momentum METROPOLITAN

# Financial Intelligence Centre Amendment Act: Risk Management and Compliance Programme Momentum Metropolitan Group

**Contents**

**DEFINITIONS**

| | |
|---|---|
| **Anti-money Laundering** | Encompasses all operational processes in respect of managing the risk of money laundering (AML) and combating of financing of terrorist activities (CFT) and combating proliferation financing (CPF). Where the abbreviation AML is used it is inclusive of CFT and CPF. |
| **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. |
| **Cash** | Is defined as coin and paper money of a 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. |
| **Client** (All roles CDD processes who should be applicable to) | A client is defined as a person (Natural, Legal or Otherwise) who enters into a business relationship or a single transaction with an AI.<br><br>A person acting on behalf of a client is normally the person introducing the prospective client to an AI or is acting on behalf of a client in terms of a mandate from a client or based on a contractual arrangement between the person and the AI. Examples would include Intermediaries who supplied financial advice and assistance to clients and who maybe in their own rights AI's.<br><br>List of clients:<br>• Prospective policyholder or policy owner.<br>• Policyholder or policy owner.<br>• Life insured.<br>• Premium payer.<br>• Beneficiary (At claims stage, maturity or payment to beneficiary (See 4.1).<br>• Investment investor.<br>• Cessionary (If the cessionary is not a known bank).<br>• A person acting on behalf of a client is deemed for the purposes of this RMCP a "client" and all CDD processes would be applicable to such persons, for example, financial advisers, official appointed power of attorney or curator. |

| | |
|---|---|
| **Client Due Diligence** | **Client Due Diligence,** can be defined as the process in which, reasonable **ongoing** steps are taken by an AI to know **prospective clients, persons acting on behalf of clients or the client acting on behalf of another** by verifying the identity of the prospective client(s), risk rating the client(s), establishing and verifying the source of wealth of the client(s) and the source of funds of each transaction, before concluding a single transaction or establishing a business relationship.<br><br>Certain prospective clients, especially related to their risk rating may have additional requirements imposed on them prior to or during the course business relationship or transaction. |
| **Client Due Diligence Checklists** | CDD checklists were created for each applicable client type. The list/s provide guidance to the client relating to the types of documents MMLL will accept for CCD purposes. Checklists have been designed for:<br><br>• Natural person or sole proprietor Closed Corporation<br>• Partnership<br>• Listed Company<br>• Private Company<br>• Foreign Company<br>• Trusts<br>• Other Legal Persons: Stokvels/churches/clubs/schools/municipalities, homeowner associations, etc. |
| **Dawn Raid Policy** | A “dawn raid” is a surprise investigation, in terms of specific legislation, that can take place at any of MMLL’s premises and is usually without warning. Many authorities have the power to gain entry and search premises without notice and can also arrest individuals during dawn raids. |
| **Effective Control** | Means ability to materially influence key decisions in relation to a legal person (e.g., the way the majority of voting rights attached to shareholdings are exercised, the appointment of directors of a legal person, decisions taken by a board of directors, key commercial decisions of a legal person), or the ability to take advantage of capital or assets of a legal person. |
| **MMLL** | Momentum Metropolitan Holdings Limited and its subsidiaries in all jurisdictions. |
| **MMLL Board** | Board of Directors of Momentum Metropolitan Life Limited. |
| **Management** | The line of business management structures, chief risk officers, operational risk managers, financial control officers, compliance officers. |

| | |
|---|---|
| **Proliferation Financing** | Is defined by the FATF as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or where applicable, international obligations. |
| **Risk** | Means the impact and likelihood of ML/TF/PF taking place. Risk refers to inherent risk, i.e., the level of risk that exists before mitigation. It does not refer to residual risk, i.e., the level of risk that remains after mitigation. |
| **Risk-based approach** | Means an approach whereby accountable institutions identify, assess and understand the ML/TF/PF risks to which institutions are exposed and take AML/CFT/CPF measures that are proportionate to those risks. |
| **Risk factors** | Means variables that, either on their own or in combination, may increase or decrease the ML/TF/PF risk posed by a business relationship or single transaction. |
| **Risk Management and Compliance Programme** | Section 42(1) obligates an AI to develop, document, maintain and implement a programme for anti-money laundering, counter-terrorist financing and counter-proliferation financing risk management and compliance.<br><br>A Risk Management and Compliance Programme must-<br><br>Enable the AI to-<br>(i) Identify.<br>(ii) Assess.<br>(iii) Monitor.<br>(iv) Mitigate; and<br>(v) Manage.<br><br>The risk that the provision by the AI of products or services may involve or facilitate money laundering activities, or financing of terrorist activities or proliferation financing. |
| **Senior Management** | An accountable institution is determined by the size, structure, and nature of the institution, as per Schedule 1 of the FICA Act. The senior managers whose approval is sought for purposes of the FICA Act, should have sufficient seniority and oversight to take informed decisions concerning the institution's compliance with the FICA Act, that bind the institutions to those decisions. |

| | |
|---|---|
| **Source of Funds** | Means the origin of the funds involved in a business relationship or single transaction. It includes both the activity that generated the funds used in the business relationship (for example the client's salary, occupation, business activities, proceeds of sale, corporate dividends, etc.), as well as the means through which the client's funds were transferred. |
| **Source of Wealth** | Means the activities that have generated the total net worth of the client that is, the activities that produced the client's funds and property (for example inheritance or savings), to fund the contract. |
| **Transaction** | Receiving an instruction or application that will result in a conclusion of a transaction or an alteration to any policy/Investment contract; and/or<br><br>Receiving an instruction or application that would create an inflow or outflow of funds on any new or existing policy/Investment contract and includes dealing in second-hand policies. Including ending of contract. |

**ABBREVIATIONS**

| | |
|---|---|
| **AI or AI's** | Means Accountable Institutions (AI) in terms of Schedule 1 of the FICA Act. |
| **AML** | Means anti-money laundering. |
| **AML/CFT/CPF** | Means anti-money laundering, counter terrorist financing and counter proliferation financing |
| **ATMS** | Automated Transaction Monitoring System. |
| **CDD** | Refers to Section 21 of the FICA Act. |
| **CTR** | Refers to a Cash Threshold Report submitted in terms of Section 28 of the FICA Act. |
| **DNFBP** | Designated Non-Financial Businesses and Professions |
| **DPEP** | Refers to Domestic Politically Exposed Person. |
| **DPIP** | Refers to Domestic Prominent Influential Person. |
| **EDD** | Enhanced Due Diligence is when additional information or documents are required or documents need to be certified, depending on the risk rating of the client. |
| **FATF** | Refers to Financial Action Task Force. |
| **FICA Act** | Financial Intelligence Centre Act as Amended, dated 1 of 2017 |
| **FPEP** | Refers to Foreign Politically Exposed Person. |
| **MLCO** | Refers to the Money Laundering Compliance Officer. |
| **MLRO** | Refers to the Money Laundering Reporting Officer. |
| **MLTFC Regulations** | Refers to Money Laundering and Terrorist Financing Control Regulations issued under the FICA Act. |
| **NPWMD** | Non-Proliferation of Weapons of Mass Destruction |
| **OGS** | On-going screening |
| **PA** | Refers to the Prudential Authority. |
| **PEP** | Refers to a Politically Exposed Person. |
| **PF** | Refers to Proliferation Financing |
| **RMCP** | Refers to the Risk Management and Compliance Programme. |
| **STR** | Refers to a Suspicious Transaction Report in terms of Section 29 of the FICA Act. |

| | |
|---|---|
| **TFS** | Refers to the Targeted Financial Sanctions List pursuant to Section 26A of the FICA Act. |
| **TF** | Refers to Terrorist Financing |
| **TPR** | Refers to a Terrorist Property Report in terms of Section 28A of the FICA Act. |
| **UBO** | Refers to the Ultimate Beneficial Owner. |
| **WMD** | Refers to Weapons of Mass Destruction |

# 1. INTRODUCTION

## 1.1. Purpose of document

The Financial Intelligence Centre Amendment Act ("FICA Act: Act 1 of 2017") is formal legislation intended to combat money laundering activities and the financing of terrorist and related 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, terrorist financing and proliferation financing, South African law also imposes several control measures that must be adhered to which are aimed to facilitate the prevention, detection and investigation of money laundering, terrorist financing activities and proliferation financing.

These control measures introduced by the FICA Act, 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, the FICA Act further imposes on AIs the requirement to implement a formal Anti-money laundering (AML), Counter-Terrorist Financing (CTF) and Counter Proliferation Financing (CPF), Risk Management and Compliance programme (RMCP).

The Financial Action Task Force (FATF) is a global inter-governmental body, that sets international standards for combating money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.

As a policy-making body, the FATF attempts to generate the political will to bring about national legislative and regulatory reforms in countries, who are committed to implementing these reforms. South Africa became a member of the FATF in 2003 and is one of 39 member countries.

Mutual evaluations and peer reviews are used to assess countries' level of compliance to the FATF AML/CFT/CPF standards and identify steps necessary for them to increase their effectiveness. Countries undergo these evaluations at regular intervals. South Africa was previously evaluated in 2003 and 2009.

The most recent review by the FATF and the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), commenced in April 2019 and was concluded in May 2021.

Various immediate outcomes were identified during the FATF evaluation, which had to be addressed, not only to be compliant to the FICA Act, but to also continue to actively prevent money laundering, terrorist financing and proliferation financing by applying applicable preventative measures.

The findings of mutual evaluations are geared to assist member countries in strengthening their financial system, thereby enhancing the integrity of their financial system. Preventative measures are deemed of critical importance, and it is therefore importance that AIs must adequately implement measures to mitigate their risks.

South Africa was given one year to report on the progress made to achieve the recommendations set out in the 2021 Mutual Evaluation Report, failing which the country would be added to the list of "jurisdictions under increased monitoring" (the "grey list") at the following FATF plenary meeting in February 2023.

At the plenary meeting, held on 24 February 2023, the FATF determined that South Africa had serious weaknesses in its AML/CTF/CPF framework and had not successfully demonstrated sufficient compliance with the FATF recommendations. This posed a threat to the international finance system and as a result South Africa was added to the "grey list".

The FATF has prescribed an eight-step action plan which, if achieved, will result in South Africa being lifted from the grey list. The action plan is detailed as follows:

- Demonstrate a sustained increase in outbound mutual legal assistance requests that help facilitate money laundering and terrorist financing investigations and confiscations of different types of assets in line with its risk profile.
- Improve risk-based supervision of DNFBPs and demonstrate that all AML/CTF supervisors apply effective, proportionate, and effective sanctions for noncompliance.
- Ensure that competent authorities have timely access to accurate and up-to-date beneficial ownership information on legal persons and arrangements and applying sanctions for breaches of violations by legal persons to beneficial ownership obligations.
- Demonstrate a sustained increase in law enforcement agencies' requests for financial intelligence from the FIC for its money laundering and terrorist financing investigations.
- Demonstrate a sustained increase in investigations and prosecutions of serious and complex money laundering and the full range of terrorist financing activities in line with its risk profile.
- Enhance its identification, seizure, and confiscation of proceeds and instrumentalities of a wider range of predicate crimes, in line with its risk profile.
- Update its terrorist financing risk assessment to inform the implementation of a comprehensive national counter-financing of terrorism strategy.
- Ensure the effective implementation of targeted financial sanctions and demonstrate an effective mechanism to identify individuals and entities that meet the criteria for domestic designation.
- Prioritise law enforcement initiatives where regulators are required to increase their level of supervision, ensuring that investigations are sufficiently and effectively supported, both locally and internationally.

South Africa has committed to resolving the eight strategic actions by January 2025. The length of time that South Africa will remain on the grey list will depend on the speed at which the deficiencies are resolved.

### 1.2. Defining Anti-Money Laundering (AML), Countering the Financing of Terrorism and Proliferation Financing

The difference between AML and CFT preventative measures and CPF, are dealt with together, in the FICA Act. It is important to note that a distinction exists in the nature of the 3 (three) offences.

Money Laundering is the process used by criminals to hide, conceal, or disguise the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds.

Criminals who have generated an income from their criminal activities usually follow 3 (three) common stages to launder their money. The first stage is commonly referred to as ‘placement’. This is when criminals introduce their illegally derived proceeds into legitimate financial systems. An example of this would be splitting a large portion of cash into smaller sums and thereafter depositing the smaller amounts into bank accounts.

The second stage is called ‘layering’. During this stage, the launderer engages in a series of transactions, conversions, or movements of the funds to cloud the trail of the funds and separate them from their illegitimate source. The funds might be channelled through various means for example, the purchase and sale of financial products.

The third stage is ‘integration’. This generally ensues the successful stages of placement and layering. The launderer at this stage causes the funds to re-enter the economy and appear to be legitimate. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

Although the use of all 3 (three) stages are common, it is not always utilised by the criminal who wishes to launder the funds. In some instances, criminals may choose to merely ‘place’ the illegally derived funds into the economy by merely depositing the money into his or her bank account, without any layering occurring. They can withdraw the money and spend it at their will.

Financing of terrorism is the collection or provision of funds for the purpose of enhancing the ability of an entity or anyone who is involved in terrorism or related activities to commit an act that is regarded as a terrorist act. There are different types of terrorism and acts of terrorism, for example, Civil disorder, which is sometimes a violent form of protest held by a group of individuals, usually in opposition to a political policy or action. Political terrorism, which is used by one political faction to intimidate another. Funds may be raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping, and extortion.

Terrorist and violent extremist groups continue to exploit the internet and online media platforms to spread their radical views and propaganda for the recruitment, financing, training and incitement to commit acts of terrorism. In this context, the threat posed by lone actors, who are self-radicalised, poses a particular security challenge. These lone actors have the ability to conduct largely unsophisticated, but lethal attacks against targets. These attackers often have few or no formal ties or direct exposure to terrorist groups.

The terrorism financing risk presents a security risk as well as a reputational risk due to obligations in accordance with the United Nations and international oversight bodies, including the FATF. South Africa is a member of both bodies, which requires the country to take the necessary measures to effectively prevent exploitation for terrorism financing purposes.

Terrorism financing poses a direct threat to South Africa's national security as well as the integrity and reputation of its financial system. Terrorism financing has the potential to finance and enable terrorist activities locally and abroad. Over and above posing a security threat, it also impacts the integrity of non-financial institutions such as charities and non-profit organisations (NPOs) which could be exploited, often unwittingly, for the financing of terrorism.

Terrorist groups make use of multiple methods to raise, move, store and/or use funds and exploit the inherent vulnerabilities of countries' regulatory, financial, law enforcement and security frameworks. Their techniques vary and depend on the sophistication and objectives of terrorists, terrorist organisations and their sympathisers. Terrorism financing investigations are usually extremely complex, particularly with regard to the identification of financiers and ultimate end-users of the generated funds.

Terrorism financing is the financial and logistical support, in any form, of terrorism or of individuals, entities or groups that encourage, plan or engage in acts of terrorism and includes plans or intended plans to support or commit an act of terrorism. It generally falls into two broad categories:

- Funding the direct costs associated with undertaking a terrorism act, for example expenses for recruitment, travel, explosive materials, weapons, vehicles and training, etc.
- Funding required to sustain a terrorist, a terrorist group, network or cell, either inside the country, transiting the country, or emanating from abroad.

Current terrorist activities in northern Mozambique have brought the terrorism threat closer, with the movement of a small number of terrorist suspects between South Africa and Mozambique having been recorded. These terrorist suspects are likely to travel with cash to be used for personal consumption or to fund the activities of the insurgents in Mozambique. Claims of funding for attacks in Mozambique and Kenya emanating from South Africa is of serious concern and investigations to confirm or refute claims and quantify the possible movement of funds across borders are ongoing. International crime syndicates and refugees travelling through the region may also abuse South Africa, potentially facilitating the movement of cash or other assets to terrorist groups in the region.

The key consideration when taking measures to prevent terrorist financing is to examine the intended use or destination of the funds as opposed to its origin. The FATF provided a working definition of proliferation financing which reads as follows:

> *"Proliferation financing" refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.*

The FATF also have a narrower definition for PF risk:

> *"The potential breach, non-implementation or evasion of the targeted financial sanctions"*

PF is confined to instances where funding is made available to or for the benefit of a person or entity whose name appears on a TFS list, due to the proliferation of WMD.

Proliferators use several evasive techniques and tactics to circumvent the financial sanctions restrictions applied against them, providing them access to the financial system. Some key methods are:

- To avoid detection or distance themselves from certain transactions.
- Attempt to hide behind legal persons, trusts and partnerships.
- Utilise shell or front companies to obscure either the identity of the beneficial owner, the goods or activity being provided or the geographic area where the goods are destined.
- Hides the nature of the industry and the associated nature of goods they operate in.
- This risk could be further heightened, given the nature of the accountable institution's product offered to the client.

The Non-Proliferation of Weapons of Mass Destruction Act, 1993 (Act 87 of 1993) (NPWMD Act) defines a WMD, as:

> *"Any weapon designed to kill, harm or infect people, animals or plants through the effects of a nuclear explosion or the toxic properties of a chemical warfare agent, or the infectious or toxic properties of a biological warfare agent and includes a deliver system exclusively designed, adapted or intended to deliver such weapons."*

AIs should conduct risk assessments at business and client level, as well as in terms of new products and processes, in order to identify and determine the risk of PF and implement controls to monitor, mitigate and manage these risks within their framework.

When AIs have a better understanding of proliferation financing risks, it will positively contribute to its ability to prevent persons and entities involved in WMD or proliferation from

raising, moving and using funds, and thus the implementation of targeted financial sanctions contributes to a stronger counter proliferation financing regime.

**Proliferation Financing Risks**

At a country level, South African PF of WMD risk factors stem from several environmental vulnerabilities that can be exploited to facilitate PF, which, inter alia, may consist of the following:

- Poor enforcement of security protocols and contraventions by officials in the border security environment in the issuing of travel and identity documentation is the first major PF vulnerability.
- In the context of a large informal economy that is mostly cash-based, many remittances from refugee communities to their host countries, including high-risk countries, present a further vulnerability that can be abused for PF.
- Against the background of voluntary registration, NPOs that operate in high-risk jurisdictions and insufficient attention being applied to security.
- Concerns linked to PF by regulatory authorities; and within SA, it is possible for accountable institutions, to inadvertently process funds that are unknowingly linked to PF and/or the movement of funds/goods destined for PF of WMD.

AIs cannot rely on sanction screenings alone, to identify PF, AIs are to delve into the potential for heightened PF of WMD risk factors within South Africa's financial system.

To ensure an effective risk approach, a PF risk assessment that is undertaken will assist an AI.

It is important that AIs fully understand and document their inherent and residual PF of WMD risks to which the business's operations could be exposed to.

**Heightened PF risk factors include, but is not limited to:**

- Type of client
- Activities/Nature of client's business
- Geographic location
- Products and Services offered to client.

**A PF risk assessment should include the following:**

- Identification of all PF threats and vulnerabilities by compiling a list of major known or suspected threats, key sectors, products or services, activities that designated individuals/entities engaged in or that have been exploited, based upon known typologies; and

- Assessment and risk rating of the identified PF threats and vulnerabilities considering the nature, scale, complexity and geographical footprint of the AI, its target market/s and client profiles, the volume and size of its transactions and the products and services offered.
- Regular PF of WMD risk assessments are necessary to enhance and update the AI's PF risk understanding and be in a position to evidence same.
- AIs must articulate their understanding of their PF of WMD risks in their implemented corporate governance, risk management, internal controls, policies, processes and procedures to ensure ongoing compliance and adequate risk management of their respective exposures to risk.

**PF client risk assessment:**

PF client risk should be identified and assessed in accordance with the processes, procedures and methodology outlined in the AI's RMCP.

In assessing PF client risk, AIs should:

- Scrutinise all clients at onboarding to ensure that the client is not a sanctioned person/entity.
- Assess whether the client is connected or situated in a country that is subject to relevant UN sanctions.
- Assess the client's legal structure if it appears overly complex to hide beneficial owners that are subject to PF TFS screening.
- Assess the use of joint ventures by legal persons to evade TFS.
- Assess clients who offer certain products and services that face heightened risk of being abused for PF, e.g., import and export businesses, freighting companies, airlines, warehouses, chemical manufacturing companies, precious metal dealers and ammunition manufacturers, to name a few.
- Assess the type of business the client engages in, particularly businesses dealing in
- dual-use goods or goods subject to export control or complex transactions.
- Consider that a client who lists a dual-use good as being traded may have a legitimate
- purpose for the dual-use good and would need to apply to the appropriate authority (such as the Non-proliferation Council) for a permit to obtain on to trade therein and that where such permit is produced may be a contributing factor for consideration in the overall risk assessment of the client, for example importing of technologies like drones. *(http://non-proliferation.thedtic.gov.za/)*
- Consider that proliferators may not openly indicate that they wish to trade in controlled goods and may also seek to trade in goods that have specifications that are slightly below the specifications of controlled goods and may modify/upgrade/process goods further down the line to the controlled specifications as per their requirements for use in proliferation activities. *(https://www.un.org/securitycouncil/sanctions/1718/prohibited-items)*
- Assess whether the client's duration of the business accords with the knowledge and transactional activity of the client.
- Consider how the geographic proximity to jurisdictions that are vulnerable to PF of WMD risk may impact it.

- Consider if the client is diplomatic personnel or linked to any embassy or diplomatic personnel from high-risk countries with high PF and/or WMD proliferation concerns.
- Consider if higher PF and/or WMD proliferation risks may be present where there are active ports and potential PF transit/transhipment routes (South Africa has large and active ports in Africa).
- Assess whether the client, beneficial owner or person acting on behalf of the client is a DPEP/FPPO/DPIP or government entity dealing in high-risk sector or trading in controlled goods.
- Consider if the client is represented by a third-party in a manner that is not aligned to the client's profile or that does not make business sense or seems unnecessary.
- Consider the cross-border financial and trade flow with high-risk jurisdictions.
- Assess the level of disclosure or proposed trading activities by clients during onboarding or the vagueness of such disclosure when requested to do so.
- Assess whether clients have the requisite technical knowledge/skill to align to the stated business activity that they wish to conduct.
- Assess whether the utilization of numerous third parties and/or complex trade-based activities are aligned to the business profile held in respect of the client at onboarding or during the client relationship.
- Ensure that where trade finance transactions are concerned in respect of clients, that they thoroughly understand the activities of their clients with regards to the trade finance transactions being engaged in, including the beneficial owners, the parties to the transaction and the flow of funds in terms of geographical areas, with increased scrutiny being applied where heightened risk is identified.
- Assess whether the originator and/or beneficiary of a transaction is a person or entity resident or domiciled in a country of PF or diversion concern; and/or consider additional factors such as the purpose of the relationship, corporate structure and volume of anticipated transactions which may be indicators of increased potential for PF risk.
- Where additional information is required clarity whether a transaction poses a PF risk and where such information is not provided, the AI should consider submitting a STR in terms of Section 29 of the FICA Act.

| **COMPARISON BETWEEN MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING** | | | |
|---|---|---|---|
| | **MONEY LAUNDERING** | **TERRORIST FINANCING** | **PROLIFERATION FINANCING** |
| **Source of Funds** | Nationally from within criminal organisations | Nationally from self-funding organisations/groups/gangs (centred on criminal activity). | Often state sponsored programs but also through fundraising activities by public sector |
| **Conduits** | Favours formal financial system | Favours cash couriers or informal financial systems such as Hawala and currency exchange firms | Formal financial system preferred up until the point of entry into where the money is |

| | | | |
|---|---|---|---|
| | | | designated to, then taken out in cash. |
| **Detection Focus** | Suspicious transactions such as deposits uncharacteristic of customer's wealth or the expected activity | Suspicious relationships, such as electronic transfers between seemingly unrelated parties | Individuals, entities, states, goods and materials, activities |
| **Transaction Amounts** | Large amounts often structured to avoid reporting requirements | Small amounts usually below reporting thresholds | Moderate amounts |
| **Financial Activity** | Complex web of transactions often involving shell or front companies, bearer shares, offshore secrecy havens | Varied methods including formal banking system, informal value-transfer systems, smuggling of cash and valuables | Transactions look like normal commercial activity, structured to hide connection to proliferator or proliferation activities |
| **Money Trail** | Circular – money eventually ends up with the person who generated it | Linear – money generated is used to propagate terrorist groups and activities | Linear – money is used to purchase goods and materials from brokers or manufacturers. The money can also move in the opposite direction (i.e., from the broker/manufacturer to the proliferator). |

**AML, TF and PF Combating measures include, but not limited to:-**

- the implementation of the Targeted Financial Sanctions,
- supervision and monitoring of compliance,
- establishing the source of funds,
- establishing to whom payments are processed to,
- identifying clients by means of stringent CDD processes,
- knowing the client's business; and
- whether the client is involved in WMD and establishing and implementing asset freeze processes.

**Adherence to content**

This document is therefore prepared to comply with Section 42 of the FICA Act as to advise all permanent and temporary employees, including independent contractors of the specific duties required, which stem from the requirements of the Act. The duties that the Act imposes on employees also form part of the employment contracts of MMLL employees.

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

Due to the complexity of the MMLL Group structure, this document sets the standards for the multiple business units, which must be adhered to.

Each business unit is responsible to compile their own business specific RMCP, which is applicable to their business environment.

The primary legislation related to AML/CTF/CPF in force in South Africa are the Financial Intelligence Centre Amendment Act, 1 of 2017, the Prevention of Organised Crime Act, 121 of 1998 (POCA) and the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 33 of 2004 (POCDATARA).

**The Prevention of Organised Crime Act, No 121 of 1998 (POCA)**

**Purpose**

To create a mechanism for criminal confiscation of proceeds of crime and civil loss of proceeds.

POCA creates serious offences relating to ML.

These offences include but are not limited to the involvement in money laundering transactions, the rendering of assistance or advice to a criminal to assist him to control the proceeds of unlawful activities and the acquisition and use or possession of the proceeds of unlawful activities of another.

The offences can also be committed negligently by third parties who assist criminals to conclude transactions that launder proceeds of unlawful activities.

**Offences under POCA**

- Offences involving proceeds of all forms of crime and therefore all pattern of racketeering;
- Receiving property copied from racketeering and using that property; and/or
- Receiving property from an enterprise, knowing that the property results from racketeering.

**Penalties under POCA**

A maximum fine of up to R100 million, and/or imprisonment of up to 30 years.

**The Protection of Constitutional Democracy Against Terrorism and Related Activities, Act No 33 of 2004. (POCDATARA)**

**Purpose**

The anti-money laundering measures have been broadened because of money laundering by terrorist organisations. In South Africa this led to the 2004 POCADATARA Act. In Section 28A of the FICA Act it requires the reporting of any offence linked to terrorist activities, including terrorist financing.

**Objectives**

To provide for measures to prevent and combat terrorist and related activities; to provide for an offence of terrorism and other offences associated or connected with terrorist activities; to provide for Convention offences; to give effect to international instruments dealing with terrorist and related activities; to provide for a mechanism to comply with United Nations Security Council Resolutions, which are binding on member States, in respect of terrorist and related activities; to provide for measures to prevent and combat the financing of terrorist and related activities; to provide for investigative measures in respect of terrorist and related activities; and to provide for matters connected therewith.

POCDATARA creates its own reporting obligations but also amended the FICA Act by inserting a new reporting provision in respect of property associated with terrorism and related activities. The duty to report suspicious and unusual transactions under FICA Act was also extended to transactions that are known to be, or suspected of being, linked to terrorist financing.

**Offences associated or connected with financing of specified offences**

**4.** (1) Any person who, directly or indirectly, in whole or in part, and by any means or-

a) acquires property;
b) collects property;
c) uses property;
d) possesses property;
e) owns property;
f) provides or makes available, or invites a person to provide or make available property;
g) provides or makes available, or invites a person to provide or make available any financial or other service;
h) provides or makes available, or invites a person to provide or make available economic support; or
i) facilitates the acquisition, collection, use or provision of property, or the provision of any financial or other service, or the provision of economic support,
j) intending that the property, financial or other service or economic support, as the case may be, be used, or while such person knows or ought reasonably to have known or suspected that the property, service or support concerned will be used, directly or indirectly, in whole or in part-

(i) to commit or facilitate the commission of a specified offence;

(ii) for the benefit of, or on behalf of, or at the direction of, or under the control of an entity which commits or attempts to commit or facilitates the commission of a specified offence; or
(iii) for the benefit of a specific entity identified in a notice issued by the President under Section 26A, is guilty of an offence.

(2) Any person who, directly or indirectly, in whole or in part, and by any means or
a) deals with, enters into or facilitates any transaction or performs any other act in connection with property which such person knows or ought reasonably to have known or suspected to have been acquired, collected, used, possessed, owned or provided-

(i) to commit or facilitate the commission of a specified offence;
(ii) for the benefit of, or on behalf of, or at the direction of, or under the control of an entity which commits or attempts to commit or facilitates the commission of a specified offence; or
(iii) for the benefit of a specific entity identified in a notice issued by the President under Section 26A; or

b) provides financial or other services in respect of property referred to in paragraph (a), is guilty of an offence.

(3) Any person who knows or ought reasonably to have known or suspected that property is Property referred to in subsection *(2)* arrangement which in any way has or is likely to have the effect of- *(a)* and enters into, or becomes concerned in, an arrangement which in any way has or is likely to have the effect of-
a) facilitating the retention or control of such property by or on behalf of-
(i) an entity which commits or attempts to commit or facilitates the commission of a specified offence; or
(ii) a specific entity identified in a notice issued by the President under Section 26A;
b) converting such property;
c) concealing or disguising the nature, source, location, disposition or movement of such property, the ownership thereof or any interest anyone may have therein;
d) removing such property from a jurisdiction; or
e) transferring such property to a nominee is guilty of an offence.

**Penalties under POCDATARA**

POCDATARA provides penalties for contravention of Section 4. A person who is convicted of such an offence is liable, in the case of a sentence to be person who is convicted of such an offence is liable, in the case of a sentence to be imposed by a High Court or a regional court, to a fine not exceeding R100 million or to imprisonment for a period not exceeding 15 (fifteen) years. If the sentence is imposed by a magistrate's court, the maximum fine is R250 000.00 and the maximum term of imprisonment is 5 (five) year.

### 1.3. Key elements to ensure compliance with the FICA Act

**Board Responsibility for Oversight of Compliance**

The Board of MMLL has effective accountability to ensure compliance with the FICA Act and internal RMCPs, furthermore any reference to compliance in this RMCP should be regarded as a reference to compliance with the FICA Act.

The MMLL Board and Senior Management of any MMLL business are responsible for managing the business effectively and compliantly.

The MMLL Board and Senior Management acknowledge the ultimate responsibility to ensure that the MMLL AIs maintains an effective internal AML/CTF control structure through an RMCP. A culture of compliance is expected within each specific AI exists to ensure that the relevant AI's policies, procedures and processes are designed to limit, manage and control the risk of money laundering, terrorist financing and proliferation financing.

The MMLL Board and Senior Management are fully engaged in decision-making processes and take ownership of the risk-based measures as they are aware that they will be held accountable if the content of the RMCP and its applications are found to be inadequate.

The MMLL Board takes responsibility to ensure compliance by MMLL and must consider the appropriateness and effectiveness of compliance and the review of thereof, at appropriate intervals.

In this regard approval of the RMCP by the MMLL Board of directors and Senior Management of the relevant AI will establish a formal annual review process, or sooner where legislation changes require action.

