# POLICY GUIDELINES ON 'KNOW YOUR CUSTOMER' NORMS AND ANTI- MONEY LAUNDERING MEASURES

| | |
|---|---|
| PROPOSED BY | Shane Samson, Sr. Manager - Risk Policy |
| RECOMMENDED BY | Shimnay West, Head – Risk Management and Floor Plan |
| **APPROVED BY** | Justin Warren Paulse - Executive Director |

## PURPOSE

This policy document gives an overview on the standards issued by the South African Reserve Bank (SARB) and the Payments Association of South Africa (PASA) on the 'Know your Customer' and 'Anti Money Laundering' for Non-Banking Financial Companies thereby setting standards for prevention of money laundering activities and corporate practices while dealing with their customers. The company shall adopt all best practices prescribed by the SARB and PASA from time to time and shall make appropriate modifications if necessary to this code to conform to the standards so prescribed. This policy is applicable across all business segments of the company and is to be read in conjunction with related operational guidelines issued from time to time. The contents of the policy shall also be auto corrected with any changes/modifications recommended by the SARB and PASA from time to time.

## SCOPE

The scope of this policy extends to all business segments of Rapid Financial Services (Pty) Ltd (RFS). The company is committed to transparency and fairness in dealing with all stake holders and customers in ensuring adherence to all laws and regulations. The company ensures that information collected from customers for any purpose will be kept as confidential. The company also commits that the information sought from the customer is relevant to the perceived risk and is not intrusive and is in conformity with the guidelines issued in this regard. Any other information from the customer shall be sought from the customer separately with his/her consent and after effective rendering of service. The company shall also communicate its KYC norms to its customers.

## APPLIES TO

This policy applies to all RFS staff. All new joiners are required to acknowledge having read the policy document and sign a letter of acknowledgment and irrevocable adherence to the policy.

**TABLE OF CONTENTS**

## 1. INTRODUCTION

'KNOW YOUR CUSTOMER'

The South African Reserve Bank (SARB) and the Payments Association of South Africa (PASA) has issued comprehensive guidelines on 'Know Your Customer' (KYC) norms and Anti-money Laundering (AML) standards and has advised all Non-Banking Financial Companies (hereinafter, NBFCs) to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Companies Director(s).

Accordingly, in compliance with the guidelines issued by the SARB and PASA from time to time, the following KYC & AML policy is approved by the Director(s) of Rapid Financial Services (Pty) Ltd t/a RAPID PAYMENTS (hereinafter "RFS" or "the Company").

This policy is applicable to all categories of products and services offered by the Company.

## 2. OBJECTIVE

Objective of the SARB and PASA guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandates making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

## 3. GLOSSARY

| | |
|---|---|
| AML | Anti-Money Laundering |
| CIP | Customer Identification Program |
| CCR | Counterfeit Currency Report |
| FIC - SA | Financial Intelligence Centre – South Africa (FIC-SA) |
| PEP | Politically Exposed Persons |
| PMLA | Prevention of Money Laundering Act |
| Principal Officer | RFS Officer/Director of rank of GM and above who is responsible for implementing the KYC and AML Policy of the Company |
| STR | Suspicious Transaction Reporting |
| UNSCR | United Nations Security Council Resolution - South Africa |

## 4. CUSTOMER ACCEPTANCE POLICY

The Company shall follow the following norms while accepting and dealing with its customers:

1. Customer must be a major (i.e. 18 years or above) and must not be incapacitated for entering into a contract as required by South African law;
2. Customers can be a foreign entity, however it is necessary to take approval from the Risk Head of RFS before any commitment is made to a customer;

3. Name of the customer should not appear in the list of banned entities as circulated by UNSCR;
4. Company officials must be satisfied as regards KYC due diligence of the customer;
5. Customer name should not have been included in the list of STR and PMLA submitted to SARB and PASA under PMLA;
6. In case of customers being PEP or becoming PEP subsequently, it is necessary to take approval of the Risk Head of RFS.

