

**TIPMARKETS (PTY) LTD**

**AML POLICY**

Version 1.2, October 2025

## Contents

<b>TIPMARKETS (PTY) LTD</b> .....	1
<b>I. PURPOSE</b> .....	3
<b>II. THE OFFENCE OF MONEY LAUNDERING</b> .....	4
<b>III. PROCEEDS OF CRIME</b> .....	4
<b>IV. KNOWLEDGE UNDER THE South Africa ' AML ACT</b> .....	4
<b>V. REPORTING ENTITIES AND THEIR OBLIGATIONS</b> .....	5
<b>VI. INTERNAL CONTROLS, POLICIES AND PROCEDURES</b> .....	6
<b>VII. TRAINING</b> .....	7
IDENTIFICATION .....	8
<b>VIII. REQUIREMENTS</b> .....	8
<b>IX. ENHANCED IDENTIFICATION REQUIREMENTS</b> .....	9
<b>X. CUSTOMER RISK ASSESSMENT</b> .....	12
<b>XI. BRANCHES AND SUBSIDIARIES</b> .....	13
<b>XII. LIABILITY OF EMPLOYERS AND PRINCIPALS</b> .....	13
<b>XIII. LIABILITY OF DIRECTORS</b> .....	13

## I. PURPOSE

TIPMARKETS (PTY) LTD is an Investment Firm that owns and operates the brand “TipMarkets” (<https://tipmarkets.com/>). TIPMARKETS (PTY) LTD is registered in South Africa, company number 2016/214844/07, and is authorized and regulated by the Financial Sector Conduct Authority ("FSCA") of South Africa with license number 47159 to carry out certain categories of financial investment business as permitted under section 8 of the Financial Advisory and Intermediary Services Act, 2002 (Act No.37 of 2002). The Company’s registered office is located at 2<sup>nd</sup> Floor, Rivonia Village, Cnr Mutual Road and Rivonia Boulevard, Rivonia Village, 2191. Please refer to the website of the Company (<https://tipmarkets.com/>) for more information.

The Company is operating under the Section 8 of the Financial Advisory and Intermediary Services Act, 2002 (Act No.37 of 2002) (collectively the “Act and Applicable Regulations”).

The brand “TipMarkets” is owned and operated by TIPMARKETS (PTY) LTD duly registered in South Africa with a registration number 2016/214844/07 holder of an FSCA license with number 47159 and registered address at 2<sup>nd</sup> Floor, Rivonia Village, Cnr Mutual Road and Rivonia Boulevard, Rivonia Village, 2191.

The purpose of this Manual is to provide guidance on the Anti-Money Laundering and Know your Client Policy which is followed by TIPMARKETS (PTY) LTD (hereafter “the Company”) in order to achieve full compliance with the relevant anti-money laundering legislation in South Africa.

The aim of the AML Act 2001 is to address the deficiencies that existed in the previous legislation and ensure that South Africa is in line with international standards and best practice. It will better equip the regulators and law enforcement agencies in the fight against money laundering and terrorism financing.

According to the AML Act 2001, reporting entities have an obligation to verify a customer’s identity, maintain records and monitor transactions. In addition, reporting entities are required to ensure that accounts are in the true names of clients, to ensure that money transmissions include originator information. Also, the reporting entities have an obligation to report suspicious transactions or certain information and appoint a compliance officer.

These guidelines do not purport to be a comprehensive summary of the Anti-Money Laundering and the Prevention of Terrorism Procedures or a substitute thereof and should be read in conjunction with both Acts which are the source of the law.

The Manual shall be read and followed by all staff of the Company, who shall sign an acknowledgement form that have read and understood their rights and obligations stemming from this Manual.