Directive 8, issued by the FIC, on 31 March 2023, in terms of the FICA Act, section 43A(1), requires ALL AIs to screen prospective employees and current employees for competence and integrity, as well as to scrutinise employee information against the TFS sanctions lists, in order to identify, assess, monitor, mitigate and manage the risk of ML, TF and PF.

MMLL, Group Forensic Services, will subject all employees to the Group's TFS standard screening process to identify and scrutinise employee information. All records will be kept electronically on WorldCheck1, relating to the details scrutinised.

If a prospective employee be identified as a match to the TFS list, the individual will be reported to the FIC via the MMLL MLRO, on the go-AML facility linked to the FIC. MMLL, will not employ the individual, identified. Should an existing employee be identified on the list, the individual will be reported to the FIC via the MMLL MLRO, on the go-AML facility linked to the FIC. This employee will also be reported to the Human Capital for off-boarding, as per their established Human Capital processes.

Directive 8 also obligates AIs to screen prospective and current employees on a risk-based approach, for competence and integrity periodically. These processes are to be established and embedded within the Human Capital environments and will be included in the standard on-boarding processes of a prospective employee. (*Work in progress.)*

The MMLL Board ratified the current MMLL AML Policy, which states inter alia that: -

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

- Be provided with the relevant RMCP documentation which, must provide substantial information to the MMLL Board to gain a full appreciation for the ML/TF/PF risks the AI faces and the controls that are in place to mitigate and manage the risk and whether the RMCP enable compliance by the AI.
- Ensure that the compliance policy considers 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.
- Consider whether it would be appropriate to maintain a separate audit function to assess the adequacy and effectiveness of the area of compliance.
- Ensure that when a review of compliance is discussed by the MMLL Board at appropriate intervals the necessary action is taken to remedy any identified deficiencies.
- Ensure that the MMLL financial services businesses are meeting its obligation, that its branches and subsidiaries operating outside South Africa comply with the Regulations and applicable local law which is consistent with the **FATF** Recommendations.
- Ensure that adequate resources either from within the financial services business, within the group, or externally exists to ensure that the AML/CTF/CPF policies are adhered to.
- Ensure that the RMCP is adequate, suitable and effective for the AI.
- Ensure that the RMCP and relevant documentation is approved, by the MMLL Board, as per section 42(2B) of the FICA Act.
- Ensure that documentation provided to the FIC or supervisory body, upon request or during an inspection, must be approved by the MMLL Board.
- Inadequate RMCP documentation provided to the FIC or supervisory body, constitutes non-compliance with the FICA Act and may lead to the imposition of administrative sanctions, in terms of Section 61 of the FICA Act.
- The MMLL Board cannot approve a RMCP document that merely references elements of its RMCP, as the MMLL Board would not have adequately discharged its duty in terms of Section 42A(1) of its obligations.

**In this regard the affected Senior Management acting on behalf of the MMLL Board will:**

- Provide adequate resources either from within the AI or financial services business, or externally to ensure that the AML/CTF/CPF policies are adhered to.
- Implement appropriate AML/ CTF/CPF policies.
- Implement processes for ongoing review and governance of policies.
- Implement governance structures roles and responsibilities, reporting frameworks and processes.
- Manage assurance and regulatory reviews.
- Appoint accountable persons to manage ML, TF and PF risks.
- Ensure the necessary AML/ CTF/CPF skilled resources are employed.
- Implementation of appropriate AML/CTF/CPF training programs.
- Implement simplified and enhanced CDD measures.
- Implement CDD programs to meet regulatory requirements whilst remaining customer centric.
- Establish effective records management practices and processes with supporting systems.
- Source appropriate supporting AML/CTF/CPF technology solutions and systems.
- Ensure that the financial services business is meeting its obligation that its branches and subsidiaries operating outside South Africa comply with the applicable local law which is consistent with the FATF Recommendations.

**The MMLL Compliance and Risk Managements Structure**

MMLL has a centralized, supported by a decentralised business compliance structure, within the MMLL Group. The MMLL centralized Compliance Team provides guidance and assistance to the various AIs within the MMLL Group structure.

The relevant Board of an AI will appoint the AML/TF Compliance Officers and the Risk Management Team within each AI is responsible for the following functions:

**The Role of the MMLL Chief Risk Officer:**

- Implement appropriate AML/CTF and CPF policies.
- Implement processes for ongoing review and governance of policies.
- Implement governance structures roles and responsibilities, reporting frameworks and processes.
- Managing assurance and regulatory reviews as part of the Own Risk and Solvency Assessment programme.

**Accountability for the implementation of the RMCP**

The Board of MMLL has complete accountability to ensure compliance with the FICA Act as well as ensuring the implementation of and managing of internal RMCPs.

**Senior Management of an AI or financial services business will ensure that this RMCP is effectively embedded in totality within an AI or financial services business.**

**The Role of Compliance**

The compliance function will ensure that the compliance policy takes into account of, 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. Furthermore, the compliance function will ensure that when a review of compliance is discussed by the Senior Management at appropriate intervals, the necessary action is taken to remedy any identified deficiencies.

The compliance function shall act proactively to assure the quality of compliance in the Group through information, advice, control, and follow-up within the compliance areas, thereby supporting the business activities and management. The compliance functions provides guidance and assurance on the level of compliance to the MMLL Boards and relevant Board Committees. Further to this it promotes a corporate culture of compliance. MMLL has approved a zero-risk appetite for regulatory non-compliance.

**Process: -**

- The compliance functions in the Group assist the MMLL Board in overseeing and monitoring that the AIs meets its legal and regulatory obligations and promotes and sustains a sound compliance culture.
- The compliance functions have implemented risk-based compliance monitoring plan to:
    - monitor compliance of the AI's systems of compliance and related internal controls, as well as legal and regulatory obligations; and
    - Identify, assess and report on key legal and regulatory risks.
- The compliance functions assess the appropriateness of policies, processes, and controls in respect of key areas of legal, regulatory, and ethical obligations and the effective monitoring thereof.
- The compliance functions monitor compliance shortcomings and instances of non-compliance and report to the relevant regulatory authorities.
- The compliance functions ensure that regular training is conducted on compliance obligations, particularly for employees in positions of trust or responsibility, or who are involved in activities that have significant legal or regulatory risk.
- The compliance functions are responsible for ensuring that staff who wish to report concerns on the AIs functions and processes are able to do so with appropriate protection, unless the role is assigned to another suitable function.
- The compliance functions have unhindered access to the MMLL Board, or a Committee of the Board identified by the MMLL Board on:
    - the strategy of the compliance function;
    - the compliance monitoring plan, including specific annual or other short-term goals being pursued and the performance against such goals; and
    - information on its resources, including an analysis on the appropriateness of those resources.
    - the effectiveness of the function, and the effectiveness of business processes and controls of dealing with AML, CTF and CPF.

**The Role of Internal Audit**

**Appropriate independent audits to assess the adequacy and effectiveness of the business processes related to this RMCP and areas of required compliance.**

Internal audit is an independent Group-wide function that reports directly to the MMLL Board. The main responsibility of internal audit is to provide reliable and objective assurance to the MMLL Board regarding the effectiveness of controls, risk management and governance processes, with the aim of mitigating current and evolving high risks and in so doing improve the control culture within the Group. MMLL has an internal audit function that provides independent, objective assurance to the MMLL Board in respect of the effectiveness of its governance, risk management and internal controls.

**Process: -**

- The internal audit function has the capability of providing the MMLL Board with independent assurance in respect of the adequacy and effectiveness of the AI's corporate governance framework, and systems for risk management and internal control.
- The internal audit function provides independent assurance to the MMLL Board, through regular audit activities, on matters such as:
    - the means by which the AI preserves its assets and those of policyholders, and seeks to prevent fraud, misappropriation or misapplication of such assets.
    - the reliability, integrity and completeness of the accounting, financial, risk mitigation and compliance, as well as the capacity and adaptability of the AI's information technology architecture to provide all relevant information in a timely manner to the MMLL Board, Senior Management and regulators.
    - the design and operational effectiveness of the AI's controls in respect of the above matters.
    - other matters as may be requested by the MMLL Board, Senior Management, and regulators or external auditors; and
    - other matters which the internal audit function determines should be reviewed to fulfil its responsibilities as set out in its charter.
- The heads of the AIs internal audit function reports directly to the Board of Directors or the Audit Committee. In its reporting, the internal audit function will address at least the following:
    - the function's annual or other periodic risk-based audit plan, detailing the proposed areas of audit focus, and any significant modifications to the audit plan.
    - any factors that may adversely affect the internal audit function's independence, objectivity or effectiveness.
    - material findings from audits or reviews conducted; and
    - The extent of Senior Management's compliance with agreed corrective or risk-mitigating measures in response to identified control deficiencies, system weaknesses, or compliance violations.

**Ensure that the financial services business is meeting its obligation that its branches and subsidiaries operating outside South Africa comply with the applicable local law which is consistent with the FATF Recommendations.**

**Process: -**

Extract from MMLL Governance Framework:

- MMLL subsidiaries are required to take cognisance of all guidelines, policies, procedures and the like, developed by MMLL and customize these for use, as far as reasonably possible, subject to taking into account local laws and prescriptions. This form of adoption will ensure that any fundamental developments and business decisions (financial, business and reputation) taken by MMLL subsidiaries which materially impact on that particular subsidiary or MMLL as a group, may be dealt with appropriately through documents and processes applied consistently within the group in order to mitigate material systemic risks to the group.

**This RMCP in terms of Section 42(2) of the FICA Act provides the way** the RMCP is implemented in the various branches, subsidiaries or other operations of MMLL in foreign countries in order to enable MMLL to comply with its obligations under the FICA Act.

MMLL will determine if the host country of a foreign branch or subsidiary permits the implementation of measures required under the FICA Act.

MMLL will inform the FIC and supervisory body concerned if the host country contemplated does not permit the implementation of measures required under the FICA Act.

**The Role of Risk Management**

The risk management function assists MMLL in performing specialised analysis and performing quality reviews of the risk management system, monitoring the risk management system and maintaining an organisation wide view of the risk profile.

**Process:-**

- AIs have effective risk management functions, capable of assisting the Board of Directors and Senior Management to develop and maintain a risk management system to identify, assess, monitor, and mitigate the AI's material risks, and promote a sound risk culture.
- An AI's risk management function is responsible for providing reasonable assurance that adequate mechanisms and procedures are established, implemented, and maintained to:
    - identify the individual and aggregated risks (current and emerging) the AI faces;
    - assess, monitor and help manage identified risks effectively;
    - gain and maintain an aggregated view of the risk profile; and

  - establish a forward-looking assessment of the risk profile and financial position of the AI, including the conducting of regular stress testing and scenario analyses as defined in GOI 3.1 (Own Risk and Solvency Assessment (ORSA) for AIs), against the risk appetite and risk limits of the AI.
- The risk management function must assess the appropriateness of policies, processes, and controls in respect of risk management and the effective monitoring thereof by the AI.
- The risk management function must:
  - regularly provide written reports to Senior Management, other key persons in control functions and the Board of Directors on the AI's risk profile and details on the risk exposures facing the AI and related mitigation actions as appropriate;
  - document and report material changes affecting the AI's risk management system to the Board of Directors to help ensure that the system is maintained and improved; and
  - have access to and report to the Board of Directors or a committee of the Board identified by the Board of directors on the strategy of the risk management function and information on its resources, including an analysis on the appropriateness of those resources.

### 1.4. AML/TF Risk Management and Compliance Programme

This RMCP is a documented record of MMLL AIs compliance and control measures and efforts that satisfies the obligations under the FICA Act on a "risk sensitive" basis.

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

- Develop, document, maintain and implement a RMCP for each AI;
- Incorporate all the elements of the FICA Act, regulations and Guidance Notes that are linked to CDD.
- Describe the application and implementation of measures of the AI's risk-based approach that will as a minimum include: -
  - The end-to-end CDD process, i.e., from establishing a business relationship, onboarding a client, engaging in transactions, 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.
  - Measures to deal with suspicion formed of ML, TF or PF activities formed post client onboarding; and
  - Measures to prevent entering into, or maintaining business relationships, or concluding transactions if an AI cannot perform CDD and the manner in

which an AI will terminate an existing business relationship when unable to complete CDD requirements, etc.

- Description of implemented governance processes; related to executing reporting obligations, training programs, monitoring programs etc.

**Checklist for an effective business specific RMCP must include the "how" or "manner" in which:-**

- How an AI identifies, assesses, monitors, mitigates and manages ML/TF/PF risk?
- How an AI determines if person is a prospective/existing client?
- How an AI ensures no anonymous clients?
- How an AI identifies and verifies different types of clients and why?
- How an AI determines if future transactions consistent with AI's knowledge of prospective client?
- How an AI conducts additional due diligence for legal persons, partnerships and trusts?
- How an AI conducts ongoing due diligence and account monitoring?
- How an AI examines and keeps written findings of complex/unusually large transactions and unusual patterns of transactions/which have no apparent business/lawful purpose?
- How an AI will confirm information relating client where there are doubts about veracity of previously obtained information?
- How an AI will perform CDD in course of business relationship where AI suspects the veracity /transaction is suspicious?
- How an AI will terminate existing business relationship if unable to conduct CDD?
- How an AI determines if prospective client is a DPEP/FPEP/DPIP?
- How an AI conducts enhanced due diligence for high-risk relationships and when simplified CDD may be permitted?
- How and where records are kept?
- Enables an AI to determine if transaction/activity is reportable to the FIC?
- Provides process for reporting information to the FIC.
- How the RMCP is implemented in branches, subsidiaries and other operations in foreign countries?
- How the AI will determine if the host country or foreign branch/subsidiary permits implementation of measures required under the FICA Act?
- How the AI implements its RMCP?

**International Business Units**

- MMLL must ensure compliance within each host country where a subsidiary is held, meaning that MMLL must adhere to both the host country's legislation and the South African standard of legislation.
- Where a resident country has weak or limited legislation MMLL must implement the minimum requirements as per South African legislation.
- Sharing of information between branches and subsidiaries.
- Establish alignment in policies and processes, within the MMLL Group.

- Ensure regular exchange and sharing of concerning matters within the Group and the resolutions/actions of the matters raised and addressed.

### 1.5. Identification of Accountable Institution

In terms of Schedule 1 of the FICA Act ***MM Life Limited*** is an AI (Schedule 1: Financial Service Provider in terms of the Long-Term Assurance Act) which is registered at the FIC, with the FIC Organisation Identity Number: **21420**

| **MOMENTUM METROPOLITAN LIFE LIMITED GROUP STRUCTURE** | | |
|---|---|---|
| **goAML Org ID** | **FIC Schedule Item** | **Name** |
| ***21420*** | ***S1I8- Long-Term Insurer*** | ***MM Life Limited T/A Momentum Metropolitan Ltd*** |
| 23671 | S1/12- Investment Advisor or Intermediaries | MET COLLECTIVE INVESMENTS (RF) |
| 11860 | S1/2- Trust Company | MOMENTUM TRUST LIMITED |
| 24021 | S1/12- Investment Advisor or Intermediaries | MOMENTUM CONSULTANTS AND ACTUARIES (PTY) LTD |
| 24022 | S1/12- Investment Advisor or Intermediaries | MOMENTUM CONSULT (PTY)LTD |
| 24016 | S1/12- Investment Advisor or Intermediaries | MOMENTUM WEALTH (PTY) LTD |
| 24017 | S1/12- Investment Advisor or Intermediaries | MOMENTUM ALTERNATIVE INVESTMENTS (PTY) LTD |
| 24018 | S1/12- Investment Advisor or Intermediaries | MOMENTUM ASSET MANAGEMENT PTY LTD |
| 21220 | S1/5- Unit Trusts (Collective Investment Schemes Managers) | MOMENTUM COLLECTIVE INVESTMENTS (RF) LIMITED |
| 24020 | S1/12- Investment Advisor or Intermediaries | EQUILIBRIUM INVESTMENT MANAGEMENT LIMITED *(Prev: Momentum Investment Consulting)* |
| 25132 | S1/12- Investment Advisor or Intermediaries | MOMENTUM OUTCOME-BASED SOLUTIONS PTY LTD |
| 25871 | S1/12- Investment Advisor or Intermediaries | MOMENTUM HEALTHCARE DISTRIBUTION (PTY) LTD |
| 25985 | S1/12- Investment Advisor or Intermediaries | MOMENTUM CONNECT (PTY) LTD |
| 23883 | S1/12- Investment Advisor or Intermediaries | MM Life Limited T/A Metropolitan Ltd |
| 50288 | S1I19 - Cross-border Money or Value Transfer Services Provider | MOMENTUM MULTIPLY (PTY) LTD |
| 24975 | S1/12- Investment Advisor or Intermediaries | METROPOLITAN FRANCHISE (PTY) LTD |

| | | |
|---|---|---|
| 54608 | Insurance Company | MOMENTUM METROPOLITAN LIFE (BERMUDA) |
| 54407 | S1/2- Trust Company | ISOBELO TRUST |
| 38019 | S1/12- Investment Advisor or Intermediaries | MOMENTUM WEALTH INTERNATIONAL LTD |
| 37501 | S1/12- Investment Advisor or Intermediaries | MOMENTUM GLOBAL INVESTMENT MANAGEMENT |
| 25552 | S1/12- Investment Advisor or Intermediaries | MOMENTUM SECURITIES (PTY) LIMITED |
| 21127 | S1I4- Authorised Users of an Exchange | MOMENTUM SECURITIES (PTY) LIMITED |
| 21131 | S1I20 - High Value Goods Dealers - Kruger Rand Dealers | MOMENTUM SECURITIES (PTY) LIMITED |
| 40649 | S1/11-Money Lender Against Securities | MOMENTUM SECURITIES (PTY) LIMITED |
| 21365 | S1/8- Long-Term Insurer | GUARDRISK LIFE LIMITED |
| 21421 | S1/8- Long-Term Insurer | MOMENTUM ABILITY LIMITED |
| 37067 | S1/12- Investment Advisor or Intermediaries | GUARDRISK ALLIED PRODUCTS & SERVICES (PTY) LTD |
| 54256 | S1/8- Long-Term Insurer | GUARDRISK MICROINSURNACE LIMITED |
| 49424 | BE - Business Entity with a Reporting Obligation in terms of Section 29 of the FICA Act | GUARDRISK INSURANCE COMPANY LIMITED |

Under the provisions of Section 42A(2) of the FICA Act, ***MM Life Limited*** and Metropolitan Life International Services Limited, has appointed a competent Anti-Money Laundering Compliance Officer (**MLCO**), namely:

Douw Lotter
Head: Group Forensic Services and Anti-Money Laundering Solutions
268 West Avenue, Centurion, 0157
PO Box 7400, Centurion, 0046
Tel: 012 673 7669, Fax: 012 663 5735
E-mail: mailto: dlotter@mmltd.co.za

(See Curriculum vitae attached, marked Annexure 13.)

**Reporting Officer:**

Charlotte Archer
Anti-Money Laundering Solutions Specialist
Group Forensic Services
268 West Avenue, Centurion, 0157
PO Box 7400, Centurion, 0046
Tel: 012 673 7348, Fax: 012 663 5735
E-mail: charlotte.archer@mmltd.co.za

**Functions of Group Anti-Money Laundering Solutions**

**Responsibility of Group Forensic Services (GFS) and Anti Money Laundering (AML) Solutions**

GFS and AML Solutions will assist business in implementing a standardised MMLL and individual business processes and controls to mitigate ML/TF/PF risk across MMLL.

**Responsibility of Reporting Officer(s)**

The Money Laundering Reporting Officer (MLRO) has a responsibility and authority to monitor and maintain all the AI information on the go-AML messages board and to *inter alia* complete and submit intelligence reports to the FIC via go-AML web reporting tools that includes reports relating to cash receipts (above the regulated amount), suspicious and unusual transactions activities, transactions or activities relating to financing of activities linked to terrorism as well as responding to specific requests from the FIC.

**Responsibility of Money Laundering Compliance Officer (MLCO)**

Section 43(b) of the FICA Act requires all AIs to appoint a MLCO, which it appointed by the AI's Board of directors, with the responsibility to ensure compliance by the AI and its employees with the obligations imposed by the provisions of the FICA Act.

The MLCO should be sufficiently competent and have seniority to assist the Board(s) and Senior Management in discharging their obligations under the FICA Act.

The MLCO will be responsible for:

- Ensuring that an appropriate AI specific AML Risk Management and Compliance Program is in place and adhered to by business.
- Ensuring that ongoing monitoring and reporting transpires within each business area to establish the effectiveness and efficiencies of the RMCP.
- Ensuring corrective action is enforced where weak and unsteady processes were identified.
- Providing independent oversight and guidance to business in respect of the AML Risk Management Compliance Program; and
- Providing independent assurance to the board and other stakeholders on the effectiveness of the management of AML compliance risk.

**FIC Reporting obligations:**

The MMLL Group MLCO and MLRO within GFS, are responsible for assisting the FIC with any requests submitted by the FIC to MMLL, in terms of Sections, 27, 32, 34 and 35 of the FICA Act.

The MLCO and MLRO are also responsible in submitting reports as defined in Sections 28, 28A and 29 of the FICA Act.

All matters relating to Section 29 of the FICA Act, must be reported to the MMLL MLRO, as soon as possible of discovering or identifying the matter as suspicious. The MMLL MLRO, must submit a Section 29 report to the FIC, via the go-AML tool, **as soon as possible** but **not later than 15 (fifteen) days** after a natural person has **become aware of a fact** concerning a transaction based on which knowledge or a suspicion concerning the transaction must be reported, unless the FIC has approved of the report being sent after the expiry of this period.

Emphasis must be placed on submitting a report under section 29 of the FICA Act, as soon as possible after a person became aware of the facts which give rise to a suspicion. In terms of regulation 24(3) of the MLTFC Regulations this period must not be longer than 15 (fifteen) days, excluding Saturdays, Sundays and Public Holidays, as this it will enable the FIC to assess and act on the most recent and accurate information, which could enable the FIC to place a block on a transaction, if so required.

**Note: Please refer to the attached addendums for the complete business processes, which are implemented when receiving and submitting reports to the FIC, by the MLRO.**

**Group AML Solutions** provides AIs with various operational tools to enable compliancy to the FICA Act, namely: - a Key Risk Indicator System (KR1S Ukwazi), Refinitiv\World-Check and by assuming the FIC reporting obligations to the FIC.

**KR1S:**

KR1S is a web-based application. User access is restricted to particular user groups, where segregation of duties rules is always adhered to. User access is monitored and reviewed, quarterly.

The Users of the KR1S Ukwazi application are set up to receive text and/or email alerts for any relevant/new exceptions that are added to reports.

The creation of reports are based on “jobs” read from various data sources in MMLL. The results, in the form of exception reports, are presented in the KR1S Ukwazi Application.

KR1S is a continuous auditing solution that ‘sits-on-top’ of source data and extracts exception reports based on specifications received from business.

These exception reports are scheduled to run on a continuous basis, at pre-determined timeslots and at any defined frequency; minutely, hourly, daily, weekly, monthly, yearly etc.

KR1S is used for various functions, as per the specifications set by an AI, for example, it can: -

- Extract of scheduled jobs;

- Monitor external services for alerts relating to any failures or anomalies;
- Job Monitoring Service;
- Alerts generated by the monitoring service;
- Email Header for the alerts generated;
- Report alerts managed using KR1S;
- Auditing tool for internal and external auditors and regulators.

(The list of functions delivered by KR1S is infinitive.)

Users are able to clear any exceptions found via the KR1S Ukwazi Application (e.g., from red to green).


| REPORTDATE | DP_TYPE | POLNO | CRCRNO |
|---|---|---|---|
| 2020-03-13 | DPS | HM 30758871 | 16622 |
| 2020-03-13 | DPS | HM 30758871 | 21977 |
| 2020-03-13 | DP | GE 85974335 | 39368 |
| 2020-03-13 | DP | GE 85974335 | 40079 |
| 2020-03-13 | DPO | 01 8049409 | 163799 |
| 2020-03-13 | DPS | SL 96889656 | 11856 |
| 2020-03-13 | DPO | 01 8049409 | 40075 |
| 2020-03-13 | DPS | 204476202001 | 20678 |
| 2020-03-13 | DPO | SL 29148998 | 357 |
| 2020-03-13 | DPS | 204476202001 | 21164 |
| 2020-03-12 | DPO | SL 42169750 | 316381 |
| 2020-03-12 | DPO | SL 42169750 | 40017 |
| 2020-01-15 | DP | 87909495 | 562437 |
| 2020-03-12 | DP | 87909495 | 562437 |
| 2020-01-15 | DP | 87909495 | 562436 |
| 2020-03-12 | DP | 87909495 | 562437 |
| 2020-03-12 | DPS | HM 31744461 | 12600 |

KR1S is partnered with on-premises I&O database administrators who, monitor and back-up the MMLL KR1S Servers, on a daily basis.

MMLL has a strong foundation of business continuity processes in place, should any infrastructure failures be experienced. These infrastructure failure alerts are managed by I&O and are forwarded to the KR1S administrators, immediately.

**Refinitiv/World-Check:**

MMLL has since 2007, utilised the services of World-Check, to assist MMLL to meet regulatory obligations, make informed decisions and prevent MMLL being used for ML, TF and PF activities. Refinitiv the current owner relies on the structure of the World-Check risk intelligence functionalities. Combined with screening software applications, ensuring a screening solution that is cost effective and delivers fast, reliable results. Refinitiv/World-Check is used by MMLL in support of its AML/CTF functions to *inter alia* to identify DPEPs, FPEPs, DPIPs and individuals linked to criminal activities and untoward behaviour.

Refinitiv/World-Check gathers and delivers accurate and reliable information, from across the globe, adhering to the stringent research guidelines, as they collate information from

reliable and reputable sources – such as watch lists, government records, sanctions lists and media searches.

The Refinitiv/World-Check data is fully structured, aggregated, and de-duplicated.

MMLL has recently selected a more a modernized offering for sanction screening from Refinitiv, namely their World-Check One facility, in which an Application Program Interface (API) is used for screening during the onboarding of new business and other trigger events. At minimum the screening for both initial and for Ongoing screening (OGS) and should include the client's (individual or organisation) full name. OGS is managed via the World-Check One portal.

Auto resolution is applied for both initial and OGS. Where possible matches are deemed as false these are auto resolved and the audit trail is kept. Auto resolution is done based on the following secondary identifiers, where these identifiers are available on both the client data as well as the World-Check entry:

- Individuals
    - Country location
    - Place of birth
    - Citizenship
    - Gender
    - Date of birth
    - Identification number

- Organisation
    - Company registration number

Each AI is responsible to screen and monitor their clients for the sanctions screening.

**Refinitiv/World-Check coverage includes:**

- PDPEPs/FPEPs/DPIPs), close associates, and family members;
- State owned entities and state invested enterprises;
- Global sanctions lists;
- Narrative sanctions (sanctions ownership information);
- Global regulatory and law enforcement lists;
- Negative media;
- Iran economic interest (IEI);
- US SAM;
- Targeted Financial Sanctions lists;
- Vessels information; to name a few.

(A complete list of sanctions screening and other lists of importance utilized within the World-Check One screening facility is attached as a separate addendum.

Please refer to the attached addendums for additional information relating to the specific criteria used, to identify DPEPs/FPEPs/DPIPs and persons closely associated with them.

## 2. A RISK BASED APPROACH TO MANAGE AND COMPLY WITH THE FICA ACT

The FICA Act stipulates a **Risk Based Approach** in the AML/CTF regulatory framework. The risk-based approach requires an AI to understand its inherent and specific exposure to money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks and to establish a reasonable RMCP to manage the risks of ML, TF and PF, with the intent to protect and maintain the integrity of the South African financial system.

A risk-based approach allows for flexibility to exercise judgment in determining the extent and nature of for example CDD measures that are to be imposed on clients by AIs. It is thus important to realise that various sectors in the financial services industry – whether in terms of products/services or delivery channel or typical customers, can differ materially. An approach to preventing ML, TF and PF that is appropriate in one sector may be inappropriate in another. A financial services business should be able to take such an approach to the risk of being used for the purposes of ML, TF and PF and to ensure that its policies, procedures and controls are appropriately designed and implemented and are effectively operated to reduce the risk of the financial services business being used in connection with ML, TF and PF.

Applying a risk-based approach ensures that AIs can implement measures that are proportionate within the ML/TF/PF risks involved. The systems and controls by which an AI decides to manage ML/TF/PF risks and the levels of due diligence it chooses to apply in relation to various risk levels must be documented.

To assist the overall objective **to prevent the abuse** of the financial services sector a **risk-based approach** must:

- Recognise that the ML/TF/PF threat to a financial services business varies across its customers, countries/territories, products/services and delivery channels.
- Allow the Board and Senior Management to differentiate between their customers in a way that matches the risk in their particular business.
- Allow the Board and Senior Management to apply their own approach to the policies, procedures and controls of the financial services business in particular circumstances.
- Help to produce a more cost-effective system.
- Promote the prioritisation of effort and activity by reference to the likelihood of ML, TF or PF taking place.
- Reflect experience and proportionality through the tailoring of effort and activity to risk; and
- Allow a financial services business to apply the RMCP sensibly and to consider all relevant factors applicable and not only consider a single factor.

The general principles of a **Risk Based Approach** are: -

- Risk identification and assessment – taking account of the customer and the business relationship or occasional transaction and of the product/service/delivery channel to identify the ML, TF and PF risk to the financial services business.
- Risk mitigation – applying appropriate and effective policies, procedures and controls to manage and mitigate the risks identified.
- Risk monitoring – monitoring the effective operation of a financial services business' policies, procedures and controls; and
- Policies, procedures and controls – having documented policies, procedures and controls to ensure accountability to the Board and Senior Management.

**An AI must always provide the grounds on which it can base its justification for a decision that an appropriate balance was struck, in any given circumstance**.

The following must be considered and abided by the AI: -

**Technical compliancy of the AI's RMCP:**

- Affirm that the AI's RMCP complies with Sections 20A-21H and Section 42 of the FICA Act.

**Soundness Test:**

- Test that risk assessments consider the sense of risk ratings and factors awarded.
- That ML/TF/PF risks are effectively mitigated.
- That enhanced/simplified due diligence processes are sufficient.
- That the AI's risk-based approach caters for high, medium and low risk clients.

**Effectiveness of compliance:**

- Testing must be done to ensure that the AI follows their own RMCP.
- Consideration must be given to the AI's RMCP to ensure alignment with the relevant sector's RMCP.
- That the AI complies with the minimum requirements of a risk-based approach.

## 3. CLIENT IDENTIFICATION: ESTABLISHING A RELATIONSHIP AND CLIENT ONBOARDING

**Establishing a relationship** with **a client** is the process where a client approaches or is approached by an AI, either with or without the intention, to establish a business relationship or to conclude a single transaction regarding the offering by an AI of a service or product.

CDD starts with the AI knowing the identity of its client. In terms of section 21 of the FICA Act an AI must, while establishing a business relationship or entering into a single transaction, establish and verify **the identity of the client** and, if applicable, **the person representing the clien**t as well as **any other person on whose behalf the client** is acting.

The objective of this provision is that an AI, after applying its processes to establish and verify a client's identity, should have confidence that it knows who the client is with sufficient certainty.

An AI is required to understand the nature of the client's business and understand the ownership and control structure of the client. This will enable the AI to identify and take reasonable steps to verify the beneficial owner(s), thereby reducing the heightened risk when dealing with legal persons, trusts as partnerships, by mitigating the risks.