Key considerations:

- Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in to enable categorization of customers into low, medium and high risk. The illustrative list of such risk categorisation is provided in Annexure – I.
- The customer profile contains information relating to customer's identity, social/financial status, nature of business activity, information about his/her clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Company. However, while preparing the customer profile, the Company will seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein will not be divulged for cross-selling or any other purpose.
- The intent of the Policy is not to result in denial of financial services to the general public, especially to those, who are financially or socially disadvantaged. While carrying out due diligence, the Company will ensure that the procedure adopted does not result in denial of services to any genuine customers.
- The Company shall carry out full scale customer due diligence (CDD) before opening an account. When the true identity of the account holder is not known, the Company shall file Suspicious Transaction Reporting (STR) as provided below in clause 9.

## 5. CUSTOMER IDENTIFICATION PROCEDURE

Customer identification means identifying the customer and verifying his / her identity by using reliable and independent source of documents, data or information to ensure that the customer is not a fictitious person. The Company shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each customer and the purpose of the intended nature of business relationship.

An effective Customer Identification Program (CIP) is an important part of the effort by the Company to know its customers. The Company's CIP is integrated into the AML (Anti Money Laundering) program for the company in terms of the Prevention of Money Laundering Act, 2002 and the relevant rules notified there under (PMLA), which contains provisions requiring the business processes to:

1. **verify the identity of any Person** transacting with the Company to the extent reasonable and practicable;
2. **maintain records of the information** used to verify a customer's identity, including name, address and other identifying information and
3. **consult lists of known or suspected terrorists** or terrorist organizations provided to the Company by any applicable government agency to determine whether a person opening an account or an existing customer appears on any such list.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing. The procedures, documentation, types of information obtained and levels of KYC due diligence to be performed will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations) between the Company and the customer and the risk profile of the customer.

**5.1 Required "KYC" due diligence for all customers**

The Company shall take reasonable measures to ascertain and verify the true identity of all customers who transact with the Company. Each business process shall design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers and the associated risks. Such standards and procedures shall include, at a minimum, the following elements:

For the purpose of identifying and verifying the identity of customers at the time of commencement of a merchant account-based relationship, RFS may rely on a third party; subject to the conditions that-

i. The company immediately obtains necessary information of such client due diligence carried out by the third party;

ii. The company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;

iii. The company is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;

iv. The third party is not based in a country or jurisdiction assessed as high risk; and

v. The company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

**Customer Identification Procedure (CIP)**

**A) Identification**

All the customers shall be identified by a **unique identification code**, as established by RFS, to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of RFS customers.

Each business process shall implement procedures to obtain from each customer, prior to transacting, the following information as may be relevant, to that business:

1. Name - procedures require business processes to use reasonable efforts to ensure that the name recorded on the Company systems as the customer will be exactly the same as (and not merely similar to, or a variation of) the name that appears on any identifying documentation reviewed in connection with the merchant facility;
2. For individuals - age / date of birth; For a person other than individual (such as corporation, partnership or trust) - date of incorporation;
3. Address including the documentary proof thereof;
    i. For an individual, a residential or business street address;
    ii. For a Juristic other than an individual (such as a corporation, partnership, or trust), the principal place of business, local office, or other physical location;
4. Telephone/Fax number/E-mail ID;
5. Identification number:
    i. A taxpayer identification number; passport number and country of issuance; bearing a photograph or similar safeguard. When opening an account for a person (other than an individual) that does not have an identification number, the business process must request alternative government issued documentation certifying the existence of the business or enterprise; RFS will be extending merchant facilities to Resident South Africans and Non-Resident South Africans and will ensure adequate safeguards are in place.

    ii. For a customer who has applied for, but has not received an identification number, the merchant facility may be sanctioned, but each business process shall implement procedures to confirm that the application was filed before the merchant facility is sanctioned to the customer and to obtain the identification number within a reasonable period of time, before activation of the merchant facility with RFS.

The list of documents that can be accepted as proof of identity and address from customers across various merchant services as offered by the Company is given as **Annexure - III** to this policy. These are appropriately covered in the merchant agreement of the respective businesses and communicated to the Payments Association of South Africa (PASA).

**B) Verification**

Each business process as a part of the company policy will document and implement appropriate risk-based procedures designed to verify that it can form a reasonable belief that it knows the true identity of its customers. Verification of customer identity should occur before transacting with the customer. Procedures for each business process shall describe acceptable methods of verification of customer identity, which may include verification through documents or non-documentary verification methods that are appropriate given the nature of the business process, the products and services provided and the associated risks.

i. *Verification through documents:*

These documents may include, but are not limited to the list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company as provided in **Annexure - III** to this policy.

ii.