## II. THE OFFENCE OF MONEY LAUNDERING

1. A person who -
  - (a) converts or transfers property knowingly or having reason to believe that the property is the proceeds of a crime with the aim of concealing or disguising the illicit origin of that property, or of aiding any person involved in the commission of the offence to evade the legal consequences thereof;
  - (b) conceals or disguises the true nature, origin, location, disposition, movement or ownership of the property knowing or having reason to believe that the property is the proceeds of a crime;
  - (c) acquires, possesses or uses property knowing or having reason to believe that the property is the proceeds of a crime, commits the offence of money laundering.
2. Every person who -
  - (a) organizes or directs others to commit;
  - (b) attempts to commit;
  - (c) conspires to commit;
  - (d) participates as an accomplice to a person committing, or attempting to commit, an offence under subsection 1 commits the offence of money laundering.
3. Knowledge, intent or purpose required as an element of any act referred to in subsection 1 may be inferred from surrounding facts.
4. Where it is necessary in the case of an offence of money laundering alleged to have been committed by a body corporate to establish the state of mind of the body corporate, it shall be sufficient to show that a director, officer, employee or agent of the body corporate, acting in the course of employment or agency as the case may be, had that state of mind.

## III. PROCEEDS OF CRIME

The crime of money laundering is not restricted to operations connected with money obtained from drug trafficking but include many types of criminal activity that can yield proceeds.

The money laundering offence is also committed by a person who aids, abets, or in any way assists or prepares, the commission of money laundering.

## IV. KNOWLEDGE UNDER THE South Africa ' AML ACT

The definition of money laundering covers those operations where a person knows, or should have reason to believe, that the money with which they are concerned is derived, obtained or realized, directly or indirectly, from an unlawful activity as described above.

It is only necessary that the person should have knowledge or reasonable grounds for knowledge of the unlawful source of the funds to be guilty of the offence. Positive knowledge is not the test; knowledge may be inferred from objective factual circumstances.

What knowledge entails in the case of corporate bodies is clearly stated in the law. It is sufficient that a

director, officer, employee or agent of the body corporate acting in the course of his employment or agency had that state of mind. Guilty knowledge of any employee can result in an offence being committed by the employer (as well as by the employee). Crimes committed outside South Africa.

The unlawful activity from which the "dirty money" is derived is any act or omission which was committed or done in South Africa. Also, acts or omissions committed or done outside South Africa constitute an offence in South Africa if they are punishable in South Africa.

## V. REPORTING ENTITIES AND THEIR OBLIGATIONS

The Anti-Money Laundering Act defines a reporting entity as those persons that carry out certain businesses and activities which can be either financial or non-financial in nature. Reporting entities include banks (including offshore banks), credit unions, bureaux de change (including hotels), insurance companies, money transfer companies, securities companies, trust and company service providers, dealers in precious metals and precious stones, casinos, real estate agents.

The obligations of the reporting entities include the following:

- The need to identify and verify the identity of a customer when establishing a business relationship; If the customer is a politically exposed person ("PEP"), a reporting entity shall adequately identify the person and verify his or her identity. In addition, to have appropriate risk management systems to determine whether the customer is a PEP.
- Take reasonable measures to ascertain the purpose of any transaction in excess of R 100,000 or of R 50,000 in the case of cash transactions and the origin and ultimate destination of the funds involved in the transaction;
- In relation to its cross-border banking and other similar relationships adequately identify the identity of the person, gather sufficient information about the nature of the business, assess the AML/CFT controls and obtain senior management's permission before entering into a new relationship;
- To not proceed with a transaction if there is no satisfactory evidence of a customer's identity; To
- maintain records on a customer's identity for a minimum period of 7 years from the date of any transaction or correspondence or on which the business relationship ceases; A reporting entity that fails to maintain records is guilty of an offence.
- Maintain accounts in the clients' true name;
- Ensure that money transmission includes accurate originator information on electronic funds transfers and that the information shall remain with the transfer;
- To monitor complex, unusual or large transactions with no apparent economic or lawful purpose as well as ongoing monitoring of business relationships /transactions undertaken throughout the course of the relationship;
- To report any transaction or attempted transaction that may be related to the commission of an offence of ML/FT to the FIU.