**IMPORTANT NOTE:** In terms of Exemption 4, an AI could previously rely on a certificate issued in terms of the regulations to the 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 MMLL 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 MMLL AI follows a CDD process and obtain all relevant CDD documentation. Therefore, in those cases where a MMLL AI does not have CDD information and documentation on record, a full CDD process will be required for all investment instructions, new business, ad hoc investments etc. **A business relationship is defined as an agreement between the client and the AI for the purpose of concluding transactions on an ongoing basis.**

A **Single Transaction** is a once off or occasional transaction where there is no expectation on the part of the client or AI that the engagement would recur over a period of time, and where the value of the transaction does not exceed R5 000-00 (five thousand Rand).

When establishing a business relationship AIs will obtain at the onboarding stage, and on an ongoing basis, information which will enable the AI **to determine whether the current and future transactions** that will be performed during the business **relationship are consistent with the knowledge** of the prospective or existing client information **regarding sources of wealth and sources of funding.**

**Client onboarding, post client identification,** is the start of the **CDD** a process where information and documents are obtained which are required to assist the AI to mitigate ML/TF/PF risks before the AI eventually accepts a mandate to conclude either a single transaction or establish a business relationship.

## 4. CUSTOMER DUE DILIGENCE

The CDD process is defined as the reasonable ongoing steps taken by an AI to know its prospective clients, persons acting on behalf of its clients or the client acting on behalf of another by *verifying* the identity of the prospective client(s), risk rating the client(s), establishing and *verifying* the source of wealth of the client(s) and the source of funds of each transaction, before concluding a single transaction or establishing a business relationship.

Certain prospective clients, especially related to their risk rating may have additional requirements imposed on them prior to or during a business relationship or related to a transaction.

**According to Section 20A of the FICA Act, an AI may NOT establish a business relationship or conclude a single transaction with an anonymous client or a client with an apparent false or fictitious name.**

### 4.1 Identification of Clients/Persons Acting on Behalf of Clients

**A client** is defined as a person (natural, legal or otherwise) who enters a business relationship or a single transaction with an AI.

A person **acting** on behalf of a client is normally the person introducing the prospective client to an AI or is acting on behalf of a client in terms of a mandate from a client or based on a contractual arrangement between the person and the AI. Examples would include intermediaries who supplied financial advice and assistance to clients and who maybe in their own right is an AI.

**IMPORTANT NOTE: A person acting on behalf of a client is deemed for the purposes of this RMCP a "client" and all CDD processes would be applicable to such persons**.

**CDD processes pertaining to nominated beneficiaries and Second Life/Co- Assured, as role-players on policies/contracts: -**

The meaning of the term *beneficiary* in the FATF Recommendations depends on the context:

- In trust law, a beneficiary is defined as the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period, which is usually referred to in the trust deed, as the trust period.

- In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy.

A contract owner can nominate and change beneficiaries throughout the lifespan of a long-term insurance contract. In this regard MMLL would each time be obligated to implement the CDD processes on each new beneficiary, who are not clients of MMLL or has not entered a business relationship with MMLL. This would create additional complications and delays in administering CDD on such persons/entities which are deemed to have no influence on the contract or the proceeds thereof until the insured event occurs.

MMLL's stance is that it does not enter into a business relationship, with either a beneficiary or a Second/Co Life Assured, at onboarding stage and thus no additional CDD details or documents are required, on the notification of a nominated beneficiary.

MMLL acknowledges the Directive issued by the Prudential Authority, dated 15 December 2022, and as such, MMLL will follow a risk-based approach at nomination of a beneficiary and before proceeds are paid at claim stage.

MMLL will as part of the CDD processes obtain minimum, identification particulars of the beneficiary of life insurance policies, as soon as a beneficiary is identified, designated, or amended by the client, for example, the detail required when nominating a natural person as a beneficiary, is the person's full names, identity number (or at least date of birth), relationship, and percentage of the funds due to him upon claim stage. In the event of a legal person, the requirement would be the legal person's full names, registration number and percentage due upon claim stage.

At nomination stage, these details must be verified against a trusted third-party service provider to verify the existence of the person or entity, as a valid person or entity in the event of a legal person.

**A nominated beneficiary on a long-term insurance contract** is only regarded by MMLL as the AI's client, when the beneficiary **has a vested claim against the insurance product**. The payment of the policy proceeds in terms of an insured/ claim event to the nominated beneficiary serves as the conclusion of a single transaction. **MMLL will therefore only enter a business relationship with a beneficiary, when this specific trigger event takes place**. For example, if the life assured on a life insurance contract dies, the funds will be payable to the nominated beneficiary, in terms of the contract and the AI will implement its CDD process.

In respect of a beneficiary that is identified as a specifically named natural person or a legal person, a risk assessment and CDD measures must be conducted in accordance with the FICA Act on such named natural and legal persons, before actual proceeds of the policy is paid to the beneficiary. This CDD process must include the screening of the beneficiary against the Financial Targeted Sanctions list.

MMLL also does not have a business relationship with a Second/Co Life Assured on an **investment contract**. The nomination of such a role player does not necessarily mean that the Second Life/Co- Assured, becomes the new owner of the investment, when the first life assured dies. **It merely allows for the investment to continue until the set maturity date.** At such a time the ownership will be determined by the last will and testament of the original owner or by the appointed Executor of the Late Estate. It is only then that MMLL will apply the required CDD process, before entering a business relationship or concluding a single transaction, with its new client.

It must be noted, that in the event when a beneficiary is nominated **on a retirement product** of a client, the funds allocated to the nominated beneficiary will only be paid to the beneficiary, post an insured event (death) when it has been determined if the deceased client did not have persons that were dependent on the client. Only once the status of

such persons has been considered, a CDD process will have to be applied on the dependents identified or in the alternative, a nominated beneficiary if applicable, may funds be paid.

**CDD processes on Trust Beneficiaries**

As specified in the FICA Act, **a CDD compliance checklist** has been created for trusts. AIs are required to obtain all the relevant details, information and documents noted on the checklist, including the identification of the trust beneficiaries and confirmation of their physical addresses.

It has been decided that only once the insured event as per a contract or as per the Trust Deed takes place and in which instance the funds are due to a beneficiary or a trust beneficiary, will the AI implement the full CDD process, before entering into a business relationship or conclude a single transaction, with a beneficiary.

An AI is obligated to determine the type of client that it engages with, especially with the focus on identifying clients with a **Higher Risk** profile.

AIs will firstly determine in which category the prospective client falls; which categories include:

- Natural person or sole proprietor.
- Closed Corporation.
- Partnership.
- Listed Company.
- Private Company.
- Foreign Company.
- Trusts.
- Other Legal Persons: Stokvels/churches/clubs/schools/municipalities, homeowner associations/body corporates, etc.

In addition to determining the category of a client an AI will determine the risk profile of clients to establish whether a client is a **Low, Medium or High-Risk client**.
Ideally the AI should provide more than a single reason per risk factor, to motivate the conclusion of a client's risk rating.

The AI should steer away from a general statement that the factor is a low risk for money laundering unless they refer to a finding within the sectors or national risk assessment.

Each AI, has available a **Client Risk Matrix**, which will assist AI's (See **individual RMCP's specifically developed and documented for Momentum Life, Metropolitan Life, Momentum Investments and Momentum Corporate**) in determining a client's risk level depending on:

- Product type;
- Client type;

- Nature of the client's business;
- Source of Income or Wealth/Source of Funds (Funds used to transact);
- DPEP/Family members and known close associates;
- DPIP/Family members and known close associates;
- FPEP/Family members and known close associates;
- Transactional client history;
- Client's existing profile;
- Type of Engagement channel.

**Clients** will **be re-evaluated from time to time** depending on the particular risk factors and appropriateness of previous risk-ratings. Specific trigger events or risks will determine the intervals at which this will be done.

Post the **identification and verification of a client(s) identity** an AI must perform the profiling of client(s) and would need to determine the following basic elements: -

- Social status (e.g. DPEP/DPIP/FPEP);
- Economic status (Occupation/Employment);
- Micro-environment (in which areas perform payments and payments of cash);
- Criminal history (based on online data and public information);
- Nature and intended purpose of the business relationship;
- Resident or Non-resident;
- Sanction lists;
- High risk countries; and
- Face-to-Face or non-face-to-face interaction.

**Clients can be classified as:**

1. Low Risk (*Simplified CDD*)
2. Medium (*Standard CDD*)
3. High (*Enhanced CDD*)

**1. <u>Classification of Low-Risk clients (Simplified CDD) if:</u>**

- The identity and sources of wealth of the individuals and entities can be easily identified.
- Transactions in client's accounts conform to the known client profile.
- Engaging in products with an inherent low risk from money laundering and financing terrorism point of view, e.g., assurance products that include risk cover without significant investment portions; and/or
- Employees whose salary structures are well defined.

These clients qualify for **Simplified CDD (Low Risk)** as these clients pose a lower-than-average ML/TF/PF risk to the AI. This risk profile will arise from a predominance of low risk factors being present in the client's profile. The client's risk profile may be elevated, dependent on further information, or any reports which may arise on the client's transactional behaviour.

The AI may therefore apply a Simplified Due Diligence Verification Standard with less stringent due diligence measures.

A client's identification information will be subject to an independent verification check performed by the AI against a credible vendor. In order for the AI to proceed with the application, the client will be required to provide minimum information as prescribed by the FIC. If the AI is unable to do an independent verification/E-verification, a client will then be required to provide copies of verification documents as per the appropriate CDD checklist.

The client will as a minimum also be subject to a World-Check screening process to determine their status with regards to UNSEC1267 security lists and possible status as FPPO and DPIP (this will include PEP statuses).

## 2. Classification of Medium Risk clients (Standard CDD):

This classification will be applicable to the majority of clients and relates to clients which are not deemed to be high risk clients.

Clients qualifying for Standard CDD (Medium Risk) are those clients who pose an average ML/TF/PF risk to the AI. This risk profile may arise due to a mixture of high, medium and low risk factors being present in the client's profile or the presence of a majority of medium risk factors. The client's risk profile may be lowered or elevated dependant on further information, or any reports which may arise on the client's transactional behaviour.

Until such time as the information available on existing clients is sufficient to allow for a risk rating, the majority of existing clients will be treated as medium risk clients.

In cases where the AI does not have CDD information and documentation already on record, a full CDD process will be required for all investment instructions, new business, ad hoc investments etc.

**The Medium Due Diligence Verification standard is the following:**

In order for an AI to proceed with the application, the client will be required to provide at a minimum the following information as listed in the checklist of MML and its subsidiaries. In addition to the provided information, a client will be required to provide **copies of identification and other verification documents,** as per the CDD compliance checklists.

**Additional CDD processes may include:**

- At the AI's discretion a client could also be subjected to an independent verification check performed by the AI against a credible vendor.
- The client will as a minimum be subject to a World-Check screening to determine their status with regards to UNSEC security lists, Targeted Financial Checklists and possible status as DPEP/FPEP/ and DPIP (this will include PEP statuses).

- The aforementioned screening is implemented on all contract owners (natural persons and legal entities) and related parties connected to a business relationship or transaction.

3. **<u>Classification of High-Risk clients (Enhanced Client Due Diligence):</u>**
   These clients will be categorised based on applying strict criteria. The criteria considered for these assessments includes: -

   - Client profile risk.
   - The country of origin.
   - Product or service type.
   - Nature of the business relationship taking in account the source of wealth and source of funds.

**High-Risk Clients identified based on their Profile**

Clients qualifying for Enhances CDD (High Risk) pose a high to significant ML/TF/PF risk to the AI. Their risk rating stems from the presence of a majority of high-risk indicators on their profile, the presence of an automatic high risk rating indicator, or as a result of investigations into their transaction behaviours, which investigations resulted in a high-risk rating to be assigned to the client.

Clients with a higher risk from a ML/TF/PF point of view are clients whose activities can fall in one or more of the following criteria:

- Interaction with a client(s) occurs in one of two manners namely: on a face-to-face or on a non-face-to-face basis. A client that engages and/or is engaged by an AI based on a non-face-to-face-interaction is naturally deemed a higher risk, client except where reasonable mitigated circumstances exist.
- Significant and unexplainable geographic distance between the entity that would perform the activity and the place of residence or the seat of the client.
- Frequent and unexplainable movements of assets between accounts in various financial institutions.
- Frequent and unexplainable cash flows between financial institutions in different geographic areas;
  - Clients for which is difficult to identify the real owner (offshore companies).
  - Cash activities that include or originate from: -
    - Activities that offer money services (remittances, exchange of foreign-exchangeable operations, services for fast money transfer, as well as other activities offering money transfer)
    - Casinos, betting shops and other activities related to the games of chance;
    - Activities which in regular business operations are not in cash, and which generate large amounts of cash for certain transactions.
- Charity organisations and other “non-profit” organisations which are not subject of a control (especially acting across borders).

- Bank accounts of accountants, lawyers or other professionals who act in the name of their clients, who by the financial institutions are treated as VIP clients.
- Clients using non-resident accounts, especially as an opportunity for assets transfer across borders.
- Using mediators within the business relationship which are not subject to the regulation for prevention of money laundering and financing terrorism and is not supervised; and
- Using corporate mediators or other structures to unnecessarily increase the complexity and decrease the transparency.

**Enhanced Due Diligence Verification Standard**

The client will be required to provide at minimum information and requirements as per the appropriate CDD checklist. In addition to the provided information a client will be required to provide verification documents, as per the appropriate CDD checklist.

**Additional Requirements include:**

- The client will also be subject to an independent identification verification check performed by the AI against a credible vendor.
- Should any independent verification checks highlight a discrepancy with the information provided by the client, the AI will be required to engage the client to obtain further information.
- The client will as a minimum standard, be subject to a World-Check screening to determine their status with regards to UNSEC security lists and possible status as DPEP/FPEP and DPIP (this will include PEP statuses).
- The search will be done on all contract owners and related parties connected to a business relationship or transaction.
- Due to the high-risk nature of the client, certain additional due diligence measures will be taken. At onboarding, an internet search will be conducted on the client to determine whether his stated profile on the mandate is in line with the client's internet footprint.
- The client take-on for High-Risk clients, who are indicated as DPEP/FPEP/DPIP, will have to be signed off by two (2) members of the AI's Senior Management.
- The business should not seek to de-risk the engagement 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.
- The client will form part of an on-going monitoring exercise wherein the transaction pattern of the client will be compared to the client's profile.
- The following client categories will normally be regarded as clients with a higher risk profile: -
  - Closed Corporation.
  - Partnership.
  - Listed Company.
  - Private Company.

- Foreign Company.
- Trusts.
- Other Legal Persons: Stokvels/churches/clubs/schools/municipalities, homeowner associations, etc.
- Natural Persons who are FPEPs/Family members and known close associates.
- Natural Persons who are DPIPs/Family members and known close associates.
- DPEPs.

**a) Enhanced Client Due Diligence**

AIs are deeming Partnerships, Closed Corporations, Private Companies, Listed Companies, Trusts, FPEPs, DPIPs, Family Member or Known Close Associate of or DPIPs and DPEPs, **as clients with a potential higher risk profile**.

This **Enhanced Client Due Diligence (ECDD) process** is required to mitigate increased risk and therefore additional requirements are imposed in verifying the client's identity, status, source of funds, source of wealth etc. These checks are approportionate to the level of risk identified and provide confidence that any risk has been mitigated and that the risk is unlikely to materialise.

The **appropriate CDD checklist**, in which all the relevant requirements are indicated, must be used for the specific role-player type.

### 4.1.1 Enhanced Client Due Diligence Process: Partnerships

Partnerships are not legal incorporated entities and do not have legal personalities as it is only established by a mutual agreement between natural persons and liability is embedded with the individual persons.

### 4.1.2 Enhanced Client Due Diligence for Legal persons, Closed Corporations, Private Companies Listed Companies, FPEP, DPIP, Family Member or Known Close Associate of FPEP or DPEP or DPEP.

A **legal person** is any person, other than a natural person that establishes a business relationship or enters a single transaction with an AI and includes a person incorporated as a Private Company, Close Corporation, foreign company or any other form of corporate arrangement or association which excludes a trust, partnership or sole proprietor.

### 4.1.3 Enhanced Client Due Diligence: Beneficial ownership

**It is of paramount importance that the Beneficial Owner in respect of the legal person** is **identified.**

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

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

The definition of "beneficial owner", was amended to ensure that the definition encapsulates every natural person who is a beneficial owner of a client that is a legal person, partnership or trust. This is to establish the "look through principle" which means:-

- *A natural person who directly or indirectly—*
    - *Ultimately owns or exercises effective control of*
        - *A client of an AI; or*
        - *A legal person, partnership or trust that owns or exercises effective control of a client of an AI; or*
    - *Exercises control of a client of an AI on whose behalf a transaction is being conducted; and*

      *Includes: -*
        - *In respect of legal persons, each natural person contemplated in section 21(B(2)(a);*
        - *In respect of a partnership, each natural person contemplated in section 21B(3)(b);*
        - *In respect of a trust, each natural person contemplated in section 21B (4)(c),(d) and (e).*

Section 21B is amended to provide for instances where -

- other legal persons, partnerships or trusts exercise ownership or control over the legal person.
    - the partners in the partnership or, in the case of trusts, if the founders, trustees or beneficiaries are legal persons.

**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 will take reasonable measures to identify the beneficial owners and verify the identity of the beneficial owners, until reasonably satisfied that the AI knows the individual(s) who ultimately owns or controls a client and/or the individual on whose behalf a transaction is conducted.

This means that information will be obtained to identify direct and indirect ownership and/or control over specific percentage of shares or voting rights; or control over the management and their actions will.

“Control” in this sense is distinguished from mere signature authority or legal title (Ownership)

AIs must:

- Understand the substance and form of the legal person;
- Understand the reason for the transaction and source of funds;
- Identify individuals behind the institution, not only shareholding, member’s interest, or member share, but **control; and**
- Ensure that individuals purporting to act on behalf of the entity are authorised to do so.

A natural person can exercise effective control over a legal persona in different ways, including:

- Power of attorney
- Nominee shareholders
- Delegation of authority
- Delegated authority in terms of law (i.e., legislation and accounting officer) Court orders, etc.

The reason for understanding beneficial ownership is, that a lack of adequate, accurate and timely beneficial ownership identification facilitates ML\TF\PF by disguising:

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

The standard beneficial owner elimination process for an AI to determine who the natural person(s) is who, independently or together with another person, has a controlling ownership interest in the legal person, is to establish the following:

- 25 per cent or more of the shares with voting rights in a legal person as sufficient to exercise control of the legal person.
- 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 attached to different classes of shares or through shareholders agreements.

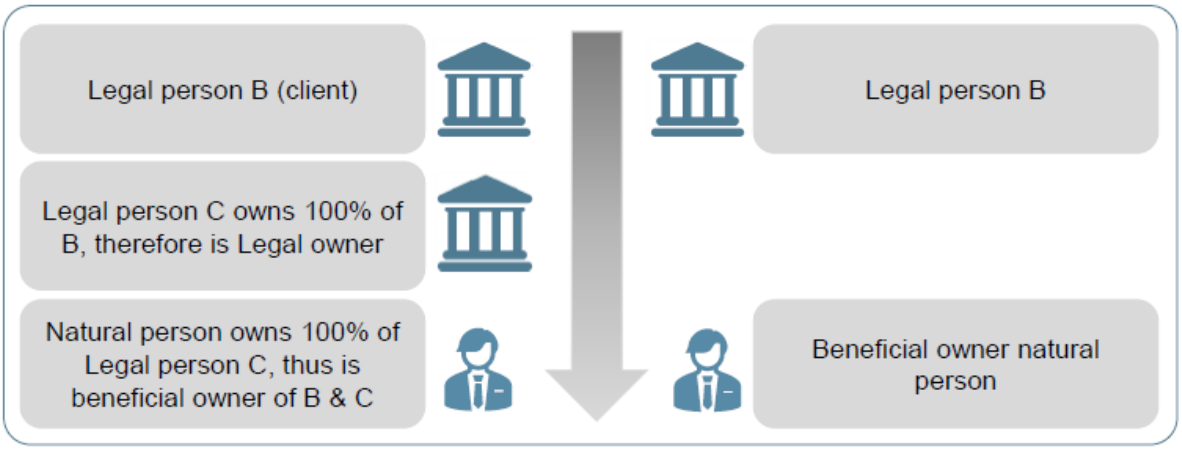
- If no natural person can be identified who exercises control through **"other means"**, the accountable institution will determine who the natural person is who exercises control over the management of the legal person, for example, in the capacity of an executive officer, non-executive director, independent non-executive director, director or manager.
- An AI will ensure that adequate, accurate and timely information of the beneficial owner and control of legal persons, are obtained and validated.
- Where legal persons are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, AIs should take effective measures to understand that they are not misused for ML/TF/PF.

**The concept of legal owner in comparison to beneficial owner.**

An AI must firstly establish the legal owner(s), in order to establish the ultimate beneficial owner(s), in other words:

If a client is a legal person, for example, a trust, a drill down into the trust's trustees, founder, beneficiaries and trust beneficiaries, needs to be conducted, if there is a further legal person, who is for example, a registered company or another type of legal entity, a further drill down is required until such time as the identities of the ultimate beneficial owner is discovered. Similar to the below process:

The legal owner of a legal person B can be legal person C, where legal person C is then owned by a natural person/s. The natural persons are the actual beneficial owners of legal person B.



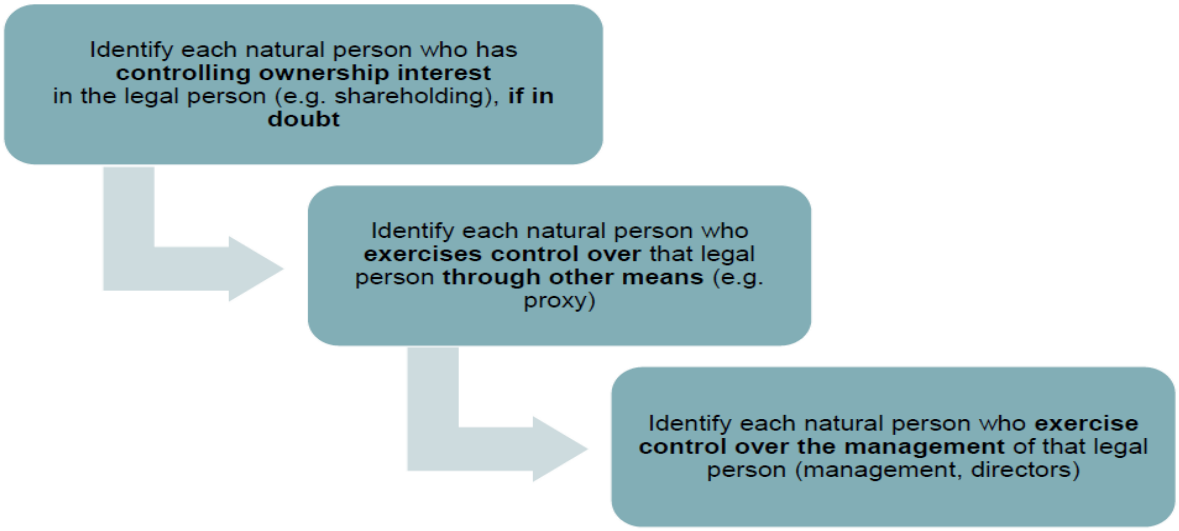

For a NPO, to make donations to individuals or organisations outside South African borders and provide humanitarian, charitable, religious, educational or cultural serviced outside South Africa's borders, the NPO needs to be registered.

The AI is required to obtain all the relevant CDD details and documents as per Sections 21, 21A, 21B, 21C, 21F, 21G and 21H of the FICA Act.

It is of importance to note that a director/person becomes "disqualified", if he is a person that has been convicted for offences in terms of the FICA Act and persons who are listed on the UNSC and TFS lists.

Thus, when an AI identifies such an individual, the AI must address the matter, as per their RMCP and if the individual is not removed from the legal entity, the AI must consider following their documented client off-boarding process.

**Beneficial ownership process of elimination:**




Where the beneficial owner of the client (a legal person, trust or partnership) is a DPIP/DPEP presenting a high ML risk or an FPEP, the requirements as set out in section 21F and 21G of the FICA Act applies to the client. The business relationship with the legal person, trust or partnership as the client would be regarded, as dealing either with a DPEP/DPIP presenting a high ML risk or an FPEP in this instance.

Trustees, founders and named beneficiaries of a trust, are all regarded as beneficial owners of the trust and as such, an AI must scrutinize their information to determine whether these beneficial owners are DPIPs/DPEPs or FPEPs.

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

### 4.1.4 Enhanced Client Due Diligence Process: Trusts

**A trust** has legal personalities. All trusts in South Africa are expressed trusts, meaning they were created during the lifetime of a person; or the trust was created in terms of a Will of a person and will come into effect after the death of that person.

A trust is a legally binding agreement between the founder of the trust (owner of assets) and the trustees. In terms of the trust, the trustees undertake to administrate the trust assets with the necessary care and diligence to benefit the beneficiaries.

**Types of Trusts**

**1. Testamentary trust (mortis causa)**

Testamentary trusts are the most common trusts in use in South Africa. They are especially suited for the protection of the interests of minors and other dependents who are not able to look after their own affairs. These types of trusts come into being only after the death of the testator.

The trust is administered by the trustees appointed in terms of the will, by the testator and is usually ended after a predetermined period or at a determined event, such as a minor turning 18 or the death of an income beneficiary. Assets that form part of the deceased's estate may be moved to this trust, with or without limited rights such as usufruct.

The trust is formed by placing a trust clause in a will, which serves the same purpose as a trust deed. During the estate settlement period of the deceased estate, the appointed trustees apply for a letter of authorisation at the same office of the Master of the High Court as where the estate is registered.

A testamentary trust may further be categorised, as either a discretionary or a vested trust.

- **Discretionary trust**
  Payment of income and/or capital is subject to the discretion of the trustees and all non-allocated income is taxable in the hands of the trust. This type of trust can therefore be used to save income tax by splitting incomes. Capital beneficiaries may only be determined at a later stage.

- **Vested trust**
  The income and capital beneficiaries are already determined and described. The income is taxable in the hands of the income beneficiary, who could also be the capital beneficiary. The capital beneficiary therefore has immediate property rights, subject to the terms of the will or Trust Property Control Act, 57 of 1988.

**2. Inter Vivos trusts (Living trusts)**

Living trusts are ideal for keeping growth assets out of your estate and are a great medium to limit estate duty and to protect assets from generation to generation. A living or inter vivos trust comes into being during the lifetime of the settlor or founder

(the person who takes the initiative to create the trust) with the signing and registration of a trust.

A living trust is formed as an arrangement between the founder/settlor and the trustees. The founder/settlor is the person who takes the initiative to create a trust.

The interested parties in a living trust are the founder/settlor, the trustees, the people or company appointed to take control of the assets and take responsibility for their administration and management; and the beneficiaries who, in terms of the Trust Act Property Control Act, are entitled to the income and/or capital of the trust.

After the trust deed has been signed off by the trustees and founder, the trust is registered with the office of the Master of the High Court in whose jurisdiction most of the assets are situated or where the administration is to take place.

**A living trust can take on several forms, namely:**

- **Family trust**
  This type of trust comes into being through an agreement between the founder and the trustees. Assets are sold to the trust and a loan account (debt) is created. Assets can also be donated to the family trust, although this carries donations tax implications. The trust may obtain other assets through purchases or an inheritance.

- **Charitable trust**
  A charitable trust is classified as non-taxable in terms of the Income Tax Act 58 of 1962. Capital loans are made to a trust, which is structured in a way that it pays no income tax. The trustees then make donations to charities, schools, churches, etc. on your behalf and according to your wishes. Since no income tax is applicable, you may make large donations.

- **Umbrella trust**
  This type of trust is linked to and used by life insurance and retirement fund group schemes. It allows unapproved funds (not governed by the Pension Funds Act 24 of 1956) to deposit death benefits to beneficiaries who are unable to handle their own affairs, to be managed on their behalf and for their sole benefit, as prescribed by the authorities and relevant legislation.

- **Guardian's trust**
  When minor children are the beneficiaries of life policy proceeds, insurers are obliged to pay this money to a natural or legal guardian to manage on the children’s behalf. If the guardian decides to use the money for other purposes, or mismanages or misappropriates it, the children will not receive the full benefit of the money they were expected to inherit. Nominating a trust is the ideal solution, as benefits payable by life policies to minor beneficiaries can be managed on their behalf, to their sole benefit, by the trustees of the trust.

- **Special trusts**
  Special trusts are taxed at the same rate as a natural person and may only be created to benefit a person suffering from serious mental illness as described in the **Mental Illness Act 18 of 1973**, or who suffers from serious physical deformity. In certain cases, testamentary trusts benefiting any living family member, of whom the youngest turns 21 (twenty-one) in a tax year, may also be classified as a special trust.

**It is of paramount importance that the Beneficial Owner of the trust is identified. The beneficial owner can be described as a person(s) whom:**

The definition for “beneficial owner” of a Trust, has been updated in the General Laws (Anti-Money Laundering and Combating Terrorism Financing Amendment Act, 22 of 2022), the definition is similar to the definition as per the FICA Act, which means:

- A natural person who directly or indirectly ultimately owns the trust property, in terms of the letter of authority from the Master of the High Court.
- A natural person who exercises effective control of the administration of the trust.
- This includes each founder, trustee, person/s authorised to act on behalf of the trust and the trust beneficiary/ies.

It is of importance to note that a trustee becomes "disqualified”, if he/she is a person has been convicted for offences in terms of the FICA Act and persons who are listed on the UNSC and TFS lists.

Thus, when an AI identifies such an individual, the AI must address the matter as per their RMCP and if the individual is not removed from the Trust, the AI must consider following their documented client off-boarding process.

### 4.1.5 Politically Exposed Persons (PEP)

A politically exposed person (PEP) is an individual who holds or has held a prominent public function. Within this position, the person has a level of influence and control over public funds, benefits, and decision-making. The abuse of such a position in office could result in corruption and bribery that may serve as a predicate offence to ML.

Although there is a heightened risk of ML associated with PEPs, it does not mean that all PEPs are linked to and engage in illicit activities.

In the South African context, the FICA Act distinguishes between 3 (three) types of politically exposed persons:

1. A **DPEP** ‘‘A domestic politically exposed person is an individual who holds, including in an acting position for a period exceeding six months, or has held a prominent public function in South Africa, as per Schedule 3A of the FICA Act, including that of—’a prominent public function including, but not limited to,

    - President or Deputy President.
    - Government minister or deputy minister.
    - Premier of a province.
    - Member of the Executive Council of a province.
    - Executive mayor and municipal managers (Financial and Tender Departments of a municipality,
    - Leaders of a political party, such as the ANC, DA or EFF, only if they have control flow of funds,
    - Member of a royal family or senior traditional leader,
    - Head accounting officer or chief financial officer of a national or provincial department or government component,
    - the municipal manager of a municipality, or
    - Chief Executive Officers and Chief Financial Officer of state entities such as Eskom, Telkom, PRASA and other
    - Chairperson of the controlling body, chief executive officer, chief financial officer or chief investment officer of a municipal entity,
    - Judges.
    - Ambassador or high commissioner or other senior representative of a foreign government based in the Republic.
    - Senior official of companies that receive certain tenders from government.
    - A member of a royal family or a senior traditional leader
    - High ranking member of the military and South African Policy Services (above the rank of major-general).