The list of documents that can be accepted as proof of identity and address from customers across various products offered by the Company is given as **Annexure - III** to this policy. These should be appropriately covered in the credit policies of the respective businesses. The customer verification processes will be covered in detail in the credit policies of every business.

iii. *Verification through non-documentary methods:*

These methods may include, but are not limited to:

1. Contacting or visiting a customer;
2. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
3. Checking references with other financial institutions; or
4. Obtaining a financial statement.

iv. *Additional verification procedures:*

If applicable, the business process verification procedures should address situations where:

1. A person is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
2. The business process associate is not familiar with the documents presented;
3. The Account is opened without obtaining documents;
4. Where the business process is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents; and
5. If the business process cannot verify the identity of a customer that is other than an individual, it may be necessary to obtain information about persons with authority or control over such account, including signatories, in order to verify the customer's identity.

**C) Resolution of Discrepancies**

Each business process shall document and implement procedures to resolve information discrepancies and to decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of such customer or cannot adequately complete necessary due diligence. These procedures should include identification of responsible decision makers and escalation paths and detailed standards relating to what actions will be taken if a customer's identity cannot be adequately verified.

**D) Reporting of Suspicious Transaction**

As a general rule, RFS prohibits cash remittance by customers and advises its customers to use acceptable cashless modes of payment (wire transfer, demand draft and/or credit card) to settle their due and/or overdue merchant fees.

The business shall have a system of internal reporting of suspicious transactions, counterfeit transactions and fraudulent transactions, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.

"Suspicious transaction" means a transaction whether or not made in cash which, to a person acting in good faith:

a. gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to have no economic rationale or bona fide purpose; or
d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
e. where the transactions are abandoned by customers on being asked to give some details or to provide documents;

Further, the Compliance Officer of RFS shall furnish information of the above mentioned transactions to the Director, Financial Intelligence Centre, South Africa (FIC-SA) and to the Payments Association of South Africa (PASA) at the prescribed address in the formats prescribed in this regard including the electronic filing of reports.

Provided that where the principal officer of the company has reason to believe that a single transaction or series of transactions integrally connected to each other, so as to defeat the provisions of the PMLA regulations, such officer shall furnish information in respect of such transactions to the Director of the Financial Intelligence Centre (FIC-SA) within the prescribed time.

In addition, it shall be the duty of the company, its designated Director, officers and employees to observe the procedure and manner of furnishing and reporting information on transactions timeously.

**5.2 Customer CIP Notice**

Each business process shall implement procedures for providing customers with adequate notice that the Company is requesting information and taking actions in order to verify their identity. Each business process shall determine the appropriate manner to deliver the notice, which shall be reasonably designed to ensure that the customer is able to view or is otherwise given such notice prior to the merchant account opening with RFS.

**5.3 Existing Customers**

The requirements of the earlier sections are not applicable to merchant accounts opened by existing customers, provided that the business process has previously verified the identity of the customer and the business process continues to have a reasonable belief that it knows the true identity of the customer. Further, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the merchant account should trigger a review of the due diligence measures.

**5.4 Enhanced Due Diligence**

The Company is primarily engaged in Third Party Payments (TPPP) to end customers and/or enterprises. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The existing policies of the Company in respect of its various financial services ensure that the Company is not transacting with such high risk customers/enterprises.

The Company shall conduct Enhanced Due Diligence in connection with all customers or merchant accounts that are determined to pose a potential high risk and are determined to warrant enhanced scrutiny. Each business process shall establish appropriate standards, methodology and procedures for conducting Enhanced Due Diligence, which shall involve conducting appropriate additional due diligence or investigative actions beyond what is required by standard KYC due diligence.

Enhanced Due Diligence shall be coordinated and performed by the Company, who may engage an appropriate outside investigative services or consult appropriate vendor sold databases when necessary. Each business process shall establish procedures to decline to do business with or discontinue relationships with any customer/enterprise when the Company cannot adequately complete necessary Enhanced Due Diligence or when the information received is deemed to have a significant adverse impact on reputational risk.