Further to the abovementioned obligations, reporting entities should therefore ensure that their staff are fully aware of their obligations found in the law and abide by them so as to ensure compliance. Therefore, a reporting entity shall appoint compliance and reporting officer who shall be responsible for ensuring the reporting entity's compliance with the provisions of this Act.

In relation to clients originating from "high risk countries" the following procedure should be followed:

1. Identifying the customers and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

2. Identifying the beneficial owner and taking reasonable measures to verify the person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;
3. Assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
4. Conducting ongoing monitoring of the business relationship including scrutiny of transaction undertaken throughout the course of relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data and information held are kept up to date,

## VI. INTERNAL CONTROLS, POLICIES AND PROCEDURES

Every Reporting Entity must take appropriate measures to make sure that its employees engaged in dealing with customers or processing business transactions maintain the identification and record-keeping procedures laid down in the Act.

The Anti-Money Laundering Act requires the appointment of a senior officer with the necessary qualifications and experience as the Compliance and Reporting Officer (CRO)

The CRO shall be responsible for the following:

- liaising with all relevant business and support areas within the Company.
- monitoring the adequacy and effectiveness of the measures and procedures of the Company.
- advising and assisting the relevant persons responsible for carrying out the investment services be in compliance with the Law.
- drafting written reports to the Senior Management and the Board making recommendations and indicating in particular whether the appropriate remedial measures have been taken in the event of any deficiencies, at least annually. These reports shall be presented to the Board and discussed during its meetings, at least annually.
- working on related changes to the Company's documentation.
- training and educating the staff of the Company at least once per year or when it is considered necessary in respect with the compliance function according to the Law.
- communicating the relevant statutes of the IOM to each employee and notify them of any relevant changes therein that relates to his/her role and responsibilities in the Company.
- ensuring that the Executive Directors or other hierarchically higher officers do not exercise inappropriate influence over the way in which a relevant person carries out the provision of payment services
- developing, designing and re-designing the appropriate procedures of the Company, so as to prevent and resolve potential conflicts of interest, ensuring that all the procedures regarding the Company's conflict of interest policy are in place, as well as establishing and maintaining Chinese Walls procedures between the various organizational units of the Company. Regular checks will be performed to ensure the latter.
- ensuring that all employees will have the ability to identify cases of potential conflicts of interest.
- keeping records regarding conflict of interest situations, where relevant.
- monitoring and reviewing the dispatch of the confirmations/notifications to Clients regarding the execution of their trading orders.
- ensuring that all relevant information is included in the Company's outsourcing agreements.

- communicating to the Senior Management of the Company any new or updated requirements of the Company in relation to the Company's activities.
- Updating of the IOM, relating to any additional requirements as regards the obligations of the Company under the Law.
- ensuring the performance of multiple functions by the Company's relevant persons does not and is not likely to prevent those persons from discharging any particular function soundly, honestly, and professionally.
- consenting to and approving the Company's policies.
- monitoring and reviewing the work undertaken by the back-office department for compliance with the relevant provisions of this IOM and the applicable legislation.

The Company applies the following measures in order to ensure that the staff follow the due diligence requirements:

- All employees shall sign the acknowledgement for the Company's AML procedures
- Every identification carried out by the Company's staff shall be executed by the employee that carried out the identification; and
- Every identification carried out by the Company's staff shall also be approved by the Company's appointed CRO.

## VII. TRAINING

The training program aims at educating employees on the latest developments in the prevention and money laundering and terrorist financing including the practical methods used for this purpose. The Company conducts training sessions on Anti-Money Laundering Compliance and other related subjects to the roles, duties and responsibilities of all The Company's personnel.

Training is provided on important legal provisions as well as updates on important legislative amendments and on the system and procedures followed in relation to the matters below:

- (a) Relevant Anti-Money Laundering Legislation which is effective in South Africa
- (b) Guidance and Circulars issued by FSA in relation to AML legal framework;
- (c) Identification and handling transaction and activities which may be related to money laundering and terrorist financing activity.

Training on issues regarding the prevention of money laundering and terrorist financing is provided at least once a year.

