government of South Africa and any other countries.

19. Annexures

19.1. **Annexure A – MC List of Product Providers**

19.2. **Annexure B – Client On-boarding process**

19.3. **Annexure C – Financial Adviser on boarding process**

19.4. **Annexure D – FICA CDD Checklist for Natural persons or Sole Proprietors**

19.5. **Annexure E – FICA checklist for Private Companies**

19.6. **Annexure F – FICA Checklist for Listed Companies**

19.7. **Annexure G – FICA Checklist for Close Corporations**

19.8. **Annexure H – FICA Checklist for Trusts**

19.9. **Annexure I – FICA Checklist for other legal persons**

19.10. **Annexure J – FICA Checklist for Partnerships**

19.11. **Annexure K – FICA Checklist for Foreign Companies**