The following are the indicative list where the risk perception of a customer may be considered higher:

i. Customers requesting for frequent change of address/contact details;
ii. Sudden change in the merchant account activity of the customer(s);
iii. Frequent closure and opening of merchant accounts by the customers.

Enhanced due diligence may be in the nature of keeping the merchant account monitored closely for a re-categorisation of risk, updation of fresh KYC documents, field investigation or visit to the customer premises, etc., which shall form part of the policies of the business.

### 5.5 Simplified measures to verify the identity of the customers

Simplified measures are applied for verifying the identity of customers, the following documents shall be deemed to be officially valid documents:

- Identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
- Letter issued by a gazetted officer, with a duly attested photograph of the person;

The simplified measures is applicable to low risk category customers considering the type of customer, business relationship, nature and value of transactions as defined in **Annexure - I**.

It would be sufficient to obtain any of the documents mentioned above for low risk category customers.

## 6. RECORDS RETENTION

Each business process shall document and implement appropriate procedures to retain records of KYC due diligence and anti-money laundering measures. The business process shall implement, at a minimum, the following procedures for retaining records:

**a. Transactions for which records need to be maintained:**

- All transactions of the value of more than ZAR 5,000.00 or its equivalent in foreign currency;
- All series of transactions integrally connected to each other which have been ***individually*** valued below ZAR 5,000.00 or its equivalent in foreign currency where such series of transactions have taken place within a period of 1 (one) month ***and the monthly aggregate exceeds*** **ZAR 100,000.000** ***or its equivalent in foreign currency*****;**
- All suspicious transactions whether or not made in cash.

**b. Information to be preserved:**

The information required to be preserved with respect to the above transactions are the nature of transactions, amount and the currency in which it was denominated, date of transaction and the parties to the transaction.

**c. Periodicity of retention:**

The following records shall be retained for a minimum period of 5 (five) years after the related merchant account is closed:

- The customer identification information and residence identification information including the documentary evidence thereof;

- All other necessary records pertaining to the transactions that could be produced as evidence for prosecution of persons involved in criminal activity.

Further, a description of the methods used to verify customer identity as well as a description of the resolution of any discrepancies in verification shall be maintained **for a period of at least 5 (Five) years** after such record was created.

The above records shall be made available to the competent authorities upon request.

## 7. RISK CATEGORISATION

The Company shall put in place a system of periodical review of risk categorization of merchant accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization and due diligence of customers will be carried out on an on-going basis with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and, wherever necessary, the source of funds.

The Company shall have a system in place for periodical updation of customer identification data after the account is opened. The periodicity of such updation shall be annually in the case of low risk category customers and not less than once every 6 (Six) months in the case of medium risk category customers and not less than once every 3 (Three) months in the case of high risk category customers.

All the customers under different service categories are categorized into low, medium and high risk based on their profile. The Credit manager while appraising the transaction and rendering his approval will prepare the profile of the customer based on risk categorization. An indicative categorization for the guidance of businesses is provided in **Annexure - I**.

Each business process adopts the risk categorization in their respective policies subject to confirmation by the RFS internal compliance team, based on the credit appraisal, customer's background, nature and location of activity, country of origin, sources of funds, client profile, etc. Where businesses believe that a particular customer falling under a category mentioned below is in his judgment falling in a different category, they may categorise the customer so, so long as appropriate justification is provided in the customer file.

## 8. MONITORING OF TRANSACTIONS

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce the risk only if it has an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the merchant account. The relevant business divisions should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

High-risk accounts are subjected to vigorous and intensified monitoring.

## 9. RISK MANAGEMENT

RFS has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters.

The RFS Risk management team from time to time will carry on the necessary quality checks and file audits to ensure that the KYC policies and Procedures are fully adhered to, from time to time.

The Risk Management team shall also from time to time also update the Director(s) of any lapses if identified during the customer acquisition process. As a part of the risk policy, the Risk Management team has provided for a comprehensive list of documents that can be used as a part of the Know Your Customer guidelines.

## 10. CUSTOMER EDUCATION

The Company may prepare specific literature/ pamphlets etc. to educate the customer of the objectives of the KYC programme. The Company on an ongoing basis educates the front desk staff, the branch staff and the new joiners on the elements of KYC through various training programmes and e-mails.