The Company shall keep a training registry which includes at least the following details:

- (a) Summarized data of the content of the training seminars.
- (b) Number and duration of the training seminars.
- (c) Number and position of the employees participating in the training seminars.
- (d) Number and position of employees who did not participate in the training seminars and their duties are relevant with the prevention of money laundering

- (e) and terrorist financing. Information on the reasons for not participating.
- (f) Instructors' names and qualifications.
- (g) Whether the training seminars were performed in-house or by an external organization or consultants.

## VIII. IDENTIFICATION REQUIREMENTS

Reporting Entities must identify prospective customers at the time of opening of an account or entering into a business relationship. The duty to identify a customer and to keep informed of the customer's business continues after the relationship is established.

Unless satisfactory evidence of identity is obtained "as soon as is reasonably practicable" the reporting entity must not proceed any further with the transaction unless directed to do so by the Financial Intelligence Unit (..FIU..). The reporting entity is also required to report the attempted transaction to the FIU.

What constitutes an acceptable time to identify the customer must be determined in the light of all the circumstances including the nature of the business, the geographical location of the parties and whether it is practical to obtain the evidence before commitments are entered into or money changes hands. Thus, the Reporting Entity can open an account or begin the business relationship provided that it promptly takes appropriate steps to verify the customer's identity.

The documents/information required for the identification of the customer are the following: ■

- The name and occupation of the individual;
- Identity card or passport;
- Recent Utility bill (dated within 3 months) reflecting the individuals current address; and ■ Bank reference.

The documents/information required for the identification of legal persons are the following: •

- Certificate of incorporation and certificate of good standing;
- Certificate of registered office;
- Certificate of directors and secretary;
- Certificate of shareholders;
- Certificate of Incumbency, if applicable (shall replace certificates of incorporation, registered office, directors and secretary and shareholders);
- Memorandum and articles of association;
- In case that registered shareholders act as nominees of the beneficial owners, a copy of the trust; agreement concluded between the nominee shareholder and the beneficial owners; and
- Documents for the verification of the identity of the registered shareholders and the beneficial owners (passport and utility bill).

The Company may rely on third parties, subject to the third parties' consent, for carrying out all or part of the client identification and due diligence procedures, but in any case, the Company remains liable for any compliance failure notwithstanding its reliance on third parties. The relevant third party should also retain its own responsibility for compliance with the money laundering requirements, including the requirement to report suspicious transactions and maintain records, to the extent that it has a relationship with the client.



The Company shall also carry out independent checks through online searches and databases in order to screen and identify the potential customers.

When must the Identity be verified?

Whenever an account is to be opened or a continuing business relationship is entered into, the identity of the prospective customer must be verified. Reporting entities are required to obtain information on the purpose and nature of the business relationship. Thereafter as long as records are maintained, no further evidence of identity is needed unless the reporting entity has any reason for suspicions, for instance if there is a marked change in the nature or volume of business passing through the account.

Reporting entities are advised to develop a customer profile based on the information obtained. A customer profile will assist the reporting entity in identifying suspicious transactions and facilitate the monitoring of accounts and transactions.

Also, when a transaction is undertaken when there is no business relationship, or an electronic funds transfer is carried out, the reporting entity is required to take the identity of the customer. Furthermore, identity must be verified in all cases where money laundering or the financing of terrorism is suspected, or where there are doubts as to the veracity or adequacy of the identification information obtained.

If a natural person conducts a transaction through a reporting entity and the latter has reasonable grounds to believe that the person is undertaking the transaction on behalf of another person, the reporting entity shall identify and verify the identity of the ultimate beneficial owner for whom the transaction is being conducted.

The obligation to obtain evidence of identity is general. Identification is not required when it concerns an occasional cash transaction under R 50,000, unless there is a suspicion that the transaction is unlawful.

## IX. ENHANCED IDENTIFICATION REQUIREMENTS

A reporting entity is under the obligation to take reasonable measures to ascertain the purpose of a transaction in excess of R 100,000 or of R 50,000. In these cases, the origin and ultimate destination of the funds should be established.