2. A **DPIP** is an individual who holds, including in an acting position for a period exceeding six months, or has held at any time in the preceding 12 (twelve) months in South Africa, a prominent public function as listed but not limited to Schedule 3C of the FICA Act, as below:

    - Chairperson of the board of directors.
    - Chairperson of the audit committee.
    - Executive officer; or
    - Chief financial officer, of a company, as defined in the Companies Act, 2008 (Act No. 71 of 2008), ***if the company provides goods or services to an organ of state and the annual transactional value of the goods or services or both exceeds an amount determined by the Minister by notice in the Gazette.***

3. A **FPEP** is an individual who holds, **or has held,** in any foreign country a prominent public function as listed in Schedule 3B of the FICA Act, but not limited to that of a:

    - Head of State or head of a country or government.
    - Member of a foreign royal family.
    - Government minister or equivalent senior politician or leader of a political party.
    - Senior judicial official.
    - Ambassador or high commissioner or other senior representative of a foreign government
    - Senior officials of companies that receive certain tenders from government.
    - Senior executive of a state-owned corporation; or
    - High-ranking member of the military or Police Services (Above the rank of major-general).

Clients that are immediate family members or known close associates of DPEPs/DPIPs and FPEPs, although not holding a DPEP/DPIP or FPEP position themselves, must be treated as DPEPs/DPIPs and FPEPs for the purposes of ML risk determination and the resulting CDD, including enhance due diligence and other applicable measures.

Holding a DPEP/DPIP/FPEP status or being an immediate family member or known close associate of a DPEP/DPIP is a characteristic of a client factor that impacts upon the client's ML profile.
The AI must establish the client's PEP status by means of various methods, including directly requesting the information, utilizing open data sources, other persons, or screening against independent commercial databases.

An AI must provide in its RMCP the method which it uses to determine whether a prospective client or an existing client is a DPEP/DPIP/FPEP.

AIs should be aware that information provided by the client and other persons indicating their DPEP/DPIP/FPEP status or known close associates of DPEPs/DPIPs/FPEPs may be misrepresented. It is therefore of grave importance that the detail must be scrutinised, to determine if the client is a DPEP/DPIP or FPEP.

#### 4.1.6 Enhanced Client Due Diligence Process: Domestic Politically Exposed Person (DPEP) (Schedule 3A) and Domestic Prominent influential Person (DPEP) (Schedule 3C)

The ML risk associated with a client that is a DPEP/DPIP must be assessed, as not all DPEPs/DPIPs pose an inherent high ML risk.

Where the time periods as set out in Schedule 3A and 3B to the FICA Act lapse, it is suggested that in terms of the risk-based approach, for the AI to regularly consider with the former DPEP/DPIP or FPPO, their immediate family member of known close associates, still poses a high risk from a ML perspective.

### 4.1.7 Enhanced Client Due Diligence Process: Foreign Politically Exposed Persons (Schedule 3B of the FICA Act)

FPEPs and their immediate family members or known associates, pose and inherent high ML risk and the AI must conduct enhanced due diligence, on such persons, as per sections 21F, 21G and 21H, of the FICA Act.

Once an AI establishes that a client or the beneficial owner of that client is a FPEP an AI should deem the business relationships as a high-risk relationship.

### 4.1.8 Enhanced Client Due Diligence Process: Family members or Known Close Associates of DPEPs/DPIPs/FPEPs

The following individuals are considered as a family member or known associate of a foreign prominent public official or domestic prominent influential person, but the list is not exhaustive: -

- Spouse or civil/life partner.
- Previous spouse or civil/life partner.
- Children and stepchildren and their spouses or civil/life partners.
- Parents.
- Siblings and step siblings and their spouses or civil/life partners.
- Business partners or associates who share beneficial ownership of corporate vehicles with the prominent person, of 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 setup for the actual benefit of the prominent person.

**When dealing with a legal person whose beneficial owner is a DPEP/DPIP/FPEP and/or**
**family members or known close associates of these persons, an AI must:**

- Establish and verify the client information. Given that the client poses a high risk, this would entail EDD,
- Understand and obtain information on the business relationship; and
- Undertake obligations set in sections 21F and sections 21G of the FICA Act.

Where a natural person, who is a role-player on a legal has been identified as a DPEP/DPIP/FPEP, the legal person and other individuals linked to the legal entity must be treated as DPEP/DPIP/FPEP.

Where the beneficial owner of a client is a DPEP/DPIP presenting a high ML risk or an FPEP, the requirements as set out in section 21F and 21G of the FICA Act applies.

Trustees, founders, and named beneficiaries, of a trust, are all regarded as beneficial owners of the trust and as such, the AI must scrutinise their information to determine whether these beneficial owners are DPEPs or FPEPs.

**Other persons –FPEP, DPEP or PIP considerations**

The application of below requirements is not limited to high-risk DPEPs/DPIPs and FPEP's:

- Obtain Senior Management approval to establish a business relationship, by means of a process descripted in the AI's RMCP.
- Establish the source of wealth and source of funds, of the DPEP/DPIP/FPEP.
- Conduct ECDD and on-going monitoring, on the DPEP/DPIP/FPEP identified.

Since a client's DPEP/DPIP/FPEP status can change over the life span of the business relationship, AIs must implement a dual process, in which all clients are subject to a **daily** World-Check/Refinitiv batch validation process, to establish if any new or existing clients have been identified as potential DPEPs/DPIPs/FPEPs.

At onboarding and during on-going CDD monitoring, the DPEP/DPIP/FPEP question as described within the new business application forms and FICA Act checklists, are asked to the client, as to establish if the PEP status of the client has not changed since previously enquired.

**It is of utmost importance that the DPEP/DPIP/FPEP question is explained to a client and that the client's correct status is captured on the line of business systems. The client must also clearly indicate the reason as to why he should be noted as a DPEP/DPIP/FPEP.**

Where a client or other persons has acknowledged to the AI that they are a DPEP/DPIP/FPEP, immediate family member or known close associate, the AI may accept that information at face value and treat that client and other persons as a DPEP/DPIP/FPEP.

An AI must within its RMCP provide a clear process, in which a newly identified DPEP/DPIP/FPEP has been identified, escalated to Senior Management and

approved/declined for onboarding, or for continuation of business in the event of an existing client.

The FIC strongly encourages AIs, that as part of their risk-based approach, it will consider whether former DPEPs/DPIPs/FPEPs still poses a high-risk from a ML perspective. As a person's DPEP/DPIP/FPEP status can change, should they no longer hold the position that qualifies them as such. However, even though a person no longer fills such a position, they could still be considered as presenting a high ML risk, by the AI. A prior FPEP or high-risk DPEP/DPIP status is a strong indicator that the client could still present a high from a ML perspective.

The fact that a client ceases to hold a position of either a DPEP/DPIP presenting a high ML risk, or an FPEP, does not eliminate the possibility that the client remains a high risk from a ML perspective. Further concerns could be that a former DPEP/DPIP or FPEP could still exercises undue influence over a current DPEP/DPIP or FPEP, to gain undue benefits for the former DPEP/DPIP or FPEP, their family members or known close associates. Or a former DPEP/DPIP or FPEP, could be connected to or exercise influence over corporate entities for example, NPO's, foundations, trusts etc., though they are able to gain undue benefits from for themselves, their immediate family members or known close associates.

MMLL AIs have therefore adopted the principal, of "Once a DPEP/DPIP/FPE always a DPEP/DPIP/FPEP".

Potential indicators of heightened ML risk when dealing with DPEPs/DPIPs, include but is not limited to:

- Nature and seniority of the DPEP/DPIP position, which may be indicative of the level of influence and sway that they may have.
- DPEP/DPIP declares that he/she is not a DPEP/DPIP, however subsequent searches through independent third-party sources indicates that the individual is in fact a DPEP/DPIP.
- DPEP/DPIP avoids providing information that would reveal that he/she is a DPEP/DPIP.
- DPEP/DPIP is the beneficial owner. Part of Senior Management, or exercises control through other means of a legal person, trust or partnership for commercial purposes.
- Legal person, trust or partnership avoids providing beneficial ownership information, and it is found that the beneficial owner is a DPEP/DPIP.
- DPEP/DPIP avoids providing source of wealth and source of funds information.
- Negative media or investigative reports on the DPEP/DPIP, immediate family members or known close associates.
- Negative commission reports, or judicial findings on the DPIP, immediate family members or known close associates.
- Unethical conduct by a DPEP/DPIP.

- DPEP/DPIP controls access to government funds, public funds or controls major public benefits, such as decisions on whether to award tenders, grants, procurement and licenses and so forth.
- Credible allegations of ML, TF, PF, bribery corruption or any other predicate offence involving the DPEP/DPIP.
- Previous convictions of the DPEP/DPIP for ML, TF, PF, bribery, corruption, or any other predicate offence.
- DPEP/DPIP is closely associated with persons who have been convicted of ML, TF, PF, bribery, corruption or any other predicate offence.
- DPEP/DPIP has been previously charged with ML, TF, PF, bribery, corruption or any other predicate offence.
- DPEP/DPIP, their immediate family members or known close associates' assets do not align to the source of wealth and source of funds.
- DPEP's/DPIP's, their immediate family members or known close associates hold accounts in other countries.
- DPEP's/DPIP's, their immediate family members or known close associates hold or utilize customer foreign currency accounts, foreign currency wallets and any other foreign currency product or store of value.
- Large amounts of cash transactions or cross-border transactions take place in the DPEP/DPIP, their immediate family members or known close associates' accounts.
- Deposits are made into the DPEP/DPIP, their immediate family members or known close associates' accounts followed by immediate transfers outward.
- DPEP's/DPIP's, their immediate family members or known close associates have numerous accounts with different banks.
- DPEP's/DPIP's immediate family members or known close associates avoid providing information that would reveal that they are linked to a DPEP/DPIP.
- DPEP's/DPIP's immediate family members and known close associates control legal persons, trusts, and/or partnerships which have been awarded public funds or benefits.
- Client is an immediate family member or known close associate of a former DPEP/DPIP that presents a high ML risk.
- DPEP's/DPIP's immediate family member and known close associate is allegedly involved in or was previously convicted of ML, TF, PF or any other predicate offence.
- AI has filed STR through to the FIC, on either the DPEP/DPIP, their known close associates or immediate family members.

The above list of potential indicators is not an exhaustive list.

#### 4.1.9 Enhanced Client Due Diligence Process: Other Legal Entities: Stokvels/Churches/Clubs/Schools/Body/Corporates/Homeowner Associations

**Once a CDD process has been followed on a legal entity as well as a further EDD process**, as required, it is important that the AI follows a verification process on the natural persons who are linked to the entity:

- The AI will decide on the degree and method of verification.
- The detail of the entity is to be verified with information obtained by a reliable and independent third-party source.
- Each individual who exercises control over the management of the legal entity, in the capacity of an authorised person on behalf of the legal entity, must be verified, with information obtained by a reliable and independent third-party source.

**Geographic Risk:**

A separate category for risk assessment is determined by geographical risk.

The exclusion of assessing geographic areas, both internationally and domestically, when determining ML/TF/PF risks may result in an incomplete and inadequate risk management process.

Consideration of geographic area risk indicators can be applicable when the AI:

- Seeks to establish or continue business operations in a particular geographic area;
- Establishes a business relationship with a client who is based in a particular geographic area;
- Seeks to conduct a single once-off transaction for a client, where such a client is based in a particular geographic area;
- Seeks to process a transaction where either the originator/s, intermediary/ies and/or beneficiary/ies are based in different geographic areas; and
- Product and/or service in relation to the client engagement is in a particular geographic area.

*This is not an exhaustive list.

**Countries with a high risk** from a ML/TF/PF point of view, are countries high on corruption indexes, unsecure economic and political systems, inefficient legal system or small number of requirements for the documentation needed for opening businesses, countries known for production, processing and trafficking drugs and weapons.

There are various sites who carry lists of these countries, for example:

- **Transparency International** issues an annual report on the corruption perceptions index (CPI). They score countries according to the perceived level of corruption of a country's public sector, according to experts and business executives. This list is useful in understanding the perceived level of corruption in a particular country.

The **Organisation for Economic Co-Operation and Development** (OECD) established the Anti-Bribery Convention, which has established standards on the prevention of bribery of foreign public officials. All countries that are members of this convention are subject to peer review examinations. The results of these assessments give an overview of the level of compliance with the Anti-Bribery Convention.

The **United Nations Office on Drugs and Crime** (UNODC), has further created the International Money-Laundering Information Network (IMoLIN) that provides for an AML/CFT research resource that focuses on the review of several countries' AML/CFT laws and regulations and has identified areas for improvement required.

The current measures imposed by the **United Nations Security Council**, sanctions are largely imposed against a particular activity that is present in a specific geographic area (country). Although the current sanctions listings do not indicate that the geographic area in and of itself is sanctioned by the UNSC, the UNSC is not precluded from doing so. The reason that has led to the UNSC sanctions listings may, however, be indicative of a higher level of PF and TF risk relating to the geographic area.

**Public Compliance Communication 49,** deals with the ML/TF/PF threats and vulnerabilities posed by international geographic areas.

A geographic area is not limited in definition and can include a specific area within the borders of a country, a country, areas of specific interest globally or countries belonging to certain groupings. Geographic areas include international areas and domestic areas i.e., areas within the borders of South Africa.

A geographic area indicator can include the geographic area in relation to the client, the product or service and the inflow and outflow of funds such as the source or destination of the funds in relation to the business relationship, or transaction with a client.

A geographic area in and of itself does not present a ML/TF/PF risk, rather the features and activities attached to the geographic area serves as an indication of the potential abuse for ML/TF/PF within that geographic area. For example, the ISIS cells identified and operating in KwaZulu Natal. Thus, there can be varying levels of ML/TF/PF risk associated with geographic areas, ranging from lower to a high risk of ML/TF/PF

The geographic area indicator should not be reviewed in isolation to other risk factors when determining the ML/TF/PF risk as the inter-connectivity between the other ML/TF/PF risk factors and the geographic areas associated to those factors may present different ML/TF/PF risks. This will allow for a holistic understanding of the risk associated with geographic areas. By means of example, the ML/TF/PF risk relating to the geographic area of where the client resides may be a different ML/TF/PF risk compared to the geographic area connected to the source of the funds. As such, the ML/TF/PF risks relating to geographic areas are to be

understood against the product/service and client risk features, activities, and the multiple geographic areas concerned.

An AI should consider various external data as published by reliable, reputable and independent third parties which can include international AML, CTF and CPF standard-setting bodies and commercial enterprises.

At a minimum, the FIC considers the listings as issued by the FATF regarding ML/TF/PF risks associated with certain geographical areas as a core data source, that has certain implications for South Africa.

As the international standard-setting body on AML/CTF/CPF matters, the FATF identifies geographic areas that have significant strategic deficiencies in their AML/CFT/CPF regimes.

When such a geographic area is identified and published by the FATF, the FIC will issue advisories explaining the considerations and actions to be taken by AIs in a South African context. These advisories can be found on the FIC's website at www.fic.gov.za

AIs are to take note of these FIC issued advisories and review the content against their compliance controls and make adjustments to their risk processes as contained in their RMCP, where so required. An AI must be able to demonstrate to their supervisory body if the information contained in the advisory is of relevance to their business and additionally, where it is, the measures taken to address the advisory.

The FATF has identified such geographic areas under the following headings:

- Jurisdictions under increased monitoring (informally referred to as the grey list); and
- High-risk jurisdictions subject to a call for action (informally referred to as the blacklist).

In order to determine the ML/TF/PF risk associated with a geographic area, an AI would need to review the geographic area against a certain set of features and/or activities. This may result in the AI deeming the risk relating to a geographic area to present either a lower risk, or a higher risk.

An AI should consider the below features or activities when reviewing a particular geographic area:

- AML/CTF/CPF regulatory framework;
- The quality of the AML/CTF/CPF regulatory framework;
- Perceived level of adherence to compliance and enforcement of the AML/CTF/ PF regulatory framework by AIs;
- Country membership to an AML/CTF/CPF organisation;

- Perceived compliance to AML/CTF/PF regulatory framework and quality of supervision by regulatory bodies;
- Perceived levels of crimes;
- Perceived level of prosecutions;
- Perceived levels of bribery and corruption;
- Perceived levels of influence of the abuse of public office by criminal entities;
- Secrecy and protection of information, and access to information regulatory regimes,
- Perceived tax havens;
- Listing of a geographic location on a sanction listing e.g., United Nations Security Council (UNSC) listing, as well as countries subject to restrictions such as trade or arms embargoes;
- Proximity to geographic area, such as bordering geographic areas that may serve as nodal points for ML/TF/PF activities or states known to have a sympathetic stance towards ML/TF/PF activity;
- Countries with porous borders including sea borders;
- Efficiency of independent state agencies in carrying out their respective mandates;
- Perceived level, activity or support of efforts aimed at undermining AML/CTF/CPF measures and interventions.

The criteria used for the ML/TF/PF risk determination relating to a geographic area must be noted in the AI's RMCP.

### 4.2 Risks from Products/Services:

The **overall client risk assessment** will also contain assessments performed according to the category of risk of **money** laundering and financing terrorism based on the inherent risks of the **product or services offered** by an AI.

**Products with high risk from** a ML/TF/PF point of view are the ones that **include high level of anonymity, offer ease of frequency of transactions or are inherently open to cash transactions**. AIs' must take into account products and the services not directly offered by them, but where they potentially play a role as mediators, i.e. their services are used to deliver the product.

Services and products which can be categorised as potentially higher risks associated with money laundering, terrorist and proliferation financing are:

- International correspondent banking services which include transactions, i.e., commercial payments for persons who are not clients of the bank-mediator.
- Services including transactions' realisations through use of non-resident accounts;
- Intermediary services;
- Third-party payments;
- Cross-border flow of money;
- Duration of relationship/transaction;

- Services including or enabling cash usage;
- Services related to trading with precious and noble metals; and
- Services related to the new technologies or developing technologies preferring client's anonymity; e.g., electronic banking etc.

Product risk factors to consider:

- Does the product enable third parties who are not known to the institution make use of the product?
- Is there another AI involved in the usage of the product?
- Can funds be converted to cash easily and quickly?
- Does the product allow for the flow of physical cash.
- Is the offering of the product subjected to regulatory approval and/or reporting?
- Is the usage of the product subject to reporting to regulators and/or "the market"?

### 4.3 Nature of the Business Relationship and the Source of Income or Wealth/Source of Funds:

AIs will be required to establish whether a client intends on establishing a business relationship with the AI, or whether a single transaction will take place, and has to collect relevant information to the potential risk identified.

The information an AI is required to obtain on its clients must be adequate to reasonably enable the AI to determine whether the transactions involved are consistent with the AI's knowledge of that client and the client's business activities, and must include particulars concerning: -

- The source of client's income/wealth; and
- The source of funds that the client expects to use in in concluding the single transaction or transactions in the course of the business relationship.

#### 4.3.1 Nature of Source of Wealth/Income

**The terms source of wealth or income** relates to the policyholder, premium payer, or contributor's entire body of wealth (total assets) that includes his/her/its regular income, which should provide the AI with a reasonable indication of how the wealth was acquired and on which he/she/it relies on for livelihood, expenditure and investments.

AIs must establish whether the premium payer and the policyholder to a specific transaction is the same person. If it is not the same person, AIs are required to determine why the person is paying the policy premium and identify the source of wealth and the relationship between the parties.

#### 4.3.2 Nature of Source of Funds:

**Source of funds** can be defined as the funds that the client intends to use in concluding a single transaction or a transaction in the course of the business relationship. The source of funds relates to the origin of the funds used to fund the policy or transaction.

### 4.4 Measures in Mitigation of ML, TF and PF Risks

#### 4.4.1 Continuous due diligence

Further to the fact that under specific circumstances an EDD process is required for **high-risk** clients, all AIs will perform **continuous CDD** on their clients and their business relationship to ensure that the past knowledge they have obtained on their clients is up to date, accurate and consistent with the continuous nature of business relationship/transactions.

The frequency of how often CDD must be implemented or reviewed will depend on the client's risk rating and specific instructions received from the client, which could result in the client's rating to be changed to a higher rating. **These types of instructions are known as "trigger events".**

The purpose of pre-defined trigger events is to identify irregular behaviour or activities measured as a variance against the client's typical behaviour or to identify transactions with no apparent business purpose, which might indicate suspicious behaviour.

When a pre-defined trigger event is identified in business, the business relationship will be re-evaluated in terms of the client risk matrix. If the client's risk rating remains unchanged, the trigger event will be processed and recorded. Alternatively, if the client's risk rating increased to a high-risk rating, i.e., from medium risk rating to high risk, an EDD needs to be performed.

**The trigger events can include instructions listed below, but is not limited to:** *(T*rigger events *should be similar between the different AIs, only thresholds could be different)*:

- A change in the premium payer.
- A change in bank account details.
- Increase in regular (monthly premium or monthly contribution) of more than R5 000.00. (As per Guidance Note 8 of the FIC, issued 6 April 2023)
- Increase in once-off (add single premium and ad-hoc payments) of more than R50 000.00. (As per Guidance Note 8 of the FIC, issued 6 April 2023)
- All payments made to beneficiaries.
- Refunds (Including cool-offs) if less than 6 months from inflow and amount for example as more than R1 000.00.
- Changes in personal information (ID number, Entity name, Entity registration number).

- Multiple changes to a client's personal detail, including mobile and physical address detail.
- Cross border funding and payments.
- Transfer or outright cession of a policy.
- Listed on World-Check since previously checked.
- If changes to a legal entity who is a relevant role player on a contract or policy.
- Fund withdrawal requests received.
- Cancellation of contract where CDD has not previously been implemented.
- Changes to physical address.
- Insured event/death of a life insured with a nominated beneficiary to the policy, subject to any dependents on the life of the life insured (Retirement Annuities).
- Stipulations in terms of a trust deed regarding payments to trust beneficiaries.

**AIs must establish a CDD Team to assist in the onboarding of clients and monitoring existing client's behaviour.**

**The CDD Team is responsible for:**

- Ensuring that all relevant information and documents required to validate client details are available;
- Ensuring all documents and information received is accurate, as the client's risk rating depends on the information and details obtained;
- Implementation of investigations relating to escalated cases, to present to Senior Management;
- Interpretation of the electronic validation systems and media searches that have been implemented, (for example, Windeed, TransUnion, World-Check, Client Validation and FNB online); and
- Escalation of details of high-risk clients to Senior Management and Compliance for sign-off, before accepting the business, or a transaction.

### 4.4.2 Doubts about veracity of previously obtained information

When an AI is doubtful of the authenticity of information which was previously collected on a client, the AI must repeat the CDD process to confirm the authenticity of the information in question and verify this information by use of a reliable third-party electronic database.

### 4.4.3 Inability to conduct customer due diligence

If an AI is unable to conduct CDD as a result of a client's unwillingness to co-operate with its CDD requirements, an AI is required to do as follows:

- Not establish or conclude a business relationship or a single transaction;

- Terminate the existing business relationship, as per the AI's documented process;
- Report the case in terms of Section 29 of FICA Act, where applicable;
- Place a hold on any funds received; and
- Funds may only be released once all the relevant CDD requirements have been received.

## 5. DUTY TO KEEP RECORDS

**Please take note that this Section applies to all AIs**

Record keeping is an essential and required process which successfully enables AIs to combat ML, TF and PF. The records held by an AI of its clients' identities and transaction activities are of paramount importance as these records can be used as documentary evidence which proves compliance with legislation and can assists law enforcement authorities in the detection, investigation, prosecution and the repossession of criminal funds where illegal flow of funds is concerned.

### 5.1 Obligation to keep customer due diligence records

An AI will retain all CDD records and information, required as per the AI's client risk rating (Low, Medium or High). These records may include, but is not limited to:

- Copies of identification documentation;
- Copies of residential address documentation;
- Copies of source of funding e.g. proof of bank statement, deposit slip;
- Documentation which proofs the nature of business relationship or occupation;
- Verification document and any other information collected about the client;
- Source of Income/Wealth and Source of Funds; and
- All information sources, such as news articles, third-party service provider details and any other detail gathered, relating to the high-risk case, which was escalated to Senior Management for approval, together with the motivation and justification of their decision concluded. The sources and history of such transactions must be ring-fenced for confidentiality purposes and only accessible to only the relevant parties.

### 5.2 Obligation to keep transaction records

An AI is obligated to retain a record of every transaction, whether the transaction is concluded during a business relationship with the client or whether it is a single transaction. The transaction record must contain such information that would enable MMLL to reconstruct the transaction.

**The following information must be reflected in the records to promote transparency:**

- The date on which transaction was concluded;
- The parties to the transaction;
- The nature of the transaction;

- Business correspondence;
- Amount and Currency use in the conclusion of the transaction;
- Where the AI provides a facility such as an application, where clients can access account information and files, such transactions should also be recorded; and
- Any and all reports submitted to the FIC.

### 5.3 Period for which records must be kept

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

- Records relating to establishment of the business relationship must be kept for at least 5 (five) years from date of termination of business relationship.
- Records relating to all transactions must be kept for at least 5 (five) years from the date which the transaction was concluded.
- Records relating to a transaction or activity which gave rise to the AI reporting a suspicious activity or transaction to FIC must be retained for at least 5 (five) years from the date which a suspicious activity or transaction was reported to the FIC.
- Records which an AI have in their possession which is connected to an ongoing investigation, must be kept until such time when the relevant law enforcement authority has confirmed that the case has been formally closed or finalised.
- All records must be stored electronically and hardcopy versions must be stored for at least 5 (five) years.

### 5.4 Record may be kept in electronic format and by a commercial third-party or intra-group centralized data storage facility

An AI is permitted to store all the retained records in any form which is convenient and safe for an AI. An AI must store records electronically at a location owned by a third-party or the intra-group centralized data storage, provided that:

- The AI has easy and free access to the records and will have the records readily available to the FIC and relevant supervisory body as and when it is required;
- The liability remains with the AI should the third-party fail to comply with the provisions of the FICA Act;
- That the AI provides the FIC and relevant supervisory bodies with the full particulars of the third-party;
- Electronically retained records should have the capability to be reproduced in a legible format;
- The AI must inform clients of its intention to retain their records with a specific third-party and must seek the clients' consent in sharing their personal information with this third-party; and
- The AI must safeguard and ensure that there are controls in place, such as firewalls, that will safeguard against any unauthorised third-party tampering with the electronic data.

#### 5.4.1 Records should be stored in a detailed manner which enables the easy identification of such records

**Records should be stored for example by:**

- The client's identity number;
- The reference number on the policy or the contract number;
- The reference number of the business correspondence;
- Relevant dates of issuing or expiring; and
- Details of the writer, etc.

## 6. REPORTING DUTIES

**Please note that this section is applicable to any person and all AIs that have reporting obligations.**

**Responsible persons**

AIs are required to, as far as possible, have allocated officers to attend to requests, interventions and orders received from the FIC in terms of Sections 27, 32, 34 and 35 of the FICA Act.

Institutions and persons are required to respond to the instructions in terms of the specified communications sent by the FIC, by responding to the original message using the same platform through which the instruction was received. Alternatively, the FIC will inform the institution or person which method to use when responding to the FIC.

### 6.1 Reporting obligations to advise the FIC of their clients, or persons acting on behalf of their clients (Section 27)

**Section 27 compels Ais and persons subject to the reporting obligations,** to advise the FIC of its clients, or persons acting on behalf of its clients, in response to a request from an authorised employee from the FIC. The purpose of such requests is to obtain information relating to specified clients and/or client account numbers of the client, held at an institution, who may be linked to ML, TF or PF activities.

The FIC may request information from an AI or any person with regards to:

- A specified person or entity is or has been a client of an AI or person;
- A specified person acting or has acted on behalf of any client of an AI or person;
- A client of an AI or person is acting or has acted for a specified person;
- 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;
- A specific bank account number is/was utilized on any contract for debits or credits;
- The type and status of a business relationship with a client of an AI; and
- The responsible person appointed by the AI, namely the MLRO, must inform the FIC accordingly.

If a suspicious transaction or activity is identified, a suspicious and unusual transaction report (STR/SAR) must also be submitted to the FIC via go-AML, by the MLRO.

### 6.2 Reporting of Cash Transactions above prescribed limit (Section 28) (CTR)

CTR provides a mechanism to monitor reported cash transactions so that potential proceeds of crime are identified and investigated.

An AI must submit an electronic report to the FIC, within a period of 72 hours (within 3 {three} business days) from the date on which the AI or any of their employees, have become aware of the transaction, in the instance that a transaction has been concluded with a client, where a single amount) received in cash, exceeded the prescribed amount of R49 999.99. An AI must submit this report if the amount was:

- Received by an AI from the client or authorized entity (Agencies), or from a person acting on behalf of a client or from a person on whose behalf a client is acting; or
- Paid by the AI to the client, or to a person on behalf of the client, or to a person on whose behalf the client is acting.

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

South Africa does not have an autonomous or domestic sanctions regime (as do countries such as the United States of America, the United Kingdom, Australia etc.). South Africa has 2 (two) targeted financial sanctions regimes based upon the country's obligation as a member of the United Nations (UN).

South Africa's targeted financial sanctions regimes originate from resolutions of the United Nations Security Council (UNSC) under Chapter VII of the Charter of the United Nations.

South Africa implements2 (two) distinct targeted financial sanctions regimes through the FICA Act and the POCDATARA Act, which form part of the AML/CFT/CPF regulatory framework. Section 4 of the POCDATARA Act read together with section 15 of the POCDATARA Act criminalises the financing and facilitating of terrorist and related activity, which offence applies to everyone, not just AIs.

The UNSC resolutions relate to the financing, prevention and suppression of terrorism and TF, as well as the prevention, suppression and disruption of the proliferation of weapons of mass destruction and its financing.

The knowledge about the origin and ownership of the property in question is based on fact and should be acquired with reference to an objective set of circumstances or facts (as opposed to a suspicion that is formed subjectively).

"Property" includes assets, any form of monetary value or funds, negotiable instruments that is owned, held or controlled directly or indirectly for the benefit of a designated person or entity.

The FATF Recommendations 6 and 7 also requires the implementation of the UNSC Resolutions on targeted financial sanctions regime for all FATF member countries.

The application of the UNSC resolutions and FATF Recommendations by South Africa are reflected in sections 26A (Notification of persons and entities), 26B (Prohibition relating to persons and entities), 26C (Permitted financial services & dealing with property and 28A of the FICA Act and section 4 of the POCDATARA Act.

(The complete list can be found at: https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list and https://www.saps.gov.za/resource_centre/acts/terrorism.php)

An AI is required to file a report with the FIC if the AI knows that it possesses or controls property of a person or entity which has committed or attempted to commit or facilitate the commission of a specified offence as defined in the POCDATARA and/or is identified in a notice issued by the President under Section 28A of FICA Act and/or a person or an entity identified pursuant to a UN resolution as contemplated in a notice referred to in Section 26A(1) of the FICA Act.

When a reporting obligation arises in terms of Section 28A of the FICA Act, regarding a client that is the client of more than one AI in a complex group structure, each AI that has in its possession or under its control property owned or controlled by, or on behalf of, or at the direction of a natural person or entity listed in terms of POCDATARA and/or Section 26A(1), Section 26B and Section 26C, of the FICA Act must submit a separate TPR to the FIC.

**"TPR"** refers to a terrorist property report which must be submitted in terms of Section 28A of the FICA Act.

**"TFS List"** means the Targeted Financial Sanctions List pursuant to Section 26A, of the FICA Act, 2001.

In order for an AI to determine if they are dealing with a person or entity on the UN1267 list; or Targeted Financial Sanctions List (TFS List) pursuant to Section 26A, Section 26B and Section 26C, they must scrutinize the information obtained concerning their clients, as per Section 28A.