### Appointment of Designated Director / Principal Officer

Mr. Justin Warren Paulse, Managing Director, is the Designated Director who is responsible for ensuring overall compliance as required under PMLA Act and the Rules.

Ms. Shimnay West, Head of Risk and Compliance, is designated as Principal Officer who shall be responsible for furnishing of information to FIC-SA, PASA and SARB.

## 11. COUNTERFEIT CURRENCY REPORT (CCR)

A separate Counterfeit Currency Report should be filed for each incident of detection of ANY Counterfeit currency. If the detected counterfeit currency notes can be segregated on the basis of tendering person, a separate CCR should be filed for each such incident. These transactions should be reported to the Director, Financial Intelligence Centre, South Africa (FIC-SA) by the 15th day of the succeeding month. In the event any fake or counterfeit note(s) are detected by staff, despite taking all precautions; then it must be noted in a cash register separately. Reporting of the case with full details like name of customer, amount, denomination, and date- must be reported by collections manager to Compliance dept.

While furnishing of information to the Director of the FIC-SA, a delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in this rule shall constitute a separate violation.

## 12. SOURCING RULES

- Marketing person shall, at the time of customer acquisition or executing any transaction, verify the record of identity, signature proof and proof of current address or addresses including permanent address of the customer.

- It is necessary that the Marketing Team verifies the photocopy of the KYC documents with the originals and certifies on the Form, the fact of having verified the same under his/her signature (Original Seen & Verified – OSV).

- It is necessary to ensure that the identity of the customer / director / partner / authorized signatory does not match with any entity with known criminal background or with banned entities available on the United Nations website. Customer name should be checked against the negative list as per the Financial Intelligence Centre (FIC-SA).

## 14. ANNEXURES

### ANNEXURE - I

**Indicative list for Risk Categorisation**

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorised as low risk.

Illustrative examples are:

1. Salaried employees whose salary structure is well-defined;
2. People belonging to lower economic strata of the society whose accounts show small balances and low turnover;
3. Government departments and Government-owned companies;
4. Statutory bodies & Regulators.

**Medium & High Risk Category**

Customers that are likely to pose a higher than average risk may be categorized as medium or high risk depending on the customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Illustrative examples are:

1. Non Resident customers;
2. High Net worth Individuals;
3. Trust, charities, NGO's and Organization receiving donations;
4. Companies having close family shareholding or beneficial ownership
5. Firms with 'sleeping partners';
6. Politically Exposed Persons (PEPs) of South African/Foreign Origin;
7. Those with dubious reputation as per public information available.

**ANNEXURE-II**

**Customer Identification Requirements**

**Trust/Nominee or Fiduciary Accounts**

In the case of any application from trust/nominee or fiduciary accounts, the Company determines whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary.

If in doubt of the persons behind the customer, the Company may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as well as also obtain details of the nature of the trust or other arrangements in place. Company takes reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories.

**Accounts of Companies and Firms**

The Company needs to be vigilant against business entities being used by individuals as a 'front' for transactions. Company should examine the control structure of the entity and identify the natural persons who have a controlling interest and who the management comprises of.

These requirements may be moderated according to the risk perception e.g. in the case of a public company.

**Client accounts opened by Professional Intermediaries**

Where the transaction is with a professional intermediary who in turn is on behalf of a single client, that client must be identified.

**Accounts of Politically Exposed Persons (PEPs)**

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

The Company if extending any financial services to non-residents should check if he/she is PEP and check all the information available about the person in the public domain. The decision to transact with the PEP should be taken only by the Head of Risk and Compliance of RFS supported by appropriate verification. The Company is also required to subject such merchant accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the contracts of the family members or close relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming PEP, the Company shall obtain the approval of its Management Committee to continue the business relationship and subject the account to the KYC due diligence measures as applicable to the customers of the PEP category including enhanced monitoring on an ongoing basis.

**Identity of Beneficial Owner**

The Company shall identify the beneficial owner and take all reasonable steps to verify his/her identity. The term "beneficial owner" has been defined as the natural person who ultimately owns

or controls a client and/or the person on whose behalf the application is being conducted and includes a person who exercises ultimate effective control over a juristic person. The Government of South Africa has since examined the issue and has specified the procedure for determination of Beneficial Ownership.

a) Where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juristic person, has a controlling ownership interest or who exercises control through other means.