A reporting entity should have a risk management system to determine if a person is a PEP. Independent checks through online databases will be performed in order to identify whether a client is a PEP. If the customer is a PEP, a reporting entity must adequately identify the person and verify his or her identity, take reasonable measures to establish the source of wealth and the source of property, and regularly monitor the account. Approval of senior management should be obtained before establishing a business relationship with the customer. PEP are only persons holding prominent public positions in a foreign country.

A Reporting Entity shall in its cross-border correspondent banking and other similar relationships undertake enhanced measures when identifying and verifying the identity of the person with whom it conducts such a business relationship. These measures include gathering sufficient information about the nature of the business, use publicly available information to determine the reputation of the correspondent and the quality of supervision to which it is subject, assess the correspondent's AML/CFT controls. Approval of senior management should be obtained before establishing a new correspondent relationship.

Where the relationship is a payable-through account, a reporting entity shall ensure that the person with whom it has established the relationship has verified the identity of and performed on-going due diligence on the person's customers and have direct access to the accounts. The reporting entity shall also ensure that the person is able to provide the relevant customer identification data upon request and that it has a physical presence in the Republic under the law which it was established unless it is part of a group that is subject to supervision as a whole.

A reporting entity shall apply customer due diligence measures when:

- (a) Establishing a business relationship
- (b) Carrying out an electronic transfer of funds
- (c) Carrying out a one- off transaction
- (d) The reporting entity has doubts on the veracity or adequacy of documents, data or information obtained for the purpose of identification or verification of a customer or
- (e) There are reasonable suspicious of money laundering, financing of terrorism or other criminal conduct.

When there is suspicious of money laundering, financing of terrorism or other criminal conduct, the reporting entity shall apply the customer due diligence measures found in regulation.

Where a reporting entity knows or has reasonable grounds to believe that a customer, or a beneficial owner of a customer, residing in or outside South Africa is or becomes a politically exposed person, the reporting entity shall apply, on a risk- sensitive basis, enhanced customer due diligence measures and enhanced ongoing monitoring. In addition, the reporting entity shall obtain the approval of the senior management before a business relationship is established with the customer and take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or one- off transaction.

When dealing with natural persons or legal entities established in third countries identified by the Commission as high-risk third countries or in the circumstances of High-Risk clients, the Company shall apply enhanced customer due diligence measures to manage and mitigate those risks appropriately.

Enhanced customer due diligence measures need not to be invoked automatically with respect to branches or majority owned subsidiaries of obliged entities established in the Union which are located in high-risk third countries, where those branches or majority-owned subsidiaries fully comply with the group-wide policies and procedures.

The Company shall examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent and economic or lawful purpose. The obliged entities shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

As part of the implementation of the enhanced due diligence procedures, the Company applies one or more of the following measures:

- Obtains additional client information, such as the client's reputation and background, before the establishment of the business relationship;

- Verifies or certifies the documents supplied, or requiring confirmatory certification by third party independent sources;
- Obtains information on the source of funds and/or the source wealth of the client and of the client's beneficial owner;
- Requires that the redemption payment is made through the initial account used for investment or an account in the sole or joint name of the client;
- Increases the frequency and intensity of transaction monitoring;

Further to the above, for high risk clients, the Company performs the following: •

- Conducts enhanced and continuous monitoring of the business relationship.
- Checks all UBO's against online databases and internet search engines to identify validity of passport, PEP status, involvement in any illegal activities, inclusion in any sanctions lists, etc.

Further to the above, for the below specific types of high-risk clients, the Company implements the following measures as part of the enhanced due diligence measures:

The Company applies the following measures in relation to clients from countries which inadequately apply Financial Action Task Force's (FATF's) recommendations:

- Exercises additional monitoring procedures and pays special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid recommendations.
- Transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic, business or investment background and purpose. If the Company cannot be fully satisfied as to the legitimacy of a transaction, then a suspicious transaction report is filed to FIU.
- With the aim of implementing the above, the CRO consults the country assessment reports prepared by the FATF, the other regional bodies that have been established and work on the principles of FATF and the International Monetary Fund. Based on the said reports, the CRO assesses the risk from transactions and business relationships with persons from various countries and decides of the countries that inadequately apply the FATF's recommendations. According to the aforesaid decision of the CRO the Company applies, when deemed necessary, enhanced due diligence measures for identifying and monitoring transactions of persons originating from countries with significant shortcomings in their legal and administrative systems for the prevention of money laundering and terrorist financing.