Section 28A of the FICA Act places a direct obligation on AIs to scrutinise a client's information to determine whether their clients are listed in terms of section 26A of the FICA Act.

An AI must determine if their client is a listed person or entity on the TFS lists, including if the client is:

- A person acting on behalf of the client; or
- A beneficial owner; or
- Is party to the transaction.

A client's information must be scrutinized regardless of the risk assigned to the business relationship or single transaction. Where there is a heightened PA risk the AI should perform enhanced scrutiny of the client information.

AIs must check whether their clients are listed on notices as and when published in terms of section 28A of the FICA Act (UN1267) and Section 26A (TFS). Should a client's name match against the UN1267 list or the TFS List, the AI must ensure that it is an exact match, by conducting a further investigation on the details provided.

Once the AI **has** determined that it controls relevant property, the AI must freeze all the designated person's or entity's, after which, the AI is required to report full particulars of the type of property concerned and a description of the property connected in relation to which the terrorist property report is made.

In the event of a new or potential client, been identified as on the lists, the AI must not establish a new business relationship or conduct a single transaction with the designated persons or entities.

An AI must **within** 5 (five) business days of having **factual knowledge** that it has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of report:

- Any entity which has committed, or attempted to commit or facilitated the commission of the financing of terrorism or related activities, as defined on the POCDATARA, 33 of 2004;
- A specific entity identified in a notice by the President, under Section 26A of the FICA Act, and/or
- A sanctioned person or entity identified on the UNSC sanctions list.

MMLL must upon publication of a proclamation by the President or a notice given by the Director of the FIC:

- Scrutinize its information concerning clients with whom an AI have business relationships in order to determine whether any such client is a person or entity mentioned in the proclamation by the President.
- Scrutinize its information concerning clients with whom an AI have business relationships in order to determine whether any such client is a person or entity mentioned in the notice by the Director of the FIC.

#### 6.3.1 Notifications of persons and entities identified by the Security Council of the United Nations (UN1267)

**Please note that this section is applicable to Any Person, AI and Reporting Institutions**

In terms of **the** FATF Recommendation 7, the United Nations Security Council requires member countries to implement **targeted financial sanctions** against

persons or entities whose property is known to be connected to **terror financing. Terror financing** measures generally restricts MMLL to deal or conduct further business with the following:

- Property received from persons or entities connected to terror financing.
- Funds received from persons or entities connected to terror financing.

In order to give effect to the sanctions the Act requires MMLL to freeze property and **transactions** pursuant to the financial sanctions imposed in the United Nations Security Council Resolution.

A notice by the Minister of Finance and the Director of Public statement (notification) is meant to advise the sanctioned person, entity and MMLL, who may have them as clients or prospective clients, of the relevant sanction.

### 6.3.2 Prohibitions relating to persons and entities identified by Security Council of the United Nations

This prohibition in Section 26 B of the FICA Act has a broad application and is applicable, but not limited to, all instances where the designated person or entity is:

- The client
- The person acting on behalf of another person
- A beneficial owner of the client or
- A party to a client's transaction, including a party who benefits in any way from a client's transaction.

Persons who are required to obtain approval (e.g., permits or authorization) in terms of applicable legislation to deal with controlled goods or activities should pay particular attention to the provisions in Section 26B of the FICA Act, as they have a potentially heightened exposure to designated persons or entities.

An AI is prohibited from directly or indirectly, in whole or in part and by any means or method to:

- Acquire, collect, use or own property of a person or entity whose name appears on the sanctions list.
- Provide or make available or invite a person to provide or make available property of a person or entity whose name appears on the sanctions list.
- Provide or make available or invite a person to provide or make available economic support or facilitate the acquisition, collection, use or provision of property, the provision of any financial or other service, or the provision of economic support of a person or entity whose name appears on the sanction list.

This in essence means that MMLL is prohibited to transact with a sanctioned person or entity. MMLL must report to the FIC, the property which MMLL is in possession of or has control of, which is owned or controlled by a person or entity on the sanction list.

### 6.3.3 Permitting financial services and dealing with property

The Minister of Finance may in writing and on conditions that he/she has considered appropriate and in accordance with the United Nations Security Council Resolution, allow an AI to permit a sanctioned person or entity to conduct financial services or deal with property affected by a sanctions order, to allow such person or entity access to basic living expenses such as:

- Rent or mortgage.
- Food (groceries).
- Medicine or medical treatment.
- Taxes.
- Insurance premiums.
- Maintenance orders.
- Public utility charges.
- Reasonable professional fees.
- Reimbursement of expenses associated with legal services.

The Director of the FIC must give notice of written permission from the Minister of Finance to MMLL and other interested parties. This must be done by means of publishing the notice containing the permissions and conditions thereto on the FIC website.

**It is vital for an AI to screen its prospective clients and existing clients to enable an AI to determine whether these clients are sanctioned persons or entities which might expose MMLL to a high degree of risk. An MMLL AI can screen clients by using the following tools:**

- World-Check Sanction List.
- Social Media Searches/ Web-based Search Engines.
- Financial Intelligence Centre Sanction List (Targeted Financial Sanctions List).

**If a client appears on any of the abovementioned lists, MMLL has an obligation to immediately freeze the assets of the person or entity on the sanction list and report same to the FIC.**

An AI does not have to obtain the consent from either the FIC or through a court order, in order to freeze the designated person's or entity's property, in terms of Section 26B of the FICA Act.

If an AI, cannot accurately determine if a transaction will breach a TFS obligation, the AI must not process any transactions with the potential client or entity and may consider seeking independent legal advice.

**Distinction between Terrorist Financing and Related Activities Reporting Obligations in terms of Section 29 and Terrorist Property Reporting in Terms of Section 28A of the FICA Act**

The obligation to report suspicious and unusual transactions and activities in terms of Section 29 applies to a wide category of persons and businesses, whereas the obligation to report in terms of Section 28A of the FICA Act is limited to AI.

A report submitted in terms of Section 29 refers to a suspicion, which is subjective, whereas a report submitted in terms of Section 28A is factual, based on the knowledge of an AI that it has property in its possession or under its control that is associated to a person listed in UNSC lists.

A report made in terms of Section 29 would refer to a particular transaction or activity which is found to be suspicious or unusual in nature, while a report in terms of Section 28A relates to property of a natural person or entity which is under an AI's control and is known to be connected to the financing of terrorist activities.

In many instances a cash transaction more than the prescribed threshold amount will be reportable as a cash threshold report in terms of Section 28 and when deemed to be suspicious or unusual transaction or activity may also be reportable in terms of Section 29.

When filing a report with the FIC in terms of Section 28A, it is an offence (as per Section 4 of the POCDATARA) to continue dealing with that property in any way, whereas if a person files a report with the FIC in terms of Section 29, they may elect to continue with the transaction as provided for in Section 33 of the FICA Act.

**Summary of difference between Section 28A and Section 29 report types:**

**Section 28A (TPR)**

- Applicable only to AI.
- Report based on knowledge by the AI of property under its control.
- May not continue with transaction – It is an offence.

**Section 29 (STR, SAR, TFTR & TFAR)**

- All businesses including AI, reporting institutions and any other persons connected to any business.
- Report suspicious or unusual activities or transactions or series of transactions related to the financing of terrorist and related activities – subjective test is used
- May elect to continue with transaction.
- Valid defence to charges brought in terms of Section 4 of the POCDATARA.

### 6.4 Reporting of Suspicious and Unusual transactions (STR) (Section 29)

**An AI or any person who carries on a business or oversees or manages a business or who is employed by a business and who knows or ought to have reasonably known or suspected that: -**

- An AI received or is about to receive proceeds of unlawful activities or property which is connected to an offense relating to the financing of terror and related activities.
- A transaction or series of transactions to which an AI is a party to facilitate or is likely to facilitate the transfer of the proceeds of unlawful activities or the property which is connected to an offense relating to financing of terror activities and related activities.
- A transaction or series of transactions to which an AI is a party that has no apparent business or lawful purpose.
- A transaction or series of transactions to which an AI is a party that may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Services.
- A transaction or series of transactions to which an AI is a party that relates to an offense relating to proliferation funding or the financing of terrorist and related activities.
- A transaction or series of transactions to which an AI is a party that relates to the contravention of prohibition relating to persons and entities identified by the UNSC sanction list.
- Any transaction that has been structured in an extraordinary or unusual way.
- Circumstances where mere suspicion exist. In other words, a state of mind of someone who believes something without adequate proof. This implies an absence of proof that a fact exists. (I suspect but I cannot prove"), for instance:
    - If a person becomes aware of "something"; or Circumstances arise in which a person can reasonably expect to be aware of "something"; or
    - Circumstances arise in which a person can reasonably be expected to suspect "something."
    - A suspicious situation may involve several factors that may on their own seem insignificant, but taken together, may raise suspicion concerning that situation. The context in which a situation arises, therefore, is a significant factor in assessing suspicion. This will vary from business to business and from one customer to another.

Each AI, by understanding their environments ML/TF risks will create and include guidelines pertaining to indicators of suspicious or unusual transactions for their specific environment, within their RMCP. This will enable employees to identify suspicious and unusual transactions, and to escalate the transactions to the AI's MLCO/MLRO, for further investigation and reporting to the FIC, **as soon as possible, but no later than fifteen (15) days from discovering the suspicious transaction.** In terms of regulation 24(3) of the MLTFC Regulations this period must not be longer than 15 (fifteen) days, excluding Saturdays, Sundays and Public Holidays.

Below are a few general indicators that can be taken into consideration.

**Indicators of suspicious and unusual transactions:**

**The following factors may be taken into consideration:**

- Deposit of funds with a request for their immediate transfer elsewhere.
- Unwarranted and unexplained international transfers.
- Payment of commissions or fees that appear excessive in relation to those normally payable.
- Transactions do not appear to be with normal industry practices.
- Purchase of commodities at prices significantly above or below market prices.
- Unnecessary complex transactions.
- A transaction seems to be unusually large or otherwise inconsistent with the client's financial standing or usual pattern of activities; or
- Buying or selling with no apparent concern for making a profit or avoiding loss.
- Lack of concern about high commissions, fees, penalties etc. incurred as a result of a particular type of transaction or particular method of transacting; or
- Performing transactions in a manner to attempt to conceal the underlying client and/ or ultimate beneficiary of the transaction; or
- Frequent cash deposits form different financial institutions and various locations.
- Regular EFT deposits from unknow bank accounts.

**General recommendations when submitting a suspicious report:**

- Why? (Why are you filing = why do you feel uneasy or find it unusual?)
- What? (What caused you to submit the report = what was the indicators/red flags?)
- How? (How did it occur = list specific modus operandi, behaviour and/or transaction modes)
- When? (When did it occur = is it once off versus a series of transactions/events)
- Who? (Who was involved = is it one or more persons, entities or accounts)
- Where? (Location where this occurred)

**The MLRO will report the details of such a transaction(s) and the basis of the knowledge or suspicion concerning the transaction electronically to the FIC, as soon as possible, but not later the 15 (fifteen) business days after discovery.**

The MLRO has created a reporting register, in which the outcome of all the reported and unreported transactions will be recorded.

**Tipping off**

A person involved in the making of a report may not inform anyone, including the customer or any other person associated with a reported transaction, of the contents of a suspicious transaction or activity report or even the fact that such a report has been made.

Section 29 of the FICA Act prohibits any reporter as well as any other person who knows or suspects that a report has been made from disclosing any information regarding that report except for information disclosed:

- within the scope of the powers and duties of that person in terms of any legislation;
- for the purpose of carrying out the provisions of the FICA Act;
- for the purpose of legal proceedings, including any proceedings before a judge in chambers;
- in terms of an order of court.

Contravening these prohibitions constitutes offences in terms of the FICA Act that carry maximum penalties of imprisonment for a period up to 15 (fifteen) years or a fine up to R100 million.

### 6.5 Reporting on the Conveyance of Cash to and from the Republic (Section 30)

**This section is not yet enforced.**

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

**This section became effective, on 1 February 2023.**

All electronic cross-border transactions (the sending of funds out of South Africa and the receiving of funds from outside of South Africa) from a prescribed value of R20 000 and above must be reported to the FIC.

In terms of section 31 of the FICA Act applies to only certain categories of the Ais who are authorised to conduct the business of cross-border electronica transfers.

These institutions are authorised in terms of the Regulations under the Currency and Exchanges Act, 1933 (Act 9 of 1933) The Exchange Control Regulations) to conduct authorised transactions under these Regulations.

Ais with this authorisation are:

- Authorised Dealers (Ads);
- Authorised Dealers with Limited Authority (ADLAs);
- A category of Financial Services Providers (FSP) that have a direct reporting dispensation under the Exchange Control Regulations; and
- The Post Office.

FNB/RMB is the MMLL preferred AD, who acts on behalf of MMLL and who is responsible for the filing of IFTRs, as soon as possible or at latest within 72 hours after FNB had become aware of the transaction.

All cross-border transactions will be submitted to the FIC, by the AD, via the AD's go-AML facility, within the prescribed timeframe.

It is thus of utmost importance that all Ais who participate in cross-border transactions must ensure that they have access to a client's most recent, correct and valid client information.

Should any AI within the MMLL Group structure fit the above criteria as an:

- AD; or
- Authorised Dealers with Limited Authority (ADLAs); or
- A category of Financial Services Providers (FSP) that have a direct reporting dispensation under the Exchange Control Regulations.

The AI must ensure that the relevant reporting processes must be documented and actioned, within their RMCP.

### 6.7 Reporting procedures and furnishing of additional information (Section 32)

Section 32 of the FICA Act is applicable to Ais and any other person that has made a report in terms of Sections 28, 28A and/or Section 29 of the FICA Act.

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

#### 6.7.1 Additional information which may be requested by the FIC in terms of Section 32 of the FICA Act includes:

- Prescribed information relating to transactional activity;
- Supporting documentation concerning the report; and
- The grounds for the report.

#### 6.7.2 Section 32 compels prescribed reporting standards and timelines.

The aforementioned institutions and persons to respond to the FIC's request for additional information in the prescribed manner and within the prescribed period with such additional information concerning the report and the grounds for the report as that institution or person may have available.

### 6.8 Intervention by the FIC (Section 34)

**Section 34 of the FICA Act is applicable to Ais, and any other person required to make a report in terms of Sections 28, 28A or 29 of the FICA Act.**

Section 34 of the FICA Act provides for intervention by the FIC should the FIC, after consulting with the abovementioned institutions or person, have reasonable grounds to suspect that a transaction or a proposed transaction may: -

(a) involve—

a. the proceeds of unlawful activities or property which is connected to an offence relating to the financing of terrorist and related activities; or
b. property owned or controlled by or on behalf of, or at the direction of a person or entity identified pursuant to a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1); or

(b) constitute—

(i) money laundering; or (ii) a transaction contemplated in section 29(1)(b), of the Act.

**Note:** Section 34 of the FICA Act does not apply to the carrying out of a transaction to which the rules of an exchange licensed in terms of the Financial Markets Act, 2012 (Act No. 19 of 2012) apply.

The FIC may direct the AI, 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 (ten) days. For the purposes of calculating the period of 10 (ten) 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 FIC considers it appropriate, to inform and advise an investigating authority or the National Director of Public Prosecutions regarding the transaction.

### 6.9 Monitoring Orders (Section 35)

Section 35 of the FICA 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).

The FIC's function in relation to a **Monitoring Order** granted in terms of Section 35 of the FICA Act is to make the AI aware of the judicial order issued, to ensure that the AI implements the order and to receive the information to be reported in terms of the order.

Monitoring orders provide the FIC with a mechanism to request the monitoring of all client accounts, including, but not limited to, transactions concluded by a specified person with the accountable institution, or all transactions conducted in respect of a specified account or facility at the accountable institution, if there are reasonable grounds to suspect that:

- Proceeds of unlawful activities or property connected to an offence relating to money laundering or terror financing and related activities, were transferred or may be transferred to the AI;
- The AI may be used for money laundering purposes or for any transaction contemplated in section 29(1)(b) of the FICA Act;

- The account or other facility has or may receive the proceeds of unlawful activities or property which is connected to an offence relating to terror financing and related activities; or
- The account or other facility is being or may be used for money laundering purposes or for terror financing or related activities or for the purpose of any transaction contemplated in section 29(1)(b) of the FICA Act.

Type of information that may be required in terms of the order include but are not limited to the following:

- Details of the transactions relating to specified accounts;
- Branch location and time of cash deposits conducted;
- Counter-account details of debits and credits into and from the accounts;
- Street location and time of cash deposits or withdrawals from Automatic Teller Machines (ATMs);
- Copies of account statements;
- Copies of any transactional notifications to and from the client by electronic means including SMS and e-mail messages for online banking purposes; and
- Relevant telephone numbers, e-mail and internet protocol (IP) addresses used to communicate with the client.

An order in terms of subsection (1) lapses after 3 (three) months unless extended in terms of subsection (3).

A judge referred to in subsection (1) may extend an order issued in terms of subsection (1) for further periods not exceeding 3 (three) months at a time if—

- the reasonable grounds for the suspicion on which the order is based still exist; and
- the judge is satisfied that the interest of justice is best served by monitoring the person, account or facility referred to in subsection (1) in the manner provided for in this section.

An application referred to in subsection (1) must be heard and an order must be issued without notice to or hearing the person or persons involved in the suspected money laundering activities.

**Type of information** that may be required in terms of the order include but are not limited to the following:

- Details of the transactions relating to specified accounts;
- Branch location and time of cash deposits conducted;
- Contra-account details of debits and credits into and from the accounts; Street location and time of cash deposits or withdrawals from Automatic Teller Machines (ATMs).
- Copies of account statements.
- Copies of any transactional notifications to and from the client by electronic means including SMS and e-mail messages for online banking purposes; and relevant telephone numbers, e-mail and internet protocol (IP) addresses used to communicate with the client.

## PROCESS TO REMEDIATE REPORTS ON THE FIC'S REGISTRATION AND REPORTING SYSTEM

The FIC has issued a notice (go-AML Notice 4A) which applies to Ais, and other businesses (reporting entities) who submit web and/or batch reports to the FIC on its registration and reporting system, go-AML. The notice explains the process to be applied by reporting entities when remediating or fixing failed and/or rejected reports on go-AML. This notice also explains the process to be applied by reporting entities when it has been discovered that the report they submitted to the FIC and was accepted by the FIC system contains incorrect/inaccurate information (defective report).

### Pre-Validation

Reports submitted to the FIC on go-AML cannot be changed after being submitted. The reporter must check the report before submitting it to the FIC to ensure that all the information captured in the report is correct and accurate.

To prevent failures and/or rejections, pre-validation of reports should be conducted before uploading and submitting a report. This will ensure that accurate information is reported to the FIC within the prescribed format and period.

### Quality reviews and assurance processes

Reporting entities must follow a multi-disciplinary approach that will enable the reporter to apply adequate quality control measures and implement assurance processes in order to identify potential issues relating to submission of reports to the FIC. This will ensure that issues are identified and rectified timeously in accordance with the FIC defined processes.

Reporting entities must also conduct post submission quality reviews on an ongoing basis to ensure that their submitted reports have indeed been processed/accepted, and the client information and transactional data reported meets the requirements outlined in the regulations, and (correlates with the information held by the entity)

### Process to remediate rejected reports on go-AML

All the reports submitted to the FIC through the go-AML system must adhere to the Money Laundering and Terrorist Financing Control Regulations (Regulations), the go-AML schema and business rules. If the report does not meet these requirements, it might be rejected by the FIC system (go-AML). If a report is rejected by go-AML, then the reporter has an obligation to remediate that report. There is no additional period given to reporters for remediation. A report is only considered reported to FIC once it is successfully processed by the FIC system and contains correct and accurate information.

Once a report is submitted on go-AML, the reporter will receive a notification through the message board whether that report was successful or rejected. If the report is rejected, the reporter has an obligation to remediate it, within two (2) business days.

### Process to remediate rejected reports submitted on go-AML web

If the rejected report was submitted as a web report the reporter must follow these steps to remediate:

- Login to go-AML
- Access the rejected report through the Submitted Reports menu on go-AML
- Select revert on the report, which will move the report to the Drafted Reports menu on go-AML.
- The reporter must then access the report on the Drafted Reports menu and then edit and correct the relevant information as per the reasons and specifications provided by the FIC through the message board and re-submit the report to the FIC.

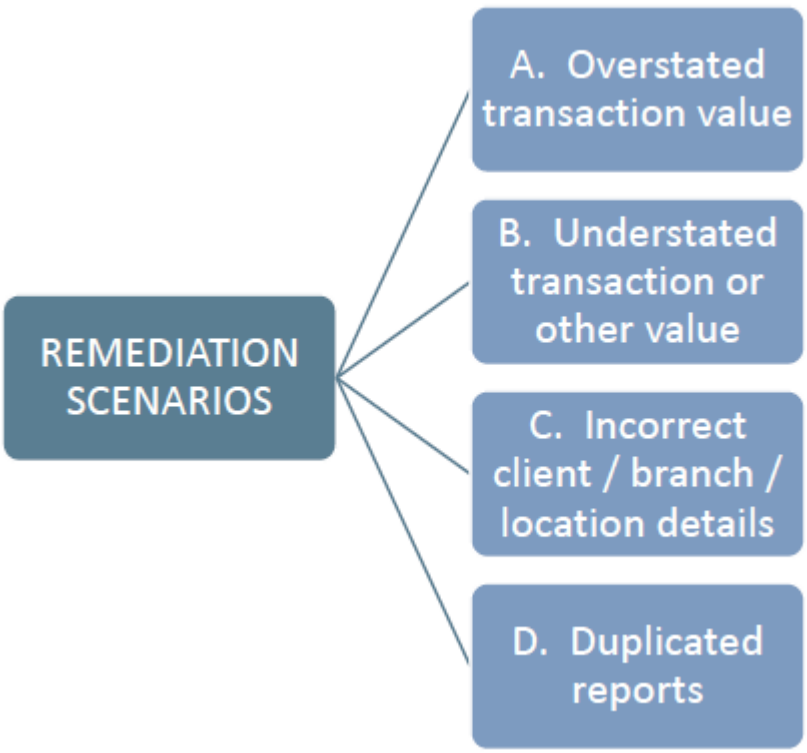
**Process to remediate successfully processed reports with incorrect information**

The FIC considers a report to be successfully received by the FIC, if it is accepted by the FIC system, adheres to the Money Laundering and Terrorist Financing Control Regulations (Regulations), the go-AML schema and business rules and it contains correct and accurate information.

It is very important that before a reporter submits any report to FIC to check it for correctness and accuracy.

Sometimes after a reporter submits a report and it is successfully processed by the FIC system, the reporter might find that the information reported is not correct or accurate.

This section explains the process to remediate different scenarios of reports successfully submitted and processed by the FIC system but contain incorrect or inaccurate information.



**A. Report submitted with an overstated transaction value**

This applies where a report was submitted with an overstated value. The reporting entity must correct the report by submitting a new report with the correct transaction amount and in the **"Comments"** field of the report, the reporting entity must state the previously overstated transaction amount and describe the reason for the correction being made. If the correct transaction amount is less than the threshold amount, and the report was not supposed to be reported, then the reporting entity must send formal correspondence to the FIC detailing the reference numbers of the report, the transaction date and value, as well as the reason for the correction.

**B. Report submitted with an understated transaction or other value**

This applies where a report was submitted with an understated transaction or other value. The reporting entity must correct the report by submitting a new report with the correct transaction or other value and in the **"Comments"** field of the report, the reporting entity must describe the reason for the correction being made. Where a series of transactions are being reported such transactions should be aggregated when applicable and captured separately.

**C. Report submitted with incorrect client/branch/location details**

This applies where any report was submitted with incorrect client and/or branch and/or location details. In this instance, the reporting entity must correct the report by submitting a new report with the correct client and/or branch and/or location information and in the "Comments" field the reporting entity must describe the reason for the correction being made. Where a series of transactions are being reported such transactions should be aggregated when applicable and captured separately.

**D. Duplicated reports**

This applies where a duplicated report was submitted to the FIC. The reporting entity must send formal correspondence to the FIC detailing the reference numbers of the duplicated reports, the transaction dates and values, as well as the reason for the duplication.

**Process to remediate the reports submitted with incorrect/inaccurate information**

When remediating reports for all types of remediation scenarios (explained above), the reporting entity must specify the previous report number (which is the "Report ID" of go-AML submitted reports) in the "FIU reference number" field and include relevant descriptions in the "Comments" field which describes the reason for remediation and the action taken.

The reporting entity must formally confirm when the remediation process has been completed and provide the FIC with the go-AML Report ID, report type, the reporter entity's internal reference number, client information (client name and unique discriminator),

transaction date and amount is listed. Note that each transaction must be listed individually and may not be grouped or consolidated with others.

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

Inspectors appointed by the Financial Intelligence Centre (FIC), the Financial Sector Conduct Authority (FSCA) or the South African Reserve Bank (SARB) including designated supervisory bodies within the SARB, in terms of section 45A(1), who conduct inspections for the purpose of determining compliance with the FICA Act, may in terms of section 45B of the FICA Act order an accountable institution, reporting institution and/or other reporter under inspection, to produce a copy of a report, or furnish a fact(s) or information regarding a section 29 report in terms of the FICA Act that the institution submitted to the FIC.

These inspectors perform the supervisory function in terms of the FICA Act and the inspected institutions should give them access to the required section 29 report information.

Inspectors appointed by any other supervisory body are allowed access to section 29 report information held by Ais, Ris and/or other reporters with the explicit, prior written consent from the FIC.

The FIC will only provide consent following a written application, and if the criteria as set out in the Money Laundering Terrorist Financing Control (MLTFC) Regulations are met.

If, during an inspection, any supervisory body obtains a section 29 report, or a fact or information about such a report, the supervisory body must inform and request information from the FIC under section 40(1C) of the FICA Act relating to the same section 29 report, which may be relevant to the inspection.

Inspectors are appointed in terms of section 45A(1) of the FICA Act by the FIC, the FSCA and the SARB to conduct inspections for the purposes of determining compliance with the FICA Act.

The request, and receipt of section 29 report information by an inspector of a supervisory body is exercised within the general inspection powers vested in an inspector in terms of section 45B of the FICA Act.

The inspector, with specific reference to section 45B(2) of the FICA Act, may during the inspection of an accountable or reporting institution interalia:

- Request documentation relating to STRs;
- Request information relating to STRs;
- Access any physical or electric storage areas where STR document and information may be kept;
- Examine and make copies of documentation and information relating to STRs.

- Inspectors must be given access to the required section 29 report information held by the inspected reporters.

Section 45B(2B) of the FICA Act requires that when an inspector of any supervisory body obtaining a section 29 report or a fact or information about the section 29 report during an inspection, the supervisory body must inform and request information from the FIC under section 40(1C) of the FICA Act relating to the same section 29 report which may be relevant to the inspection.

- The FIC requires the supervisory body to advise the FIC, in writing, of the following:
- Confirmation that the supervisory body has requested a section 29 report and/or section 29 report information;
- Confirmation of the specific entity and organisation identity (ORG ID) number relating to the section 29 report in question; and must request the following information:
- That the section 29 report information is a true reflection as compared to the FIC's records; Timeous submission of the section 29 report by the reporter;
- Quality of information captured within the section 29 report by the reporter; and
- Completeness and accuracy of information captured in the section 29 report by the reporter.

Requests for information by the supervisory body to the FIC in relation to section 40(1C) of the FICA Act must comply with the below requirements. The request must:

- Be in writing following the request for information process;
- Be submitted by an authorised officer at the supervisory body;
- Specify the accountable institution, reporting institution or reporter;
- Specify the required information and the purpose for which the information is required;
- Specify which inspector, and any other persons, who will be receiving and reviewing the content of the FIC's information and the section 29 report information obtained;
- Provide a reasonable time period for when this information is due by the FIC, not less than 20 (twenty) business days; and
- Acknowledge that this request is subject to handling conditions.

To ensure confidentiality of the information submitted by the FIC, the Director has a discretion to, as a condition, make reasonable procedural arrangements and impose reasonable safeguards regarding the furnishing of such information before the information is provided in terms of section 40(3) of the FICA Act.

Information from the FIC is subject to handling conditions as envisaged in section 40(3) to the FICA Act. A person who obtains information from the FIC may use that information only:

- for the purpose and within the scope of that person's powers and duties in facilitating the inspection and enforcement of the FICA Act; and

- for the purpose specified in the request;
- with the permission of the FIC;
- for the purposes of legal proceedings, including any proceedings before a judge in chambers; or
- in terms of a court order.

Information obtained by persons in terms of section 40 of the FICA Act is sensitive and classified. No person is entitled to be in possession of such information unless such possession is justified in terms of sections 40 and 41 of the FICA Act.

This information may not be compromised in any way through any disclosure to any person who is not required to use the information in accordance with section 40 of the FICA Act.

The information may not be disclosed directly or indirectly to individuals or entities that form the subject matter of the information.

Confidentiality of the information is maintained before and after the information is provided.

The recipient of this information must immediately notify and forewarn the FIC of any demand or any legal proceedings (including any notice of intended legal proceedings) to seek access to or the disclosure of this information received from the FIC.

Any person who discloses a fact or information of a section 29 report or such a report, obtained during an inspection or uses information obtained from the FIC other than in accordance with any arrangements or safeguards made or imposed by the Director in terms of section 40 or 41 of the FICA Act is guilty of an offence in terms of section 60 of the FICA Act.

An inspector may only obtain information for purposes of determining compliance with the FICA Act as envisaged by section 45B(1)(b) of the FICA Act.

An inspector is not permitted to disclose any information obtained during an inspection, including section 29 report and related information to any person other than for the purposes of enforcing compliance with the FICA Act, legal proceedings and when required to do so by a court of law. This includes providing information to the subject the section 29 report or providing a fact that a section 29 report was submitted. Failure to do so is considered an offence in terms of section 60 of the FICA Act.

Failure to keep this information confidential by the inspector is deemed unauthorised disclosure, which is a criminal offence in terms of section 53 of the FICA Act.

The FIC advises that supervisory bodies should not make copies of, nor remove any physical copies relating to the content of any section 29 report or information relating to such report. The supervisory body should note the details of the section 29 report, excluding the content related to the suspicion being reported. This will reduce the potential of any information being abused by third parties and would further secure the confidentiality of sensitive information.

Supervisory bodies are only allowed access to section 29 reports, facts and information to the extent required in terms of its supervisory powers relating to the conduct of the accountable institutions under inspection.

Section 29 report information requests from supervisory bodies, **other that the FIC, FSCA and SARB, must meet certain criteria that may be determined by the Director in terms of sections 40 and 41 of the FICA Act,** before they may access any section 29 report, facts, information or reports, from either the reporting entity or the FIC.

Process to be followed by a supervisory body, other than the SARB and FSCA when a section 29 report information is required:

The supervisory body is to be in the process of conducting an inspection for the purposes of determining FICA Act compliance by the reporting entity.

The supervisory body is to first seek and obtain permission from the FIC before they may proceed requesting section 29 report information from either the FIC or the reporting entity. This permission will be provided for in writing and must be given to the reporting entity covering the request for section 29 report information.