Explanation- For the purpose of this sub-clause-

- "Controlling ownership interest" means ownership of or entitlement to more than 25% (twenty-five percent) of shares or capital or profits of the company;
- "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

b) Where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juristic person, has ownership of/entitlement to more than 15% (fifteen percent) of capital or profits of the partnership;

c) Where the client is an unincorporated association (Sole-Proprietor) or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juristic person, has ownership of or entitlement to more than 15% (fifteen percent) of the property or capital or profits of such association or body of individuals;

d) Where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

e) Where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% (fifteen percent) or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

f) Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

**ANNEXURE-III**

**Customer Identification Procedure**

**Features to be verified and documents that may be obtained from customers**

***Documents for proof of identity and address required for Individuals*;**

Any one document from the Officially Valid Document (OVD) is only allowed. They are:

i) Passport
ii) Driving License
iii) Identification card
iv) Voter's identity card issued by the Electoral Commission of South Africa

It is implied that proof of address also follows from the above documents only.

A customer shall not be required to furnish separate proof of current address, if it is different from the address recorded in the OVD. In such cases, a declaration from the customer in the application form to be taken, indicating the address to which all correspondence will be made.

In case of accounts of proprietorship concerns, it has been decided to lay down criteria for the customer identification procedure for merchant account opening by proprietary concerns. Accordingly, apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, RFS should call for and verify the following documents before opening of accounts in the name of a proprietary concern:

a) Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST / VAT certificate, certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, License issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of South Africa, Institute of Cost Accountants South Africa, Institute of Company Secretaries of South Africa, South African Medical Council, Food and Drug Control authorities, Financial Sector Conduct Authority (FSCA) etc.

b) Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department. RFS may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of SARS (South African Revenue Services) as an identity document for opening of a merchant account.

c) The complete Income Tax return (not just the acknowledgment) in the name of the sole proprietor where the firm's income is reflected duly authenticated/acknowledged by the Income Tax Authorities.

d) Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concerned.

Any two of the above documents would suffice. These documents MUST be in the name of the proprietary concerned.

***Documents for Identification and verification of Companies***

a) Certificate of Incorporation;
b) Memorandum and Articles of Association;
c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and
d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.

***Documents for Identification and Verification of Partnership firms***

a) Registration certificate;
b) Partnership deed; and
c) An officially valid document in respect of the person holding an attorney to transact on its behalf.

***Documents for Identification and verification of Trusts and Foundations***

a) Registration certificate;
b) Trust Deed; and
c) An officially valid document in respect of the person holding an attorney to transact on its
d) behalf.

In view of the change in the definition of Officially Valid Documents (OVD), henceforth, only the documents mentioned above would be accepted for opening merchant accounts of individuals and/ or enterprises. RFS would not have the discretion to accept any other document(s) for this purpose.

**Note:**

*All the customers namely applicant, co applicants and guarantor shall have valid ID and address proof as prescribed above.*

**ANNEXURE-IV**

**Illustrative list of activities which would be construed as suspicious transactions:**

- Activities not consistent with the customer's business, i.e. accounts with large volume of credits whereas the nature of business does not justify such credits.

- Any attempt to avoid Reporting/Record-keeping Requirements/provides insufficient / suspicious information:
  - A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
  - Any individual or group that coerces/induces or attempts to coerce/induce the Company employee from not filing any report or any other forms.

- A merchant account where there are several transactions below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

- Certain Employees of the Company arousing suspicion:
  - An employee whose lavish lifestyle cannot be supported by his or her salary.
  - Negligence of employees/wilful blindness is reported repeatedly.

- Some examples of suspicious activities/transactions to be monitored by the operating staff:
  - Multiple accounts under the same name;
  - Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful etc.;
  - There are reasonable doubts over the real beneficiary of the merchant account;
  - Frequent requests for change of address;

**This POLICY GUIDELINES ON 'KNOW YOUR CUSTOMER' (KYC) NORMS AND ANTI- MONEY LAUNDERING MEASURES , has been approved by the director of RAPID FINANCIAL SERVICES (PTY) LTD T/A RAPID PAYMENTS.**

Signed at Cape Town on this 01st Day of November 2022.

_____

Full Name: JUSTIN WARREN PAULSE
Designation: Director