Where a reporting entity relies on an intermediary or third party, it shall immediately obtain the identification data and ensure that copies are made available upon request without delay. Where the reporting entity is a financial institution, it shall satisfy itself that the third party or intermediary is regulated and supervised for and has measures to comply with the requirements of the Act

A reporting entity shall comply the requirements of this Act notwithstanding any obligations as to confidentiality or other restriction on the disclosure of information imposed any written law or otherwise.

The Company, in cases where there is an attempt of executing transactions which it knows or suspects that are related to money laundering or terrorist financing, reports through the CRO its suspicion to FIU.

In this respect, all the Company's Directors and employees should comply with the following

procedure, to ensure that all known regulatory requirements as to reporting knowledge or suspicion of money laundering are met. In this respect, the Company's staff, in the case of suspicions of money

laundering shall formally report to the Company's CRO, through an official letter or email. This will serve to absolve the employee from any potential criminal liability.

## **X. CUSTOMER RISK ASSESSMENT**

The Company categorizes its clients in three risk level categories, namely low, medium and high. The categorization of the clients depends on whether the client is linked to a high - risk jurisdiction, the nature of the client's business, the amount of the client's overall deposits, the transaction pattern (i.e. are complex or unusual) and any suspicious change in the transaction pattern or whether the client is a PEP or family or close associate where is automatically high risk. Depending on the client's classification the Company will reassess the high - risk clients every 6 months, the medium/normal every one year and the low risk clients every 2 years. All clients are subject to monitoring and review according to their categorization. All clients are being screened during the registration process as well as during the business relationship with the Company according to their risk categorization and in cases there is change of their details or categorization. The company exercises on going screening to all of its clients and therefore whenever there is change to client's details the company will review the client's personal information and status. In this respect, the client exercises simplified due diligence measures to low risk clients, provided that it has previously ensured that the business relationship or transaction bears lower degree of risk and EDD measures will apply to clients who were classified as high – risk (i.e. clients who are involved in high risk industry, clients from countries which inadequately apply FATF's recommendations, any other Client determined by the Company itself to be classified as such).

## **XI. BRANCHES AND SUBSIDIARIES**

A reporting entity shall require its branches and subsidiaries outside South Africa to apply, to the extent permitted by the laws of the country where they are located, measures at least equivalent to those set out in the Regulations with regard to customer due diligence, ongoing monitoring and record-keeping.

Where no such equivalent customers due diligence measures are required under the laws of the country where the branches and subsidiaries are located, the reporting entity shall

- (a) Inform its supervisory authority accordingly
- (b) Apply the customer due diligence measures provided in the Regulations, as applicable to the risk of money laundering, financing of terrorism or other criminal conduct and
- (c) Produce to the FIU, without delay on request, all information data and documents in the possession or control of such branch or subsidiary undertaking in accordance with the obligations of the reporting entity under the Regulations.

## **XII. LIABILITY OF EMPLOYERS AND PRINCIPALS**

Further to the Act, any act done or omission made by a person as an employee or agent shall be treated as done or made by that person's employer or principal if it was done or made with the knowledge or approval of the employer or principal or without such knowledge or approval if it was the result of lack of supervision, provided, in the case of an agent, that he or she acted within the terms of his or her agency or contract.

## **XIII. LIABILITY OF DIRECTORS**

Where anybody corporate is convicted of an offence under the AML Act or any Regulations made under the Act, every person being the director, controller or officer concerned in the management of the body corporate shall be guilty of the offence where it is proved that the act or omission that constituted the offence took place with that person's knowledge, authority, permission or consent.