The FIC will provide permission only if the supervisory body can demonstrate that is has met the minimum prescribed criteria. Prescribed criteria to be met for other supervisory bodies

The MLTFC Regulation 27D sets out the criteria for supervisory bodies to request information relating to a report made in terms of section 29 of the FICA Act. Such supervisory bodies must, to the satisfaction of the FIC have:

- appropriate measures to ensure that the information obtained from the section 29 report is processed only for the purposes of determining compliance with the FICA Act;
- appropriate measures to prevent unlawful access to the information contained in the section 29 report; and
- appropriate security safeguards for the protection of information contained in the section 29 report.

The FIC must advise the accountable institution, reporting institution or other persons concerned in writing of its decision on whether a supervisory body meets the prescribed criteria. Process if the prescribed criteria is not met by a supervisory body.

Should the FIC decline a request for information on a section 29 report from a supervisory body in terms of section 45B(2A)(c) of the FICA Act, the supervisory body's inspectors shall not be allowed to request and acquire access to a section 29 report or related information held by the accountable, reporting institution or other reporters.

Such supervisory bodies may only gain access to information relating to a section 29 report submitted to the FIC in terms of section 40(d) and 40(1C) of the FICA Act, from the FIC directly.

This is provided that such information is relevant to the exercise of its powers as a supervisory body or its functions under any law.

## 7. BUSINESS PROCESSES TO PROMOTE COMPLIANCE BY AIs

### 7.1. Introduction

All AIs must compile their own business specific RMCP, which is applicable to their specific environment and which suites their Risk Base Approach model, which includes all their business processes in an attempt to combat ML and TF.

### 7.2. General MMLL Standards

**All AIs within the MMLL Group structure must abide by the MMLL Group RMCP, which sets the group wide standards for the implementation of the FICA Act, which are indicated in this document.**

#### 7.2.1 Opening of bank accounts

The **process** to open a bank account at MMLL is as follows:

- Internal client will request MMLL Treasury Account Management Platform (AMP) to open an account telephonically/email.
- AMP will provide an opening account template which the clients need to complete and sign internally.
- The Account Management Platform (AMP) team prepares the bank documentation and submits it to the relevant bank who will complete the necessary bank documentation and have it signed in accordance with the DOA.
- The bank will provide a Welcome letter with the new bank details.
- This information is then provided to FACS who will assist with the back-end set-up of the account on FACS.
- The FACS team loads the account, limits and statements and prepares a test file to the bank to ensure that transactions are processed successfully.
- AMP ensures that the account gets loaded onto MDM (this is where all bank accounts are recorded across the group).
- AI's must ensure that the account is registered in the CTR library of accounts to receive payments.
- Apply for a GL and object account from JDE Support.

#### 7.2.2 Dealing with cash transactions

- No staff member/contractor or financial advisor acting on behalf of the MMLL Group may deal in cash, they are not allowed to receive funds from a client or debtor when establishing a business relationship or concluding a business transaction.

- No staff member/contractor or financial advisor acting on behalf of the MMLL Group may deposit cash or assist in depositing cash on behalf of any client to any MMLL bank account.
- No employee may suggest to a client to pay an amount in cash in to any MMLL bank account.

### 7.2.3 Receiving of funds and publishing of bank account details

It is a contravention of Section 21 of the FICA Act for an AI to accept funds from a prospective client prior to completing the Client identification and Verification requirements in terms of an agreed **Risk Based Approach and the standards implied by the FICA Act**.

It is preferred that AIs do not make their bank account details public, e.g., by including the bank details on application forms or by placing them on websites or in advertising material, to minimize the possibility that prospective clients may take the initiative to deposit funds into their respective accounts prior to the identification and verification process being completed. Instead, it is recommended that the prospective clients provide their bank account details for collection of the funds. This will enhance the bank account verification process of the contribution payer, as MMLL will then be able to follow a bank account verification process, ensuring that the prospective client's correct and valid bank account is applied for the collection of contributions.

**IMPORTANT NOTE: Should it happen that a "person" takes the initiative to deposit unsolicited funds into the bank account of the AI prior to the client identification and verification process being completed, the AI must fulfil a client identification and verification process if it was the intent of the client to establish a business relation with the AI. An accountable employee dealing with unsolicited deposit must immediately report the matter to the MLCO and the MLCO must consider the facts of the transaction, as to potentially report the behaviour to the FIC in terms of Section 29 of the FICA Act.**

**If it was not the intent of the "person" to establish a business relation with the AI, and a request for the refund of the unsolicited funds are received, an accountable employee** dealing with unsolicited deposit **must immediately report the matter to the MLCO of the business unit,** whilst the AI implements a client identification and verification process: -

- MMLL must request CDD documents, according to the applicable checklists for a natural person or a legal entity, for refunds exceeding R1 000.00 (one thousand rand);
- Refunds of unallocated funds, are a high risk for money laundering;
- AIs consider funds to be unallocated, when the funds were not applied to a contract/policy or where funds were incorrectly paid into an MMLL bank account; and
- It must be confirmed that the funds are not premium related, and the funds were unallocated or incorrectly paid to MMLL.

**The funds must be paid into the same bank account, from where the funds were received, no exceptions are permitted. (Each AI has a documented process within their RMCP.)**

The **MLCO must consider the facts and report the** transaction and the behaviour to the FIC **in terms of Section 29 of the FICA Act where it is deemed suspicious behaviour.**

### 7.2.4 Third-party Payments

**The business of MMLL has a general rule, which does not permit making payments on policies or contracts to third parties. This is an anti-money laundering and anti-fraud standard that is applied across the majority of businesses and are therefore included in the relevant Risk Management Compliance Programmes.**

As a rule of thumb, the exception is, transfers **on behalf of a client** and **between Accountable Institutions/Pension & Provident administrators** that are related to a fund transfers between retirement products e.g., Compulsory or Voluntarily annuities, are under most circumstances deemed **Low Risk Transactions** and accepted as **"third-party payments**".

Further to this, payments from retirement funds are governed by MMLL's process rules and also by the provisions of Section 37A of the Pension Funds Act; which read as follows:

Payments from retirement funds are governed not only by MMLL's process rules but also by the provisions of Section 37A of the Pension Funds Act which reads as follows:

*(4) (a) Despite the provisions of this section, a fund may direct that a member's or beneficiary's benefit may be paid to a third-party, if that member or beneficiary provides sufficient proof that he or she is not able to open a bank account.*
*(b) Any such payment must be regarded as being a payment to that member or beneficiary.*

The Rule is therefore that unless the member or beneficiary has satisfactory proof that a bank account cannot be opened in his/her/their names no third-party payments of retirement benefits are permitted.

The transfer of a business relationship of a client or a financial payment transaction in the normal course of business, from an institution to another is deemed a **High Risk transaction** and is based on the principle that no funds of a client will flow directly from a client's product or contract to another party, and only to the client, except under special circumstances, for example where a client is deceased, a curator bonus has been appointed to act on behalf of a client or on the back of a court order.

The reason that MMLL applies this standard is that a huge burden of mitigating the risk of a third-party payment is otherwise directly placed on MMLL.

To overcome this and to mitigate the regulatory and fraud risks, the additional processes required to be executed by MMLL, would include ensuring that such an instruction explicitly originates from the client, and that a complete customer due diligence client onboarding process, is then applied to the third-party etc., as under these circumstances, such a third-party will be deemed a client of MMLL.

## 7.3. Reporting Obligations and FIC Interventions

### 7.3.1 AI Reporting Institutions and persons subject to obligations to advise the FIC of client related detail (Section 27)

**Process:**

- The AI's MLRO receives a Section 27 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 MMLL Dawn Raid Policy;
- Scan the client/entity details, as provided on the Section 27 request into the AI's client database, to search for potential clients.
- If potential clients are identified, the MLCO/MLRO must further investigate the client/entity detail to ensure that the correct client is identified, and detail is relayed to the FIC.
- Feedback must be provided, by responding on the initial email received on the AI's go-AML message board or other format, as instructed by the FIC, within the prescribed time granted.
- All requests received from the FIC contains a reference code, this is the only reference code which must be used when making use of attachments on a specific request.
- Record of all Section 27 requests are stored manually and electronically, by the MLRO, for at least 5 (five) years.

### 7.3.2 Reporting of Cash transactions above prescribed limit (Section 28)

**Process:**

When a **cash** deposit exceeding the prescribed amount of R49 999.99, is received in a known bank account, in the name of the AI, the MLCO/MLRO must, within 3 business days (72 hours) from the date on the AI or any of their employees, have become aware of the transaction:

- Verify the detail and funds as correct and valid, by investigating the cash received on the client/entity contract/policy.

- Once the cash deposit has been traced and found to be valid and correct, the MLCO/MLRO must report the transaction via the FIC go-AML system.
- All the available client detail must be provided when completing CTR form on the go-AML system;
- ALL CTR must be reported within the prescribed time frame of 72 hours (3 {three} business days);
- All CTR reports submitted to the FIC must be stored manually and electronically;
- This includes the Rejection/Accepted reports received from the FIC, after a report has been submitted; and.
- All Rejected reports must be corrected and resubmitted, within 48 hours (2 {two} business days) of been rejected, until the report has been accepted.

**IMPORTANT NOTE: It is expected that all cash deposit amounts exceeding R49 999.99 deposited into any MMLL client facing bank account will be analysed by an accountable employee, will be flagged and referred and reported to the relevant ML Reporting officer on the same business day of obtaining such information. The relevance of the cash transaction(s) in terms of the client's ongoing or past transactional behaviour should also be analysed and considered as a Suspicious and Unusual Transaction reportable in terms of Section 29.**

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

An AI must within 5 (five) days of having **factual knowledge** of the fact that it has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of report:

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

**MMLL must upon publication of a proclamation by the President or a notice given by the Director of the FIC:**

- Scrutinize its information concerning clients with whom an AI have business relationships in order to determine whether any such client is a person or entity mentioned in the proclamation by the President.
- Scrutinize its information concerning clients with whom an AI have business relationships in order to determine whether any such client is a person or entity mentioned in the notice by the Director of the FIC.
- Depending on the outcome of the investigation:
- A confirmed factual case needs to be reported to the AI's MLCO/MLRO immediately, for further investigation.

- An alert must be placed on the client/entity/contract/policy number/s, for additional monitoring.
- An investigation must be finalised and reported within the given 5 (five) business days timeframe;
- The MLCO/MLRO of the AI must submit a;
    - Terrorist Finance Activity Report (TFAR); or
    - Terrorist Finance Transaction Report (TFTR), or
    - Terrorist Property Report (TPR),
- All reporting must be submitted via the AI's credentials on the FIC's go-AML system.
- All request documents submitted to the FIC must contain the relevant reference code provided, on the initial request from the FIC.
- All TFAR/TFTR/TPR reports submitted to the FIC must be stored manually and electronically.

**MMLL must upon the publication of a Proclamation by the President or a Notice given by the Director of the FIC: -**

- Scrutinise its information concerning clients with whom an AI have business relationships in order to determine whether any such client is a person or entity mentioned in the proclamation by the President.
- Scrutinise its information concerning clients with whom an AI have business relationships in order to determine whether any such client is a person or entity mentioned in the notice by the Director of the FIC.
- The MLRO must report on the findings as dictated, by the FIC.

**Role of an AI relating to the Implementation of the UNSC resolutions:**

In order for an AI to determine if they are dealing with a person or entity on the UN1267 list or Targeted Financial Sanctions List (TFS List) pursuant to Section 26A, they must scrutinize the information obtained concerning their clients as per Section 28A.

AIs must check whether their clients are listed on notices as and when published in terms of POCDATARA and Section 26A. Should a client's name match against the UN1267 list or the TFS List, the AI MUST ensure that it is an exact match, by conducting a further investigation on the details provided.

Once the AI has determined that it controls relevant property, it is required to report full particulars of the type of property concerned and a description of the property connected in relation to which the terrorist property report is made.

An AI must within 5 (five) days of having factual knowledge that it has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of report:

- Any entity which has committed or attempted to commit or facilitated the commission of the financing of terrorism or related activities, as defined on the POCDATARA, 33 of 2004.
- A specific entity identified in a notice by the President, under Section 26A of the FICA Act (This list is known currently as the TFS List.).
- A sanctioned person or entity identified on the UNSC sanctions list.

**Current World-Check screening Process:**

- Screening must be implemented at:
  - The client onboarding process; and
  - When new lists are adopted and published. (MMLL implement daily check to identify existing client's)
- May not alert person/entity of status as sanctioned person/entity;
- May not acquire, collect or use property of such persons/entity –prohibited;
- May not transact or process transactions for sanctioned persons/entity.
- Status quo as at time of imposition of sanction in relation to property or funds must be maintained.
- No financial services may be provided to the person or entity –except in instance where Minister of Finance has permitted certain financial services or dealings with the property.
- Accountable institution must report to FIC the property in its possession/under control which is owned or controlled by or on behalf of a person or an entity identified on the sanctions list (Section 26A).
- The AI's MLCO/MLRO must report to the FIC, by means of the go-AML facility.

**IMPORTANT NOTE: This in short means that MMLL is prohibited to transact with a sanctioned person or entity. MMLL must report to the FIC, the property which MMLL is in possession of or has control of, which is owned or controlled by a person or entity on the sanction list.**

### 7.3.4 Reporting of Suspicious and Unusual transactions: STR's (Section 29)

**A suspicious or unusual transaction report (STR)** is a report which must be electronically submitted to the FIC in respect of proceeds of unlawful activities or money laundering where the report relates to transactions or a series of transactions between two or more parties.

There are 3 (three) reporting obligations under section 29 of the FICA Act:

- Money Laundering (STR/SAR)
- Terrorist Financing (TFTR/TFAR)
- Financial Sanctions (STR/SAR)

It is important to note that section 29 of the FICA 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 FICA 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).

**An AI or any person who carries on a business or is in charge of or manages a business or who is employed by a business and who knows or ought to have reasonably known or suspected that:**

- An AI received or is about to receive proceeds of unlawful activities or property which is connected to an offense relating to the financing of terror and related activities.
- A transaction or series of transactions to which an AI is a party to facilitate or is likely to facilitate the transfer of the proceeds of unlawful activities or the property which is connected to an offense relating to financing of terror activities and related activities.
- A transaction or series of transactions to which an AI is a party that has no apparent business or lawful purpose.
- A transaction or series of transactions to which an AI is a party that may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty or levy imposed by legislation administered by the Commissioner for the South African Revenue Services.
- A transaction or series of transactions to which an AI is a party that relates to an offense relating to the financing of terrorist and related activities.
- A transaction or series of transactions to which an AI is a party that relates to the contravention of prohibition relating to persons and entities identified by the UNSC sanction list.
- AI representatives of MMLL must refer any suspicious transactions or enquiries to their MLCO or Head of Compliance in their area, who will investigate the issue and who will in turn report the case, if it is deemed suspicious, to the MMLL Group MLCO or relevant MLRO appointed for that particular AI, before the close of business on that day.
- Any submission reported to the FIC will be stored in an access-controlled database to ensure the confidentiality of the person making the report.
- Must report the details of such a transaction(s) and the basis of the knowledge or suspicion concerning the transaction electronically to the FIC, as soon as possible, but not later than fifteen (15) days of becoming aware of the fact concerning a transaction.

**Automated transaction monitoring system (ATMS) for the detection and submission of regulatory reports**

In addition to the manual reporting and monitoring system of suspicious and unusual transactions, an AI may also use and implement an automated transaction monitoring system (ATMS) which permits the AI to discharge its obligation to submit regulatory

reports to the FIC in terms of the FICA Act read together with Regulation 24(3) of the Money Laundering and Terrorist Financing Control Regulations.

An ATMs which is utilised and implemented in an AI must be structured on the behavioural reporting of clients as well as trigger events. An ATMS relates to the monitoring of transaction activity only, and once an alert regarding a suspicious and unusual transaction has been generated, the 15 (fifteen) day reporting period starts.

AIs who have implemented ATMS should adhere to the following requirements:

- AIs are required to attend to all alerts generated by the ATMS within 48 hours of an alert being generated, which is included in the 15 (fifteen) day period within which STRs must be submitted to the FIC;
- AIs are deemed to have knowledge of the possible suspicious and unusual activity when an alert is generated;
- The Board of Directors, Senior Management or other person or group of persons exercising the highest level of authority in an AI is responsible to ensure the effectiveness of the compliance function of an AI and must have adequate oversight over the process of implementing the ATMS, alert management, adequacy of rules and or scenarios implemented including testing thereof, and reporting to the FIC arising from alerts generated by the ATMS;
- Responsibilities regarding reviewing, investigating and reporting alerts generated by the ATMS within the respective organisations must be clearly allocated to a person with the appropriate level of skill required to perform this function, and must be regularly trained to identify unusual and suspicious activities;
- All investigations and decisions taken relating to alerts generated by the ATMS must be adequately documented, and kept in a manner readily accessible to the respective AIs' relevant supervisory body or the FIC where applicable;
- The AI should ensure that adequately skilled staff are appointed to deal with the volumes of alerts generated by the ATMS and that there should be adequate resources to ensure timeous reporting and to prevent the creation of a backlog of unattended alerts;
- Where a suspicious or unusual transaction or activity is detected by an AI in an instance other than through the ATMS, the AI must ensure that the ATMS detection rules are developed and implemented to enable future detection of similar scenarios via the ATMS;
- The fact that an AI uses an ATMS must not prevent the AI from receiving manual reports from internal stakeholders regarding suspicious and unusual activity or transactions;
- AIs must ensure that the detection methodology and effectiveness of an ATMS are validated and tested to ensure that the system is detecting potentially suspicious and unusual transactions or series of transactions, resulting in the generation of high-quality alerts, and is being effectively utilised by the AI;

- AIs must include the process of reporting information to the FIC and the investigation of automated alerts in the AI's RMCP;
- The effectiveness of the ATMS must be periodically reviewed and approved, at least annually by the Board of Directors, Senior Management or other person or group of persons exercising the highest level of authority in the AI and in accordance with the AI's RMCP;
- The ATMS must be subject to ongoing risk assessment and calibration (tuning) and such risk assessment and tuning methodology should be included in the RMCP of the AI;
- All configuration changes to the ATMS must follow a documented governance procedure, must be adequately tested and significant changes must be authorised by the Board of Directors, Senior Management or other person or group of persons exercising the highest level of authority prior to implementation;
- A clear audit trail must always exist to demonstrate what changes, configurations, additions or withdrawal of rules and scenarios have occurred, as well as when the changes took place and the responsible person/s that effected these changes;
- AIs must ensure that the detail relating to the detection methodology including algorithms, scenarios, threshold settings or rules used by the ATMS are set out accurately and clearly, and is documented and is included in the RMCP;
- AIs must ensure that the detection methodology, including algorithms, scenarios, threshold settings or rules used by the ATMS are sufficient to address the associated money laundering and terrorist financing risks applicable to the reporter;
- Where an AI is a subsidiary or a branch of a foreign based organisation which also utilises an ATMS, the reporter must have procedures in place to ensure its usage of the ATMS is adequately customized for its domestic money laundering and terrorist financing risk within the domestic reporting regime;
- For AIs to have branches, departments and partnering agents (such as mobile service providers), the ATMS must monitor the clients and transactions effected by agents;
- Where an AI is utilising more than one ATMS which operates independently of each other, it must ensure that the systems utilised do not prevent an AI from having a holistic view of both the alerts generated and the total number of suspicious and unusual transaction or activity reports submitted in respect of a specific client of an AI.
- AIs must make available to the FIC or to the AIs relevant supervisory body, on request, reports relating to the results of an evaluation of the ATMS.

**Examples of deemed a Suspicious Transaction:-**

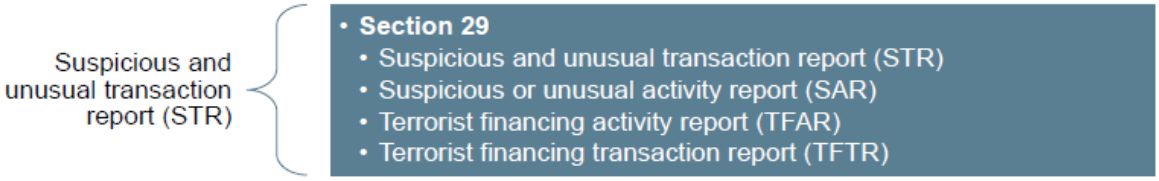
- New business or existing business transactions, where the proper identification of client/s cannot be established or information related to the identification and verification process is suspicious;

- Where the AI cannot obtain information about the business relationship with the client, in terms of the AI's RMCP;
- Where the AI cannot conduct on-going CDD on the client, in terms of the AI's RMCP;
- 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;
- 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;
- Application for a policy from a potential client in a distant place where a comparable contract could be provided "closer to home";
- Application for business outside the policyholder's normal pattern of business;
- Any transaction or suspicious transaction that involves an undisclosed party;
- 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;
- The transfer of the benefit of a product to an apparently unrelated third-party (e.g., outright cessions);
- Requests for a large purchase of a lump-sum contract where the policyholder's history shows small, regular payment contracts;
- Attempts to use third-party funding to purchase a policy;
- The applicant shows no concern for the performance of the policy but much concern for the early cancellation of the contract;
- 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;
- The applicant requests to make a lump-sum payment by a wire transfer or in foreign currency;
- The applicant appears to have policies with several institutions;
- The applicant purchases policies in amounts considered beyond the client's apparent means or income.

**Process:**

- Once a suspicious transaction or suspicious activity has been identified, the case must be reported to the AI's MLCO/MLRO, before close of business on the same day;
- The MLCO/MLRO will further investigate the transaction to establish validity of the suspicion.
- An alert must be placed on the client/entity/contract/policy number for additional monitoring and Senior Management must be advised;
- Depending on the outcome of the investigation, a decision must be made to either report the transaction or to further monitor the transaction to control behavioural issues;

- If the transaction is deemed as suspicious, it must be reported within a 15 (fifteen) business day timeframe;
- The MLCO/MLRO of the AI must submit a STR or SAR, depending on the outcome of the investigation;
    - Suspicious Transaction Activity Report (SAR); or
    - Suspicious Transaction Report (STR), or
    - Terrorist Financing Transaction Report (TFTR), or
    - Terrorist Financing Activity Report.




**"SAR"** refers to a suspicious or unusual activity report submitted in terms of section 29(1)(a), (c) or 29(2) of the FICA Act in respect of the proceeds of unlawful activities or money laundering, or suspicious or unusual activity in terms of section 29(1)(b)(vi) relating to the contravention of a prohibition under section 26B of the FICA Act, where the report relates to an activity which does not involve a transaction between two or more parties or in respect of a transaction or a series of transactions about which enquiries are made, or in respect of an incomplete, abandoned, aborted, attempted, interrupted or cancelled transaction, but which transactions has not been concluded, respectively.

**"STR"** refers to a suspicious or unusual transaction report submitted in terms of section 29(1)(b)(i) to (iv) of the FICA Act in respect of the proceeds of unlawful activities or money laundering and 29(1)(b)(vi) relating to the contravention of a prohibition under section 26B of the FICA Act where the report relates to a transaction or a series of transactions between two or more parties.

**"TFAR"** refers to a terrorist financing activity report submitted in terms of section 29(1)(a), (c) or 29(2) of the FICA Act in respect of the financing of terrorist and related activities where the report relates to an activity which does not involve a transaction between two or more parties or is in respect of a transaction or a series of transactions about which enquiries are made or in respect of an incomplete, abandoned, aborted, attempted, interrupted or cancelled transaction, but which transactions has not been concluded, respectively.

**"TFTR"** refers to a terrorist financing transaction report which must be submitted in terms of section 29(1)(b)(v) of the FICA Act in relation to the financing of terrorist and related activities where the report relates to a transaction or series of transactions between two or more parties.

Information to be provided in a section 29 Report.

In terms of regulation 22 of the MLTFC Regulations a report in terms of section 29 of the FICA Act must be filed with the FIC electronically, via the FIC's go-AML facility.

Further the MLRO in terms of section 29 of the FICA Act, reports electronically to the FIC in accordance with the requirements of regulations 23, 23A, 23B or 23C of the MLTFC Regulations.

| Type of report | Applicable Regulations |
|---|---|
| STR | Regulation 23 |
| SAR | Regulation 23A |
| TFTR | Regulation 23B |
| TFAR | Regulation 23C |

- All reporting must be submitted via the AI's credentials on the FIC's go-AML system.
- All available information must be provided whilst completing the said report on the client/entity in question.
- All SAR/STR reports submitted to the FIC must be stored manually and electronically.
- This includes the Rejection/Accepted reports received from the FIC, after a report has been submitted; and
- All Rejected reports must be corrected and resubmitted, within 48 hours (2 business days) of being rejected, until the report has been accepted.

Reactive reporting refers to the submission of a STR, SAR, TFAR and/or TFTR to the FIC following an external prompt without a prior suspicion having been formed based on the circumstances in which a particular transaction/activity or series of transactions/activities have been conducted. Examples of the prompts that may give rise to reactive reporting are:

- Receiving a subpoena in terms of section 205 of the Criminal Procedure Act, 1997 (Act No 51 of 1997) or a similar process to provide evidence concerning matters relating its business dealings with a particular customer.
- Receiving a request to confirm whether a person is a customer of an institution in terms of section 27 of the FICA Act in respect of a particular customer, MMLL will only report if there is reason for suspicion.
- Receiving an intervention order in terms of section 34 of the FICA Act in connection with a transaction involving a particular customer.
- Receiving a monitoring order in terms of section 35 of the FICA Act concerning the transactions of a particular customer.
- Receiving other types of enquiries from government agencies such as investigating authorities or the South African Revenue Service about a particular customer.

- The discovery of any adverse information whilst conducting on-going due diligence of a customer.
- Seeing information in the media that may adversely affect a particular customer.

**IMPORTANT NOTE:**

According to Public Compliance Communication 42 dated, 28 February 2020, Inspectors appointed by the Financial Intelligence Centre (FIC), the Financial Sector Conduct Authority (FSCA) or the South African Reserve Bank (SARB) including designated supervisory bodies within the SARB, who conduct inspections for the purpose of determining compliance with the FICA Act, may in terms of section 45B of the FICA Act order an accountable institution, reporting institution and/or other reporter under inspection, to produce a copy of a report, or furnish a fact(s) or information regarding a section 29 report in terms of the FICA Act that the institution submitted to the FIC. These inspectors perform the supervisory function in terms of the FICA Act and the inspected institutions should give them access to the required section 29 report information.

Inspectors appointed by any other supervisory body are allowed access to section 29 report information held by AIs, and/or other reporters with the explicit, prior written consent from the FIC. The FIC will only provide consent following a written application, and if the criteria as set out in the Money Laundering Terrorist Financing Control (MLTFC) Regulations are met.

If, during an inspection, any supervisory body obtains a section 29 report, or a fact or information about such a report, the supervisory body must inform and request information from the FIC under section 40(1C) of the FICA Act relating to the same section 29 report, which may be relevant to the inspection.

There may be instances when a client's transaction or series of transactions will give rise to more than one reporting obligation. This would mean that the AI would be required to submit more than one type of report, for the same transaction, to the FIC, for example, a STR and a CTR.

Section 33 of the FICA Act provides that a reporter may continue with and carry out a transaction in respect of which a report is required to be made unless the FIC directs the reporter not to proceed with the transaction in terms of section 34 of the FICA Act.

### 7.3.5 Reporting on the Conveyance of Cash to and from the Republic (Section 30)

**This section is not yet enforced.**

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

**This section become effective on 1 February 2023.**

All electronic cross-border transactions (the sending of funds out of South Africa and the receiving of funds from outside of South Africa) from a prescribed value of R20 000 and above must be reported to the FIC.

The terms of section 31 of the FICA Act applies to only certain categories of the AIs who are authorised to conduct the business of cross-border electronic transfers.

These institutions are authorised in terms of the Regulations under the Currency and Exchanges Act, 1933 (Act 9 of 1933) The Exchange Control Regulations) to conduct authorised transactions under these Regulations.

AIs with this authorisation are:

- Authorised Dealers (ADs);
- Authorised Dealers with Limited Authority (ADLAs);
- A category of Financial Services Providers (FSP) that have a direct reporting dispensation under the Exchange Control Regulations; and
- The Post Office.

FNB/RMB is the MMLL preferred AD, who acts on behalf of MMLL and who is responsible for the filing of IFTRs, as soon as possible or at latest within 72 hours after FNB had become aware of the transaction.

All cross-border transactions will be submitted to the FIC, by the AD, via the AD's go-AML facility, within the prescribed timeframe.

It is thus of utmost importance that all AIs who participate in cross-border transactions must ensure that they have access to a client's most recent, correct and valid client information.

### 7.3.7 Reporting procedures and furnishing of additional information (Section 32)

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

### 7.3.8 Intervention by the FIC (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 (ten) days. For the purposes of calculating the period of 10 (ten) 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 FIC considers it appropriate, to inform and advise an investigating authority or the National Director of Public Prosecutions regarding the transaction.

### 7.3.9 Monitoring Orders (Section 35)

Section 35 of the FICA Act is only applicable to AIs 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).

### 7.3.10 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 any person, provided that it is:**

- A specified person or entity that is or has been a client of an AI or person.
- A specified person acting on or that has acted on behalf of any client of an AI or person.
- A client of an AI or person is acting or has acted for a specified person.
- 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.
- The type and status of a business relationship with a client of an AI.

**Process:**

- If a person claiming to be a representative of the FIC insists on access to any records held by MMLL, MMLL staff must refer the request for information to the MMLL 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 MMLL Dawn Raid Policy.

MMH Dawn Raid
Guidance Note 09202

- 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.)**
- 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.

- In the event that a printout of the electronic records of MMLL 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 MMLL's electronic records.
- The MLCO will keep a record of all requests for information from the FIC, manually and electronically.

### 7.4. Record Keeping

**IMPORTANT NOTE:** In terms of exemption 4, an AI could previously 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 MMLL 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 MMLL AI obtain all relevant CDD documentation. Therefore, in those cases where a MMLL AI does not have CDD information and documentation on record, a full CDD process will be required for all investment instructions, new business, ad hoc investments etc.

An AI must retain records in the following manner:

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:

- Internal networks.
- Physical storage devices.
- Cloud storage.
- Fintech capabilities.
- Electronic document repository.
- The records must be stored in a safe and secure location which is tamper free.

**Process:**

MMLL must keep a record of all documentation relating to a client or a transaction.

**Hard Copy/Manual Storage**

- All documents are scanned onto the AI's Business Process Management (BPM) system.
- Original sources are to be boxed as per the AI's preferred method of filing.

- **Records should be stored for example by:**
  - The client's identity number.
  - The reference number on the policy or the contract number.
  - The reference number of the business correspondence.
  - Relevant dates of issuing or expiring.

    - Details of the writer, etc.
    - The AI can make use of a commercial third-party, who provide such a service, to store all original and boxed documents.
- AI's must ensure that their records are easily accessible and that the retrieval of data and/or documents as envisaged under the FICA Act.

**Electronic Storage**

- All documents are scanned onto the AI's Business Process Management (BPM) system.
- Electronically retained records can be reproduced in a legible format.
- 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.
- AIs must safeguard and ensure that there are controls in place such as firewalls that will safeguard against anyone tampering with the electronic data.

There are many examples of mechanisms which may be used for the storage of records which allow AIs to reduce the volume and density of records, such as:

- Internal networks;
- Physical storage devices e.g., hard drives, CDs, DVDs, memory sticks, etc.;
- Cloud storage;
- Electronic document repositories; and
- Fintech capabilities.

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

- The AI must have free and easy (in other words unencumbered) access to the relevant records;
- The records must be readily available to the FIC and the relevant supervisory body when required;
- The records must be capable of being reproduced in a legible format; and
- If the records are stored off-site the FIC and the relevant supervisory body must be provided with the details of the third-party storing the records.

It is advisable that records should include details that will assist in the identification of the records such as:

- Reference numbers on documents or letters;
- Relevant dates, such as issue or expiry; and
- Details of the issuer or writer.

AIs must ensure that records are tamper proof and that there are safeguards in place to prevent the unauthorised access to information stored electronically.

AIs which operate in groups of companies may implement group-wide policies on record-keeping which may include centralised storage of records.

AIs which 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 to provide assurance to the relevant supervisory body that the AI can access and retrieve data and/or documents as envisaged under the FICA Act.

**Important note: PCC 12 Summary:** AIs remain responsible for compliance with their obligations in terms of the FICA Act regardless of their internal arrangements relating to the manner in which those obligations are met.

An AI may utilise the services of a third-party to perform activities relating to the establishing and verifying of clients' identities as well as the collection of required documents to establish and verify the identity of their clients, and for record-keeping purposes as required in terms of the FICA Act and the Regulations to the FICA Act. However, an AI remains liable for compliance failures associated with and/or caused by such an outsourcing arrangement.

The following records are of vital importance:

- Application forms or onboarding forms/data;
- The identification and verification documents (documents submitted by the client for the purpose of verifying the details of the client);
- Details about the nature of the transaction, accounts and amounts involved;
- Details of the person who obtained the information on behalf of the AI;
- These documents must be kept for 5 years after the business relationship has ended, i.e., from the date of maturity/date of surrender/date of lapse/date of pay-out/date of repurchase of the policy or Investment contract;
- Sections 22 and 22A of the FICA Act instructs MMLL to take reasonable steps to maintain the correctness of particulars of clients, which are susceptible to change. MMLL should verify the client's details as per that client's risk rating level and when specific significant changes take place on a client profile;
- Based on the risk-based approach it is recommended that MMLL should verify particulars of clients, at any stage when MMLL interacts with the client;
- Any change in particulars should be dealt with in accordance with the CDD process.
- According to section 42 of the FICA Act, AIs must provide for the manner and processes to be implemented group-wide for all its branches and majority owned subsidiaries, to enable the institution to comply with the requirements of the Act.
- This extends to the exchange of information within its branches or subsidiaries relating to the analysis of STRs.

AIs are required to have adequate safeguards to protect the confidentiality of information exchanged, as per the company's internal POPIA policy.

### 7.5. Training

The FICA Act training is provided to all AI employees.

Regular general awareness assessments are carried out on all employees, who must pass the assessments. These assessments are loaded and monitored by MMLL Learning and Development in conjunction with Human Resources and the Compliance function.

The current FICA Act Risk Management Compliance Programs for MMLL and its subsidiaries are available to all employees, on the MMLL Intranet, under Policies and Procedures.

Also available on the MMLL Intranet site is the MMLL Fraud and Ethics Reporting Line, MMLL Fraud Guidance Note and the MMLL Fraud Risk Management Policy on Managing Commercial Crime, Bribery and Corruption, Employee Misconduct and Money Laundering.

Details regarding the type and frequency of training of employees, are documented in each of the different AI's RMCPs, as they are business specific.

## 8. THE CUSTOMER DUE DILIGENCE PROCESS

Each AI within the MMLL group structure has developed, documented and maintain the processes in the separate RMCP's relating to their specific business unit.

### 8.1. A Risk Based Approach

**The AI's agreed Risk Based Approach** will determine the level of Client Due Diligence that will be required:

- Simplified Due Diligence Process (Low Risk)
- Standard Due Diligence Process (Medium Risk)
- Enhanced Due Diligence Process (High Risk)

**Process:**

**By following the processes described in this document:**

- Establish a relationship with a client by applying client identification and verification processes.
- Establish the risk rating of a client by means of:
- Utilising a risk rating — engine
- Or apply a risk rating mechanism that included all client and product factors necessary.
- Apply a risk base approach to manage client onboarding/client identification and verification, apply a continuous behavioural monitoring process relevant to the risk the client present, the risk of the relationship and the risk of specific transactions.

This continuous monitoring would include managing the risks relevant to Trigger Events

**Examples of Trigger Events:**

- A request to change the bank details.
- Fund withdrawal requests received.
- Cancellation of contract where CDD has not previously been implemented.
- Changes to physical address.
- Specific contract alteration requests e.g., increase in premiums.
- Ad hoc/Voluntary payments received.
- Changes in contract ownership.

### 8.2. Establishing a relationship with a client

**Establishing a relationship** with a client is the process where a client approaches or is approached with either **the intent or not**, to establish a business relationship or conclude a single transaction regarding the offering by an AI of a service or product. In this regard it is required to establish and verify at this time:

- The identity of the client;
- Identity of the person acting on behalf of the client; or
- Identify the client acting on behalf of another person.

Face-to-Face client interactions normally carry less risk than **non-face-to-face interactions** when dealing with the identification and verification of a client. AIs are required to apply equally effective CDD procedures and on-going monitoring standards for non-face-to-face clients.

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 Customer Due Diligence** procedures for non-face-to-face Clients:

- Request of additional documentation that complement 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
- 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.

**Acting on behalf of a client:**

The following are examples of documents that may be accepted to confirm the authority of a person to act on behalf of another person and to confirm the particulars of the person authorising the third-party to establish the relationship:

- power of attorney;
- mandate;
- resolution duly executed by authorised signatories; or
- a court order authorising the third-party to conduct business on behalf of another person.

#### 8.2.1 Enhanced client due diligence process when establishing a business relationship with high-risk clients

Engaging High Risk clients will require an AI to implement appropriate measures and controls in order to reduce the potential risk that high-risk clients may pose to an AI. Some of the measures that can be undertaken by the AI to understand or reduce a risk are as follows:

- Reinforcement of the measures for knowing the client and reinforced analysis of the client (CDD);
- Increasing the requirements for account approval and establishing business relationship with the client;
- Increased monitoring and analysing of the transactions;
- Increased level of continuous control of the business relationship with the client.

### 8.3. Establishing a client's source and the origin of wealth/income and source of funds

#### 8.3.1 Process to establish the source of wealth of the client

**This process is relevant to Natural and Legal persons**

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 on-going monitoring.

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.

An AI must determine if/what the client's status is:

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

### 8.3.2 Establishing and verifying the source of funds related to a transaction

Identification of source of funds for specific transactions is required: -

- When an AI concludes the establishment of a business relationship with a client and expects any funding for a single or continuous transactions;
- When there is a change of banking details related to a client or contract and the AI updates the banking details.
- When there is a change of premium payers or contributors to a contract and the AI have to update the identity of the premium payers or contributors.

This process is required to enable AIs 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 (e.g., proof of address).

**Note: AIs 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.**

**Requirements:**

- If the contribution/premium payer is different from the contract owner/holder an AI has to 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.
- Where new or never provided before bank account details are provided, MMLL will implement a bank account verification process in an attempt to verify the bank account detail in the name of the client or appointed premium payer/contribution payer.
- Only if the bank account details are confirmed in the name of the account holder and that MMLL has authority to make use of the given account for the collection of premiums, will the case be accepted.

**Bank account verification (BAV)** (FACS process versus manual process):-

Each AI within the MMLL group structure has developed, documented and maintain the processes in the separate RMCP's relating to their specific business unit.

Electronic Bank Account Verifications are implemented via the MMLL financial and Account Control System (FACS). This enables users to capture the bank account details directly on to our client data, after which the details are submitted via FACS, to validate the detail against the Bankserv records.

Basic verification detail which must be captured are as follows:

- Client or entity Name.
- Client identity number or entity registration number.
- Bank branch code.
- Bank account number.
- Type of bank account.

The detail will be returned with Yes/No indicators, together with a result confirming if the bank account is older than 90 days or not.

All the information captured in the verification process, must validate correctly.

If the bank account details verify as correct, but younger than 90 days, the case will be routed to the AI's CDD Teams for further scrutinizing.

If the bank account details do not validate in the name of the client, the User must follow the preferred method of communication selected by the said banking institution. The specific bank is to be contacted as per their preferred communication instrument, either via telephone, email or facsimile.

Manual bank account verifications will also be implemented on banks who do not reside within the Bankserv domain or banks which are outside of South Africa's borders.

All AIs will have a documented process within their environment.

**Electronic Fund Transfer (EFT) Process:**

**Direct Bank deposit:**
Where a client makes a deposit directly to an AI bank account the requirement of a copy of a deposit slip that provides detail with regards to the origin of the funds (i.e., who is funding the transaction/ source of funds) exists.

Acceptable detail on a deposit would be a deposit slip** that reflects the following:

- Name of beneficiary (MMLL);
- Account number from where payment/transfer was made;
- Accountholder name;
- Date of deposit;
- Amount deposited; and
- Contract/policy number to which funds should be allocated.

******The deposit slip must reflect the account holder name and at least the last 4 digits of the bank account number from where the funds were paid. This will enable the AI to implement a bank account verification processes to confirm if the bank account belongs to the contribution payer/premium payer indicated on the completed application forms received, for example, the new business, ad hoc or alteration forms. If the bank account detail does not match to the available detail a full CDD process on the contribution payer is required.

### 8.4. Identification of clients or prospective clients and persons acting on behalf of clients

MMLL has preferred **checklists** that provide guidance and specific standards for the onboarding and maintenance of client details as the basis for CDD which deal with the different categories of clients with whom an AI may establish a relationship.

These checklists contain very specific requirements relating to the identification and the verification of information relating to the client.

**The verification** of the client's identity can be validated by appointing a reliable and independent third-party source, who has been assessed for accuracy on the information validated**. MMLL will only accept validations confirmed via the original source, which in the verification of South African citizens will be the Department of Home Affairs.**

AIs making use of electronic data sources to verify a prospective client's identity remain responsible and accountable in their own capacity for compliance with the requirements of the FICA Act.

All detail as indicated on the appropriate checklist must be provided and all supporting documents as indicated on the checklist/s must be provided, **taking into account the specific Risk the client pose.**

- Natural person or sole proprietor.
- Closed Corporation.
- Partnership.
- Listed Company.
- Private Company.
- Foreign Company.
- Trusts.
- Other Legal Persons:
  Stokvels/churches/clubs/schools/municipalities/homeowner associations, etc.
- FPEP.
- DPEP/DPIP.

### 8.4.1 Identification and verification of details of Natural persons

Each AI within the MMLL group structure has developed, documented and maintain the processes in the separate RMCP's relating to their specific business unit and products available.

**Information about a natural person's identity** may be further supplemented by applying other attributes including: -

- His/her physical appearance or other biometric information;
- Place of birth;
- Family circumstances;
- Place of employment or business;
- Residential address;
- Contact particulars (e.g., telephone numbers, e-mail addresses, social media);
- Contacts with the authorities (e.g., tax numbers); or
- Links with another AI.

## 8.5. Natural Persons: Establishing a client's FPEP or DPEP/DPIP Person status

AIs need to establish if a prospective client or existing client is a FPEP or DPEP/DPIP. AIs must consider each such relationship on its own merits to determine whether there is any reason to conclude that it brings a higher risk of abuse for money laundering and terrorist financing purposes.

Business relationships with FPEPs must always be considered as high-risk. If an AI finds out that it is dealing with an official:

- It should obtain Senior Management approval for establishing business relationships with a DPEP/FPEP/DPIP;
- When the client has been accepted, the AI should be required to obtain Senior Management approval to continue the business relationship;
- It should take reasonable measures to establish the source of wealth and the source of funds of customers and the beneficial owners identified as DPEPs/DPIPs/FPEPs;
- It should conduct enhanced ongoing monitoring of a relationship.

The notion of Senior Management in an AI is determined by the size, structure, and nature of the institution.

The appropriate level of seniority for approval should also be determined by the level of increased risk associated with the business relationship. The senior manager approving a business relationship with a prominent public official should have sufficient seniority and oversight to take informed decisions on issues that directly impact the institution's risk profile.

When considering whether to approve a business relationship with a prominent person, Senior Management should base their decision on the level of ML/TF risk the institution would be exposed to if it entered into that business relationship and how well equipped the institution is to manage that risk effectively.

The responsibility regarding final decisions on business relationships with prominent persons should be clearly described. In all cases, it is best to document the approval or refusal by those involved in writing.

AIs must ensure that all their client onboarding application forms, alteration forms, withdrawal or ad hoc forms contain the PIP definition and question which needs to be completed by the client.

The client's DPEP/DPIP/FPEP status needs to be identified by the AI and record must be kept of the client's status.

**An Enhanced Due Diligence processes is required on all DPEP/DPIP/FPEP clients:**

All clients must be regularly screened against World-Check (WC) as to identify a status change in respect of a DPEP/DPIP/FPEP status. See World-Check section 8.5.1

- During normal course of business, a relevant DPEP/DPIP/FPEP status question should be asked when specific transactions (trigger event) on existing contract/s is received for processing.
- If the response to the DPEP/DPIP/FPEP question is: "Yes", the contract must be diverted to Senior Management or a dedicated AML administrator. The AML administrator further conducts a search on WC and if a positive match on WC is

established it is reported to Senior Management for consideration and process sign-off.

- In the event of a trigger event (change physical address/change bank account details/withdrawals/ad-hoc investments) the Service Specialist must request the relevant CDD documents and details.
- The CDD documents should be used to compare and verify the client's information to the information on contract/Policy Administration systems, Credit Bureau information etc. as to ensure an EDD process.

### 8.5.1 Identification of DPEP/DPIP/ and family member or known associate as clients include:

- Head of state or head of a country or government.
- Member of a foreign royal family.
- Government minister, deputy minister or equivalent senior politician.
- Leader of a political party.
- Senior judicial officer.
- Senior executive of state-owned corporation.
- High ranking member of the military.
- President or deputy president.
- Premier of a province.
- Member of an executive council of provinces.
- An executive mayor of a municipality and municipal managers.
- A member of a royal family or senior traditional leader.
- Director-Generals and Chief Financial Officers of government departments.
- Chief Executive Officers and Chief Financial Officers of state entities like Eskom, Telkom, FIC, PRASA, NGB, etc.
- Judges.
- Leader of a political party.
- Senior officials of companies that receive certain tenders form government.
- Ambassador or high commissioner or other senior representative of a foreign government
- Senior officials of companies that receive certain tenders from government.
- Includes family members and known close associates.

**The following individuals are considered as a family member or known associates of a DPEP/DPIP, but the list is not exhaustive:**

- Spouse or civil/life partner.
- Previous spouse or civil/life partner.
- Children and stepchildren and their spouses or civil/life partners.
- Parents.
- Siblings and step siblings and their spouses or civil/life partners.

- Business partners or associates who share beneficial ownership of corporate vehicles with the prominent person, of 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.

In a situation where an AI establishes that a client is a domestic prominent influential person, authorisation must be obtained from an accountable senior manager before establishing a business relationship.

**Further to this the following actions are required:**

- Clients DPEP/DPIP status must be captured and updated on a relevant database;
- The DPEP/DPIP must be added to an enhanced ongoing monitoring list;
- The relevant ongoing monitoring activities must be implemented and managed.

### 8.5.2 Identification of the following FPEP and family member or known associate as clients:

- 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.

Once an AI has established the client's status as a FPPO, authorisation must be obtained from an accountable senior manager before concluding a transaction or establishing a business relationship. In addition, the following precautionary procedures must be followed:

- Clients DPEP/DPIP/FPEP status must be captured and updated on a relevant database;
- The DPEP/DPIP must be added to an enhanced ongoing monitoring list;
- The relevant ongoing monitoring activities must be implemented and managed.

### 8.5.3 Identification of refugees/asylum seekers

AIs can accept the permit that the Department of Home Affairs issue to refugees as proof of identity (provided that the AI has verified the information of the permit with the Department of Home Affairs). 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.

**Current process:** This monitoring list is entrusted to the CDD Teams within the AI's who implements additional monitoring and analytics upon any movements on a contract or client, which has been identified as a DPEP/DPIP/FPPO.

#### 8.5.4 Natural Persons: Utilising the World-Check facility and MMLL RedFlags Facility

**Not yet enforced.**

The **World-Check** (WC) Risk Intelligence database consists of information about heightened risk individuals and entities. MMLL is a subscriber to this facility provided by Thomson-Reuters. As part of data protection regulations and legislative obligations, World-Check provides AIs with assurance that an individual or entity may be for example be included in the Terrorism category, Sanction lists, etc.

The MMLL RedFlags database of "negative entities" is daily maintained through data analysis and feedback from the Group Forensic Services investigators and business areas. Currently it contains entities, including multiple variations of some names: doctors, undertakers, ID numbers, hospitals, bank account numbers, phone numbers and policy numbers that are flagged as either suspicious or based on past fraudulent or negative behaviour displayed against MMLL.

### 8.6. A Legal Person is any person other than a natural person, that establishes a business relationship or a single transaction with an AI which includes domestic companies, foreign companies, close corporates, and any other corporate arrangements such as Stokvels, churches, NGO's and schools, excluding a trust, partnership or sole proprietor.

#### 8.6.1 Legal Persons

The following process must be followed when implementing **Enhanced Due Diligence** measures relating to **legal persons:**

- The CDD checklist relating to legal person must be completed and the supporting documents required by the checklist must be attached.
- Additional requirements may be imposed on the legal person.

#### 8.6.2 Closed Corporations

- All relevant documentation of individual person required by the CDD checklists.
- Reasonable information of beneficial ownership

### 8.6.3 Partnerships

Partnerships are not legal incorporated entities and do not have legal personalities as it is only established by a mutual agreement between natural persons and liability is embedded with the individual persons. The process of CDD on Natural Persons must be followed on all parties.

Where possible reasonable sources of information and the information must be used to collaborate or verify the identity of the partnership.

- All relevant documentation of the partnership and individual person/s is required as per the CCD Checklists.
- Information of all partners, including silent partners.

### 8.6.4 Listed Companies

- All relevant and reasonable documentation of the business and listing information as per the CDD Checklists.
- Reasonable Information of beneficial ownership.

### 8.6.5 Private Companies

- All relevant documentation of the business and individual person/s is required as per the CDD Checklists.
- Reasonable Information of beneficial ownership.

### 8.6.6 Foreign Companies

- All relevant documentation of the business and individual person/s is required as per the CDD Checklists.
- Reasonable Information of beneficial ownership.

### 8.6.7 Trusts:

- The CDD checklist relating to trusts must be completed and the supporting documents required by the checklist/s must be attached.
- Additional requirements may be imposed on the legal person.

## 8.7. Establishing Beneficial Ownership

The **"beneficial owner"** in respect of a legal person is the natural person(s) who independently or together with another person, owns the legal person or exercises effective control of the legal person.

AIs are required to establish who the **beneficial owner(s) or "warm body" of the legal person is** and take reasonable steps to verify the beneficial owner's identity.

In summary: -

- Beneficial ownership refers to the natural person(s) who owns or exercises effective controls the client.
- Beneficial ownership applies to legal persons, partnerships and trusts.
- The lack of adequate, accurate and timely beneficial ownership information facilitates ML/TF by disguising:
  - The identity of known or suspected criminals;
  - The true purpose of an account or property held by the legal entity; or
  - The source or use of funds or property associated with the legal entity;
  - The establishment of beneficial ownership is important for two reasons:
    - Understand the customer profile to properly assess the ML/TF risks associated with the business relationship.
    - Understand who the ultimate beneficial owner is.

FATF recommendations provides for a process of elimination which AIs must follow to determine who the beneficial owner/s of a legal person is: -

- The process starts with determining who the natural person is who, independently or together with another person, has a controlling ownership interest in the legal person. The percentage of shareholding with voting rights is a good indicator of control over a legal person as a shareholder with a significant percentage of shareholding, in most cases, exercises control. In this context ownership of 25 per cent or more of the shares with voting rights in a legal person is usually sufficient to exercise control of the legal person.

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.

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.

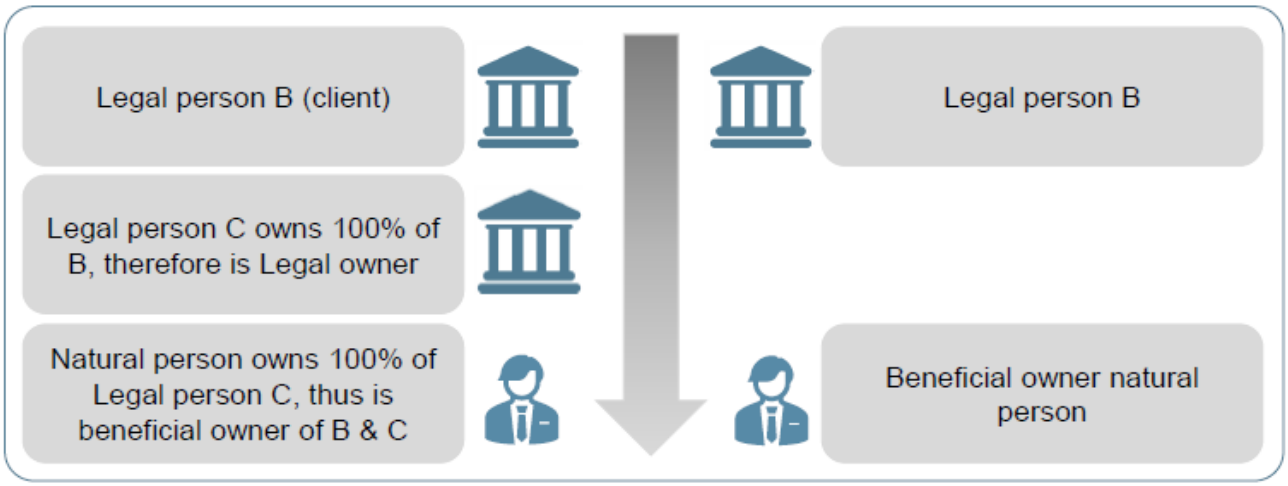
**Once the AI has determined who the beneficial owner of a legal person is, the institution must take reasonable steps to verify that person's identity.** AIs must employ the requirements, as per the appropriate checklist to verify the details of the natural person. Once the relevant CDD documents have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

The concept of legal owner in comparison to beneficial owner:

An AI must firstly establish the legal owner, to enable the AI to establish the ultimate beneficial owner, in other words:

If a client is a legal person, for example, a trust, a drill down into the trust's trustees, founder, beneficiaries and trust beneficiaries, needs to be conducted, if there is a further legal person, who is for example, a registered company or another type of legal entity, a further drill down is required until such time as the identities of the ultimate beneficial owner is discovered. Similar to the below process:

The legal owner of a legal person B can be legal person C, where legal person C is then owned by a natural person/s. The natural persons are the actual beneficial owners of legal person B.




### 8.8. Identification and verification of clients' physical address

**An AI must verify the client's residential or business address** by comparing these particulars with information which can reasonably be expected to achieve such verification and is obtained by reasonably practical means.

The **MMLL CDD checklists provide a list of acceptable documents** which may be submitted as proof of physical address. It is important to note the dates for which a document is acceptable.

It would be sufficient to review the original document and to obtain a copy of a document that offers a reasonable confirmation of the information in question. The client needs to provide the AI with an acceptable address verification document which is current or as per the specified dates indicated on the appropriate checklist.

A validation process should be followed by an AI and may include a validation process that has reliance on a trusted third-party vendor which encompasses an electronic footprint from the vendor as part of the validation process.

The electronic address validation process is also to be implemented via the appointed creditable service provider.

### 8.9. False client information/anonymous clients

AIs need to know the identity of a prospective client/the client **and therefore an AI is prohibited** from dealing or transacting with: -

- An anonymous client in the process of establishing a business relationship with AI.
- An anonymous client in the process of entering into a single transaction with AI.
- A client acting under a false or fictitious name in the process of establishing a business relationship with AI.
- A client acting under a false or fictitious name entering into a single transaction with AI.

Where a client refuses to provide requested documentation or information the business relationship should be discontinued once the client has been informed of the potential implications and given time to respond accordingly.

AIs should give special consideration to whether the circumstances that prevent them from conducting CDD are suspicious or unusual.

If a case is deemed suspicious or unusual, it must be reported to the AI's MLCO/MLRO before end of business on the same day, who will report the transaction as per Section 29 of the FICA Act.

If funds have been paid into a bank account in the name of the AI, the funds will not be released without the necessary CDD documents and proof of payment. No refunds are permitted.

If the relevant CDD documents have been received, MMLL will only refund to the same account from which the funds were received.

### 8.10. Confirmation of information relating to a client when doubts about the veracity of previously obtained information exists

When an AI is **doubtful of the authenticity of information which was previously collected** on a client, **the institution must repeat the client due diligence process to confirm the authenticity of the information** in question and verify this information.

**Process:**

- Repeating the CDD process to confirm the authenticity of the information in question.
- Verifying this information by use of a reliable third-party electronic database.
- Requesting additional information from client.

- If the client fails to provide relevant information or further information cannot be reasonable verified the following actions needs to be taken:
  - Senior Management must be advised of the facts and the information must be recorded.
  - A hold must be placed on any future transactions.
  - The MLCO who must consider a Section 29 report to the FIC.

### 8.11. Continuous due diligence and account monitoring

All AI needs to conduct continuous due diligence and account monitoring on:

- Complex transactions which have no apparent business or lawful purpose;
- Unusually large transactions which have no apparent business or lawful purpose;
- Unusual transaction patterns which have no apparent business or lawful purpose;
- Investing the withdrawing funds;
- Withdrawal of funds without consideration to penalties/commissions;
- Transfer of funds between different platforms;
- Funding contract by withdrawing funds from one contract to fund another contract;
- Rolling of premiums, withdrawals before debit collection and receiving the same funds when debit order run takes place;
- New lump sum investments followed by maximum withdrawal request shortly after acceptance of business;
- Cancellations within “cool-off” period and refunding to different account/s; and
- Third-party payment requests.

## ANNEXURE 1: SECTION 27: ACCOUNTABLE INSTITUTION'S OBLIGATIONS TO ADVISE FIC OF CLIENTS

**Roles and Responsibilities:**

The MMLL MLRO receives a notice via email, informing the MLRO that a message has been submitted to the AI, via the go-AML notice board, which needs to be attended to.

The MLRO accesses the go-AML notice board to view the Section 27 request is received.

Section 27 requests are received on an "as and when" frequency and must be responded to within the timeframe indicated on the request.

It is the responsibility of the MLRO to initiate the process in gathering the requested information from the AI's, to ensure that the feedback provided to the FIC is correct, accurate and within the said timeframe.

**Process:**

**Natural and Juristic clients**

- 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.
- The MLRO will request the MMLL Business Intelligence unit to trace any matches or potential matches to existing MMLL clients.
- A template is populated with the information as received from the FIC.
    - Name and Surname;
    - ID;
    - Registration number;
    - Date of Birth.
- This information is then submitted as part of an automated process to look for matches across various platforms within MMLL.

**The results are interrogated as follows:**

**Natural client:**

- ID number matches are obtained from the ID number match list;
- 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.
    - 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:**

- Company registration number matches are obtained from the company registration number match list;
- Name matches:
  - If 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.
  - There must be a high probability for the name match, i.e., exact or near exact name match.

**Bank accounts**

- Bank account numbers are not yet part of the existing automated process, but queries are processed on an ad-hoc basis.
- The account number provided by the FIC is “run” against the MMLL financial systems (FACS) to establish if MMLL 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. The MLRO reports the transaction/s to the FIC on the go-AML system, as per the prescribed process, namely via the go-AML facility.

The MLRO must store manual and electronic copies of all reports submitted for a minimum of 5 (five) years.

**ANNEXURE 2: SECTION 28: CASH THRESHOLD REPORTING**

**Roles and Responsibilities:**

MMLL has an automated system which reads cash values received in the different AI's bank accounts, by reading identifying indicators on the MMLL bank account statements. In addition to this daily AML files are received from ABSA, FNB and Standard Bank, with Nedbank to follow. This is to cater for bank accounts that are not administered in FACS or where bank statement data is not received.

Once a reportable transaction is identified, an email alert is sent to the MMLL MLRO, via the MMLL Key Risk Identifying System (KR1S*), informing the MLRO, that a cash payment greater of equal to R49 999.99, has been identified on the bank account statements, of an AI.

The MLRO immediately interrogates the alert received to ensure that the funds received were cash and that it does exceed the daily threshold.

Once confirmed, the MLRO will establish the ownership of the funds and whether it was a single deposit greater than or equal to R49 999.99, within the allotted time.

Once ownership and value has been established, the MLRO must report the receipt of cash within 72 hours (3 {three} business days), from the date on which the AI or any of their employees, have become aware of the transaction, to the FIC via the go-AML facility.

**Process:**

- The data is transmitted from the commercial banks to MMLL.
- All the data files are loaded into a Data Warehouse (DW), where data is examined per bank and per data source viz, bank statement/bank file to include/exclude Narratives or Transaction Codes in order to detect cash deposit transactions.
- Data is loaded into a combined Cash Threshold Report table stored in the Data Warehouse (DW), where possible duplicates from the data sources are identified and removed.
- The KR1S* report reads the combined CTR table.
- The MLRO is Alerted of CTR transactions within the set criteria, by means of an email generated by KR1S*.
- Once the interrogation process has been finalized, the MLRO compiles a feedback report to the FIC. The MLRO reports the transaction/s to the FIC on the go-AML system, as per the prescribed process, namely via the go-AML facility.
- In instances where cash funds are deposited into a MMLL bank account, without any contract number or the new business case has not yet been captured with the client's detail, the value is recorded on the relevant Errors report, e.g., AML00091 for Momentum Retail, AML00093 for Wealth, AML00105 for Investments.
- Upon receipt of the client information, the case must be reported immediately and the date of which the funds were deposited must be noted in the report, submitted to the FIC, informing their office of the delayed receipt of the client detail.
- The MLRO will also inform the AI's MLCO of the CTR submitted to the FIC.
- The FIC report number is recorded on the relevant KR1S* report.

- Once the report has been submitted, the FIC will respond to the submitted report by issuing an “Approval or Rejection” report.
- If the report is “Approved”, the Approval report must be stored manually and electronically.
- If the report was Rejected, the MLRO must investigate the reason for the failure and correct the report within 48 hours (2 {two} business days) before re-submitting the report for approval.
- The MLRO must store all responses received from the FIC as manually and electronically.
- The MLRO only has 30 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 (five) years.

## ANNEXURE 3: SECTION 28A: PROPERTY ASSOCIATED WITH TERRORIST AND RELATED ACTIVITIES AND FINANCIAL SANCTIONS PURSUANT TO UNSC AND TFS LISTS

**Roles and Responsibilities:**

The business unit who identified the individual or entity on the TFS or UNSC List, must immediately inform the MMLL MLRO that a potential client or an existing client, has been identified on the World-Check system as a potential match to an individual or entity noted on the TFS List or UNSC 1267 list.

It is the responsibility of the MLRO to immediately initiate the process in scrutinizing potential hit, to determine whether the client is noted on the said lists.

Section 28A requires an AI, to file a report with the FIC if the AI knows that it possesses or controls property of a person or entity which has committed or attempted to commit or facilitate the commission of a specified offence as defined in the FICA Act A and/or is identified in a notice issued by the President under Section 28A of the FICA Act and/or a person or an entity identified pursuant to a UN resolution as contemplated in a notice referred to in Section 26A(1) of the FICA Act.

The knowledge about the origin and ownership of the property in question is based on fact and should be acquired with reference to an objective set of circumstances or facts (as opposed to a suspicion that is formed subjectively).

When a reporting obligation arises in terms of Section 28A of the FICA Act, regarding a client, that is the client of more than one accountable institution in a complex group structure, each accountable institution that has in its possession or under its control property owned or controlled by, or on behalf of, or at the direction of a natural person or entity listed in terms of POCDATARA and/or Section 26A(1) of the FICA Act must submit a separate TPR to the FIC.

**"TPR"** refers to a terrorist property report which must be submitted in terms of Section 28A of the FICA Act.

**"TFS List"** means the Targeted Financial Sanctions List pursuant to Section 26A of the FICA Act.

**Permitting financial services and dealing with property**

The Minister of Finance may in writing and on conditions that he/she has considered appropriate and in accordance with the United Nations Security Council Resolution, allow an AI to permit a sanctioned person or entity to conduct financial services or deal with property affected by a sanctions order, to allow such person or entity access to basic living expenses such as:

- Rent or mortgage.
- Food (groceries).
- Medicine or medical treatment.

- Taxes.
- Insurance premiums.
- Maintenance orders.
- Public utility charges.
- Reasonable professional fees.
- Reimbursement of expenses associated with legal services.

The Director of the FIC must give notice of written permission from the Minister of Finance to MMLL and other interested parties. This must be done by means of publishing the notice containing the permissions and conditions thereto on the FIC website.

**Process:**

Same basic process as per Section 27 (Addendum 2) is followed, **as above**:

- If a partial match or a match is identified, an additional investigation is performed to establish if the individual or entity is in fact involved in terrorist activities or in the funding of terrorism.
- The MLRO within GFS must be notified of the potential hit, by the AI's MLCO. The GFS MLRO must investigate and scrutinise the individual's or entity's profile without delay to establish the identity, of the client.

**The MLRO will implement various checks to establish the true identity of the client:**

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

- Several ad hocs & withdrawals soon thereafter (PDS/CCF premium history/Gemstone/Lighthouse);
- Changing/updating of personal information often, especially bank account details;
- Unexplained ad hocs & withdrawals;
- Attempts for 3rd party payments;
- Incomplete CDD documents etc. (AWD/Activity Viewer);
- DPEP/DPIP/FPEP status;
- Previous/existing contracts and behaviour on these contracts;

**Check:** Electronic Systems and Media

- TransUnion: ITC details (Full names/Address/Contact details/Occupation etc.).
- Experian: ITC details ((Full names/Address/Contact details/Occupation etc.).Google searches relating to fraud/corruption & adverse media searches;
- Electronic Media searches, Facebook, Linkedin, etc.
- World-Check: Searches for clients on a data base. 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.
- Windeed: Provides details of companies that the client is/was a member on.

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

No person may enter into any transaction or establish a business relationship with persons or entities on the TFS List. Should the AI identify that they have a client or a prospective client that is specifically listed on the TFS List, they would have a reporting obligation in terms of Section 28A of the FICA Act. As a consequence of reporting to the FIC, an AI institution is required to freeze the clients' accounts and services provided.

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, via the go-AML facility.

The AI 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.

- Once the appropriate report has been submitted to the FIC, the FIC will respond to the submitted report by issuing an "Approval or Rejection" report.
- If the report is "Approved", the Approval report must be stored manually and electronically.
- If the report was Rejected, the MLRO must investigate the reason for the failure and correct the report within 48 hours (2 {two} business days) before re-submitting the report for approval.
- The MLRO must store all responses received from the FIC manually and electronically.
- The MLRO only has 30 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 (five) years.

**DPEP/DPIP/FPEP**

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

**DPEP/DPIP/FPEP BUSINESS RULE PRINCIPLES**

**Natural party:**

**1) Name matching**

- If name similarity >= 90% on full name (full name = first name, second name + surname) or permutations thereof, in other words, using name transposition, then proceed to next matching criteria, otherwise discard.

**2) Date of birth comparison**

- If no date of birth is captured for client, then proceed to next matching criteria.
- If a valid date of birth is captured for client or date of birth within 1 year and World-Check is a 100% date of birth match, then proceed to next matching criteria.
- If World-Check date of birth contains value of '00' as the day, then use the World-Check year of birth for approximate year of birth comparison.
- If no date of birth or year of birth populated on World-Check. Derive a year of birth by using the variable "WORLD-CHECK AGE DATE (AS OF DATE)" and "World-Check age".
- Allow for a difference of 1 year either side. (-1,0,1) and proceed to next matching criteria. If no World-Check date of birth or age captured, but name match = 100%, then proceed to next matching criteria.
- If derived year birth of not within 1 year of client year of birth, then discard.

**3) Gender matching**

- Where valid gender exists on both the client and World-Check, World-Check will apply auto resolution using gender.
- Match the gender of the client and the gender as defined on World-Check.
- If the gender captured on the line of business system or on World-Check is not male or female, then keep the record for review if all other matching criteria was satisfied.
- If gender was captured as male or female on client and World-Check, then proceed with matching if the gender is the same.
- If the gender is different, but the date of birth is the same, then continue with processing.

**4) Country**

- Natural party has provided an RSA ID number:

  I.e., Line of business system has a 13 digit SA ID number captured for the client, with the 11th digit = "0".
  If you were born in South Africa, then it is expected that one of the World-Check country fields contain a reference to South Africa. Therefore, World-Check country or location must contain South Africa, otherwise discard.

  It is recommended that at minimum the country of location should be populated as part of the World-Check screening process in order to enable auto resolution. AIs can also populate the place of birth and/or citizenship to enable further auto resolution.

- Natural party has not provided an RSA ID e.g., Passport number:

I.e., Line of business system does not have a 13 digit SA ID number captured for the client, or the 11th digit <> "0".
No exclusion based on World-Check country. Keep for review if all other matching criteria passed.

**Overarching principles:**

- Once a DPEP/DPIP/FPEP always a DPEP/DPIP/FPEP.
- If any one of the directors or members of a Juristic is a DPEP/DPIP/FPEP then the Juristic will be classified as a DPEP/DPIP/FPEP.
- 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:**

- No match found–- no rows returned. The business process may continue with their process.
- One or many rows returned – These transactions must follow an "unhappy path" to enable further investigation.
- World-Check screening will be provided to enable business to extract the relevant data from the World-Check data base.
- Business must arrange access to TransUnion ITC data base or the like to enable further investigations.

**What will be written away to Compliance Due Diligence data base (CDD)**

- Results from the World-Check match plus the World-Check reference number up to a max of 10 (ten).
- Results from the investigation. This is needed for reuse later on.

**APPLYING THE UNITED NATIONS SANCTIONS LIST**

The sanctions matched criteria will include the same logic as per the PIP conditions listed above.

**Outcome from the Sanction list search:**

- No match found–- no rows returned. Business process to continue with the transaction. A KR1S* alert will be triggered for Charlotte Archer, the MMLL MLRO at Group Forensic Services, who will further investigate.
- The MLRO will investigate and update the CDD data base with the positive or negative result and reroute the transaction to the specific AI.
- A positive result will be blocked on CDD and only the MLRO and CDD Teams will have access to this data.
- If the client is on the TFS list and no exemption is granted by the President or Minister, the client's existing contract/s will be "frozen" immediately.
- If it is a new business application, the AI may not enter into a business relationship with the client.

- If the client is a positive match on the TFS list, but he has been exempted by the President or minister, the MLRO, will refer the case to the AI's MLCO, to escalate to for Senior Management to decide whether they want to on-board the client or not.
- The MLRO will report the transaction to the FIC, by means of a TPR on the go-AML site.
- Once the appropriate report has been submitted to the FIC, the FIC will respond to the submitted report by issuing an "Approval or Rejection" report.
- If the report is "Approved", the Approval report must be stored electronically and manually.
- If the report was Rejected, the MLRO must investigate the reason for the failure and correct the report within 48hours (2 {two} business days) before re-submitting the report for approval.
- The MLRO must store all responses received from the FIC as hardcopies and electronically.
- The MLRO only has 30 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 (five) years.

## ANNEXURE 4: SECTION 29: SUSPICIOUS AND UNUSUAL TRANSACTION REPORTING

**Roles and Responsibilities:**

Each AI is responsible for the reporting of a suspicious and unusual transaction to the MLRO, in the prescribed format.

The MMLL MLRO receives an email alert, from the Compliance Officer within the specific AI, containing details on the suspicious transaction, in the prescribed manor, to enable further investigation.

It is the responsibility of the MLRO to immediately investigate the case reported, to determine whether the matter is reportable and to establish further actions to be implemented (Pg. 61). It is of utmost importance that the MLRO reviews the client's complete MMLL Portfolio, to establish a holistic view of the client's behaviour, before compiling a report.

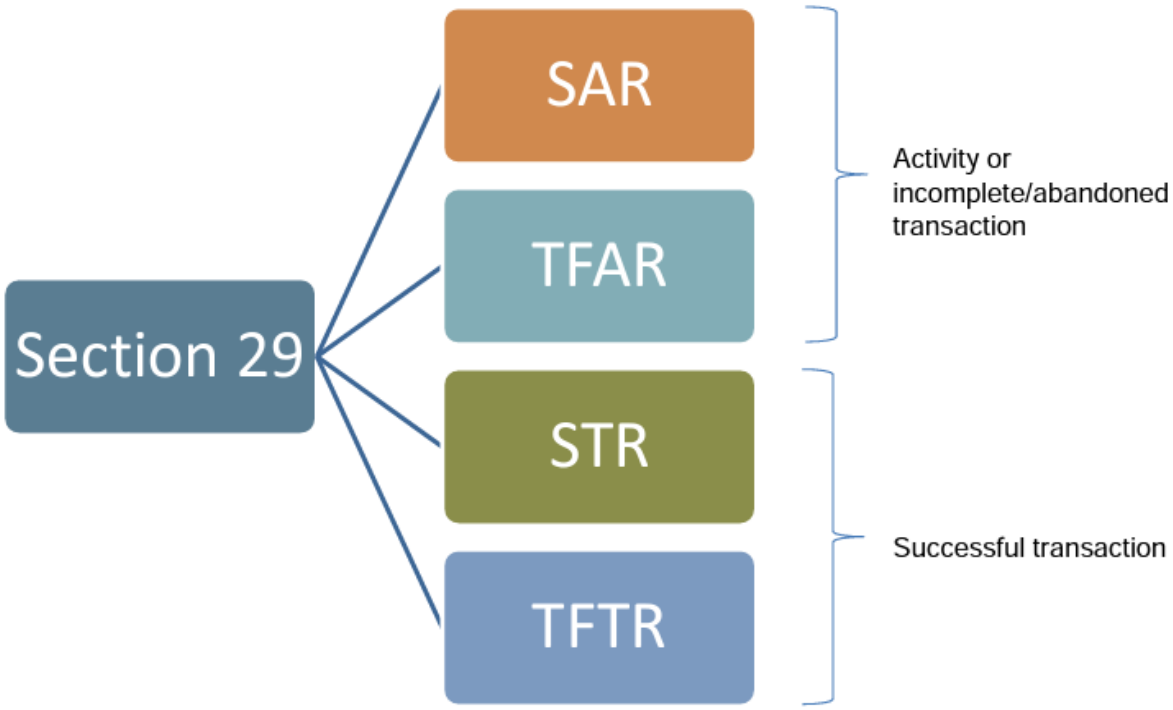
**Process:-**

Once a suspicious transaction has been identified, the staff member must complete an Anti-Money Laundering Report (STR templet):

- This report must be presented to the MLCO of their Business Unit.
- The facts must be discussed, and the matter reviewed.
- Where appropriate, additional information must be provided relating to the client or transaction if it is relevant to the matter under consideration.
- 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.
- Suspicions must not be discussed with anyone other than direct management, the Business Unit MLCO and the MMLL 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.
- Any discussion of this nature would risk a tipping-off offence.
- Staff should at all times neither confirm nor deny the existence of a report to the client or to a third-party.
- Any correspondence that could indicate the existence of a report should not be placed in the client's file.
- Once the report has been finalised, it must be presented to the MMLL MLRO, who in turn will acknowledge its receipt in writing or ratification.
- The staff member will then receive guidance from the MLRO on how to proceed with the client in question.
- In particular, if the client demands that subsequent transactions be executed, the situation must be discussed with the MMLL MLRO before any action is taken.
- In certain cases, the MMLL MLCO may decide to allow transactions to continue in order not to raise the client's suspicions. Regardless, the MMLL MLCO should be kept informed of all subsequent dealings with the client.
- The process is handled exclusively by the MMLL MLCO.

- The MMLL 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.
- If the MMLL MLCO judges that the transaction has remained suspicious, the MLRO will make an official report to the FIC via the go-AML system.

The correct type of STR report to be submitted must be decided on, according to the results of the information gathered:




- A SAR must be submitted in respect of when a suspicion relates to the proceeds of unlawful activity, or money laundering activity or a contravention of prohibitions under S26B of the FICA Act:
  - Where the report relates to an activity which does not involve a transaction between two or more parties; or
  - In respect of a transaction or a series of transactions about which enquiries are made but which has not been concluded.
  - In respect of a transaction which has been incomplete, interrupted, aborted, abandoned and ultimately not concluded.
- A TFAR must be submitted when a suspicion relates to the financing of terrorist and related activities:
  - Where the report relates to an activity which does not involve a transaction between two or more parties; or
  - In respect of a transaction or a series of transactions about which enquiries are made but which has not been concluded.
- A STR must be submitted when the suspicion is in respect of a complete transaction or series of transactions relating to the suspicion or knowledge of the proceeds of unlawful

activity or money laundering and regarding a transaction or series of transactions relating to a contravention of prohibitions under section 26B of the FICA Act.

- A TFTR must be submitted when the suspicion is in respect of a transaction, or series of transactions relating to terrorist financing and related activities.
- All reports made to the FIC must be stored manually and electronically by the MMLL MLRO
- The initiating staff member will receive an acknowledgment of the receipt of report, from the MLRO confirming that their personal legal obligations in terms of this policy have been met.
- Once the report has been submitted, the FIC will respond to the submitted report by issuing an “Approval or Rejection” report.
- If the report is Approved, the Approval report must be stored electronically and manually.
- If the report was Rejected, the MLRO must investigate the reason for the failure and correct the report within 48hours (2 {two} business days) before re-submitting the report for approval.
- The MLRO must store all responses received on a STR submitted, manually and electronically.
- The MLRO only has 30 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 (five) years.
- The MLRO keeps record of all STRs submitted to the FIC for record and future use purposes, relating to on-going monitoring between the various AIs.
- According to section 42 of the FICA Act, AIs must provide for the manner and processes in which group-wide of an AI for all its branches and majority owned subsidiaries is implemented so as to enable the institution to comply with the requirements of the Act.
- This extends to the exchange of information within its branches or subsidiaries relating to the analysis of STRs.

AIs are required to have adequate safeguards to protect the confidentiality of information exchanged, as per the company’s internal POPIA policy.

**ANNEXURE 29A**

**SECTION 29 REPORTING TEMPLET**

**MML LIMITED**

## SUSPICIOUS AND UNUSUAL ACTIVITY REPORT FORM

### DETAILS OF CLIENT BEING REPORTED:

Full name:

Address (registered if required):

Postal: Physical:

Telephone numbers (as appropriate):

Home:

Work:

Cell:

Email:

Identity /passport / company registration No:

Income Tax Number:

Name of organization client represents or works for:

Capacity:

Bank account details (If applicable):

**Nature of Suspicion:**

**Reasons for Suspicion:**

Manager Referred To:

Name:

Position:

Contact details:

Manager's Comments:

Attach any copy of supporting documentation to this report. Including

Name of Staff Member making this Report:

Contact details:

Date handed to MLRO:

SIGNATURE:

**Provide clear and concise information.**

| | |
|---|---|
| **Who?** | **The subject is 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 or transaction was completed or attempted** |
| **Why?** | **Results of the AI's investigation into why the activity/transaction is Reported/suspicious?** |

**Always provide a clear reason for suspicion in the report.**

**ANNEXURE 5: SECTION 30: CONVEYANCE OF CASH TO OR FROM SOUTH AFRICA**

**This section is not yet enforced.**

## ANNEXURE 6: SECTION 31: ELECTRONIC TRANSFERS OF MONEY TO OR FROM SOUTH AFRICA

**This section was enforced on 1 February 2023.**

All electronic cross-border transactions (the sending of funds out of South Africa and the receiving of funds from outside of South Africa) from a prescribed value of R20 000 and above must be reported to the FIC.

In terms of section 31 of the FICA Act applies to only certain categories of the AIs who are authorised to conduct the business of cross-border electronica transfers.

These institutions are authorised in terms of the Regulations under the Currency and Exchanges Act, 1933 (Act 9 of 1933) The Exchange Control Regulations) to conduct authorised transactions under these Regulations.

AIs with this authorisation are:

- Authorised Dealers (ADs);
- Authorised Dealers with Limited Authority (ADLAs);
- A category of Financial Services Providers (FSP) that have a direct reporting dispensation under the Exchange Control Regulations; and
- The Post Office.

FNB/RMB is the MMLL preferred AD, who acts on behalf of MMLL and who is responsible for the filing of IFTRs, as soon as possible or at latest within 72 hours after FNB had become aware of the transaction.

All cross-border transactions will be submitted to the FIC, by the AD, via the AD's go-AML facility, within the prescribed timeframe.
It is thus of utmost importance that all AIs who participate in cross-border transactions must ensure that they have access to a client's most recent, correct and valid client information.

**ANNEXURE 7: SECTION 32: REPORTING PROCEDURES AND FURNISHING OF ADDITIONAL INFORMATION**

**Roles and Responsibilities:**

The MMLL MLRO receives a notice via email, informing the MLRO that a message has been submitted to the AI, via the go-AML notice board, which needs to be attended to.

The MLRO accesses the go-AML notice board to view the Section 32 request is received.

Section 32 requests are received on an "as and when" frequency and must be responded to within the timeframe indicated on the request. It is usually received on a report previously submitted to the FIC, in which additional information is requested.

It is the responsibility of the MLRO to initiate the process in gathering the requested information from the AI's, to ensure that the feedback provided to the FIC is correct, accurate and within the said timeframe.

The Section 32 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 MMLL Dawn Raid Policy.

**Process:-**

The FIC will provide the client detail, based on a report reference number, previously submitted to their offices, either by means of a Section 27, 28, 28A, or 29.

MMH Dawn Raid
Guidance Note 09202

- 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.
- All information must be provided as per the Section 32 request within the given time frame.
- All AIF/AIFT reports submitted to the FIC must be stored manually and electronically.
- This includes the Rejection/Accepted reports received from the FIC, after a report has been submitted.
- 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.
- All Rejected reports must be corrected and resubmitted, within 48 hours (2 {two} business days) of been rejected, until the report has been accepted.
- The MLRO must store all responses received on a AIFT submitted, manually and electronically.
- The MLRO only has 30 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 (five) years.

**ANNEXURE 8: SECTION 34: INTERVENTION BY FIC**

**Roles and Responsibilities:**

The MMLL MLRO receives a notice via email, informing the MLRO that a message has been submitted to the AI, via the go-AML notice board, which needs to be attended to.

The MLRO accesses the go-AML notice board to view the Section 34 request is received, in the name of a specific AI.

Section 34 requests are intervention orders, in which MMLL is instructed to place a transaction/s on hold for a period of 10 days, whilst their offices further investigate the matter.

It is the responsibility of the MLRO to inform the specific AI's MLCO of the instruction and to place a hold on the transaction/s, until such time as the FIC grants MMLL further instructions. The MLRO will also gather any additional information to submit to the FIC, via the go-AML message board.

An AI will receive a Section 34 request, on the go-AML message board or 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 MMLL Dawn Raid Policy.

**Process: -**

The FIC will provide the client detail, based on a report reference number, previously submitted to their offices, either by means of a Section 27, 28, 28A, or 29.

MMH Dawn Raid
Guidance Note 09202

- The MLCO/MLRO must without delay act upon the instruction received from the FIC.
- An alert needs to be placed on the said transaction/client/contract/entity.
- The specific MLCO within the AI, must be informed of the Section 34 request received on a transaction/client/entity/contract/policy.
- Line of business must provide on-going monitoring of the transaction/client/contract entity to ensure that no unauthorised movements are processed.
- The MLCO/MLRO must report any additional relevant information with regards to any change in client behaviour or any further information received or established.
- Once the said 10 (ten) 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.
- 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.
- All communication and reports submitted to the FIC must be stored manually and electronically.

- All Rejected reports must be corrected and resubmitted, within 48 hours (2 {two} business days) of been rejected, until the report has been accepted.
- The MLRO only has 30 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 (five) years.

## ANNEXURE 9: SECTION 35: MONITORING ORDERS

**Roles and Responsibilities:**

The MMLL MLRO receives a notice via email, informing the MLRO that a message has been submitted to the AI, via the go-AML notice board, which needs to be attended to.

The MLRO accesses the go-AML notice board to view the Section 35 request is received.

Section 35 requests are monitoring orders, in which the AI is instructed to follow specific instructions in an attempt to monitor a client's transaction/s.

It is the responsibility of the MLRO to inform the MLCO in the specific AI, of the orders received and what the FIC's expectations are.

The MLCO/MLRO must without delay act upon the instruction/s received from the FIC.

**Process:**

The FIC will provide the client detail, based on a report reference number, previously submitted to their offices, either by means of a Section 27, 28, 28A, or 29.

Line of business must provide on-going monitoring of the transaction/client/contract entity to ensure that no unauthorised movements are processed.

The MLCO/MLRO must report any additional relevant information with regards to any change in client behaviour or any further information received or established.

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 MMLL Dawn Raid Policy.

MMH Dawn Raid
Guidance Note 09202

- The MLCO/MLRO must without delay act upon the instruction/s received from the FIC.
- An alert needs to be placed on the said transaction/client/contract/entity.
- Line of business must be informed of the Section 35 request received on a transaction/client/entity/contract/policy.
- Line of business must provide on-going monitoring of the transaction/client/contract entity to ensure that no unauthorised movements are processed.
- The MLCO/MLRO must report any additional relevant information with regards to any change in client behaviour or any further information received or established.
- Monitoring and reporting of the transaction/client/contract entity needs to be ad heard to as per the prescriptions of the Section 35 request, weekly, monthly etc.

- The MLCO/MLRO must report the requested information as per the instruction received.
- 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.
- 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.
- All communication and reports submitted to the FIC must be stored manually and electronically.
- 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.
- All Rejected reports must be corrected and resubmitted, within 48 hours (2 {two} business days) of been rejected, until the report has been accepted.
- The MLRO only has 30 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 (five) years.

**ANNEXURE 10: INCORRECT PAYMENTS RECEIVED FROM NON-CLIENTS**

**Process**:

- Upon receipt of a written refund request the MMLL Financial Administrator must follow the following steps:

**The Financial Administrator must verify the details, by:**

- Establishing if the funds were received from a MMLL vendor or client;
- Establish if the funds were received from a legal entity or a natural person;
- Once this information has been established, the Financial Administrator must obtain the following documents, if it has not already been received:-

**If the erroneous payment was received from a legal entity, the following is required**:

- A formal letter or email from the authorized signatory of the entity, explaining the error;
- Proof of deposit/payment into MMLL's bank account, indicating the:
  - Date of the deposit;
  - Value of the deposit paid;
  - Account number from where the funds were paid;
  - Account number into which the funds were paid;
  - Name of the account holder;
- This can be done by obtaining a bank statement from the entity, containing the required information or the entity's bank can confirm the above-mentioned detail, by means of a letter from the bank.
- The said entity must also provide the relevant details and documents, as per the appropriate CDD checklist, e.g., Unlisted Company, CC etc.
- Once the relevant details and documents have been received and noted as correct;
- The Financial Administrator must execute the bank account verification process **BEFORE** refunding the funds, to ensure that it is in the name of the entity and that it is the same account, from where the funds originated.

- If the erroneous payment was received from a **natural person,** the following is required:
  - A formal letter or email from the person explaining their error;
  - Proof of deposit/payment into MMLL's bank account, indicating the:
  - Date of the deposit;
  - Value of the deposit paid;
  - Account number from where the funds were paid;
  - Account number into which the funds were paid;
  - Name of the account holder;
  - This can be done by obtaining a bank statement from the person, containing the required information or the person's bank can confirm the above-mentioned detail, by means of a letter from the bank.
  - Complete CDD information and documentation must also be obtained, as per the Natural Persons' checklist.
  - Once the relevant details and documents have been received and noted as correct;

- The Financial Administrator must execute the bank account verification process BEFORE refunding the funds, to ensure that it is in the name of the person and that it is the same account, from where the funds originated.

**ANNEXURE 11: WORLD-CHECK ALL SANCTIONS LISTS AVAILABLE (AS AT 16/11/2022)**

World-Check all sanctions lists available as at 16 November 2022.

Refinitiv WorldCheck-One San

World-Check_Keyword-list-new (16).xlsx

**ANNEXURE 12: SCHEDULE 1: LIST OF ACCOUNTABLE INSTITUTIONS (AS AMENDED ON 19 DECEMBER 2022)**

1. (a) A [practitioner who practices as defined in section 1 of the Attorneys Act, 1979 (Act 53 of 1979)] person who is admitted and enrolled to practise as a legal practitioner as contemplated in section 24(1) of the Legal Practice Act, 2014 (Act 28 of 2014) and who is–

   (i) an attorney (including a conveyancer or notary) **practising for his or her own account as contemplated in section 34(5)(a) of that Act; or**

   **(ii) an advocate contemplated in section 34(2)(a)(ii) of that Act**.

   (b) **A commercial juristic entity, as contemplated** in section 34(7) of the Legal Practice Act, 2014.

2. (a) A [board of executors or a trust company or any other person that invests, keeps in safe custody, controls or administers trust property within the meaning of the Trust Property Control Act, 1988 (Act 57 of 1988)] person who carries on the business of preparing for, or carrying out, transactions for a client, where–

   (i) the client is assisted in the planning or execution of–

   (aa) the organisation of contributions necessary for the creation, operation or management of a company, or of an external company or of a foreign company, as defined in the Companies Act, 2008 (Act 71 of 2008);

   (bb) the creation, operation or management of a company, or of an external company or of a foreign company, as defined in the Companies Act, 2008; or

   (cc) the operation or management of a close corporation, as defined in the Close Corporations Act, 1984 (Act 69 of 1984).

   (b) A person who carries on the business of–

   (i) acting for a client as a nominee as defined in the Companies Act, 2008; or

   (ii) arranging for another person to act for a client as such a nominee.

   (c) A person who carries on the **business of creating a trust arrangement for a client**.

   (d) A person who carries on the business of **preparing for or carrying out transactions (including as a trustee) related to the investment, safe keeping, control or administering of trust property within the meaning of the Trust Property Control Act**, 1988 (Act 57 of 1988).

3. An estate agent as defined in the Estate Agency Affairs Act, 1976 (Act 112 of 1976).

4. An authorised user of an exchange as defined in the [Securities Service Act, 2004 (Act 36 of 2004)] Financial Markets Act, 2012 (Act 19 of 2012).

5. A manager registered in terms of the Collective Investment Schemes Control Act, 2002 (Act 45 of 2002), but excludes managers who only conduct business in Part VI of [the Collective Investment Schemes Control] that Act [(Act 45 of 2002)].

6. A person who carries on the “business of a bank” as defined in the Banks Act, 1990 (Act 94 of 1990).

7. A mutual bank as defined in the Mutual Banks Act, 1993 (Act 124 of 1993). 7A. **A co-operative bank as defined in the Co-operative Banks Act, 2007 (Act 40 of 2007).**

8. A person who carries on a "[long-term] life insurance business" as defined in the [Long-Term Insurance Act, 1998 (Act 52 of 1998)] Insurance Act, 2017 (Act 18 of 2017), **but excludes reinsurance business as defined in that Act.**

9. A person who carries on the business of making available a gambling activity as contemplated in section 3 of the National Gambling Act, 2004 (Act 7 of 2004) in respect of which a license is required to be issued by the National Gambling Board or a provincial licensing authority.

10. A person who carries on the business of dealing in foreign exchange.

11. (a) A person who carries on the business of [lending money against the security of securities] a credit provider as defined in the National Credit Act, 2005 (Act 34 of 2005). (b) A **person who carries on the business of providing credit in terms of any credit agreement that is excluded from the application of the National Credit Act**, 2005 by virtue of section 4(1)(a) or (b) of that Act.

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), to provide advice [and] or intermediary services in respect of the investment of any financial product (but **excluding a [short term insurance contract or policy referred to in the Short-term Insurance 5 Act, 1998 (Act 53 of 1998)] non-life insurance policy, reinsurance business** as defined in the Insurance Act, 2017 (Act 18 of 2017) and [a health service benefit provided by] the business of a medical scheme as defined in section 1(1) of the Medical Schemes Act, 1998 (Act 131 of 1998.))

13. A person who issues, sells or redeems travellers' cheques, money orders or similar instruments.

14. The South African Postbank Limited referred to in section [51] 3 of the [Postal Services Act, 1998 (Act No. 124 of 1998)] South African Postbank Act, 2010 (Act 9 of 2010).

15.

16. [The Ithala Development Finance Corporation Limited.] **(Deleted)**

17.

18.

19. A person who carries on the business of a money [remitter] or **value transfer provider**.

20. **A person who carries on the business of dealing in high-value goods in respect of any transaction where such a business receives payment in any form to the**

**value of R100 000,00 or more, whether the payment is made in a single operation or in more than one operation that appears to be linked, where "high-value goods" means any item that is valued in that business at R100 000,00 or more.**

21. **The South African Mint Company (RF) (Pty) Ltd, only to the extent that it distributes non-circulation coins in retail trade and where in respect of such transactions it receives payment in any form to the value of R100 000,00 or more, whether the payment is made in a single operation or in more than one operation that appears to be linked.**

22. **A person who carries on the business of one or more of the following activities or operations for or on behalf of a client:**

**(a) Exchanging a crypto asset for a fiat currency or vice versa;**
**(b) exchanging one form of crypto asset for another;**
**(c) conducting a transaction that transfers a crypto asset from one crypto asset address or account to another;**
**(d) safekeeping or administration of a crypto asset or an instrument enabling control over a crypto asset; and**
**(e) participation in and provision of financial services related to an issuer's offer or sale of a crypto asset, where "crypto asset" means a digital representation of perceived value that can be traded or transferred electronically within a community of users of the internet who consider it as a medium of exchange, unit of account or store of value and use it for payment or investment purposes, but does not include a digital representation of a fiat currency or a security as defined in the Financial Markets Act, 2012 (Act 19 of 2012).**

23. **A clearing system participant as defined in section 1 of the National Payment System Act, 1998 (Act 78 of 1998) that facilitates or enables the origination or receipt of any electronic funds transfer and or acts as an intermediary in receiving or transmitting the electronic funds transfer.**

****** Details in bold, are either amendments to an already existing item or is a new item***

**ANNEXURE 13: CURRICULUM VITAE: GROUP MONEY LAUNDERING COMPLIANCE OFFICER: DOUW LOTTER**

| | | |
|---|---|---|
| **DATE OF EMPLOYMENT AT MMLL** | **:** | 1998 |
| **POSITION** | **:** | Head of Group Forensic Services and AML Solutions (Since 1998) |
| **MLCO** | **:** | Appointed by the MMLL Board since 2002, aligned with the introduction of SA AML Legislation, the Financial Intelligence Centre Act, 38 of 2001. |
| **QUALIFICATIONS** | **:** | Bachelor Economics degree in Law and is also a registered Certified Fraud Examiner (Worldwide standard) |