



ANTI MONEY LAUNDERING POLICY

VaultFunder a product of Fintech Focused (Pty) Ltd

Date: 02 October 2023 Version: 1.1

1. Purpose

This Anti-Money Laundering (AML) Policy outlines the measures, procedures, and responsibilities to prevent and detect money laundering and the financing of terrorism within VaultFunder a product of Fintech Focused a product of Fintech Focused (Pty) Ltd ("the Company"). This policy is in compliance with applicable laws and regulations and establishes the procedures for identifying and verifying the identity of our customers.

2. Policy Statement

VaultFunder a product of Fintech Focused a product of Fintech Focused (Pty) Ltd is dedicated to upholding the highest standards of integrity and compliance with AML laws and regulations. The Company will not knowingly engage in activities that facilitate money laundering or the financing of terrorism. All employees, contractors, and third parties associated with the Company are responsible for adhering to this policy. This policy applies to all customers, including individuals, businesses, and other organizations.

3. Definitions

Accountable Institutions: Refers to all businesses or persons listed in Schedule 1 of the Financial Intelligence Centre Act, 2001 (Act No. 38 OF 2001), which includes listed companies, attorneys, estate agents, insurance companies, intermediaries, and unit trust management companies, identified as vulnerable to money laundering activities and subject to specific obligations.

Beneficial owner: In respect of a legal person, means a natural person who, independently or together with another person, directly or indirectly:

- has majority ownership of the legal person; or
- exercises effective control over the legal person, including in his or her capacity as executive officer, non-executive director, independent non-executive director, director, or manager, or trustee (such person is also referred to as a controlling person).

This determination is not solely based on persons noted as owners or management on business documentation. For example, if a company is owned by another company or a trust, the beneficial owners are the natural persons controlling that second company or trust.

Cash/cash transaction: Refers to coins and paper money of the Republic or of another country designated as legal tender and customarily used and accepted as a medium of exchange in the country of issue. This also includes travelers' checks but excludes negotiable instruments and fund transfers not involving physical cash.

Email: support@vaultfunder.trade

Address: 605 Touchstone House, 7 Bree Street, Cape Town, South Africa



CDD Procedures: Customer Due Diligence procedures involve the identification and verification of the identities of clients.

ECDD (Enhanced Due Diligence): The application of enhanced due diligence involves investigating and obtaining additional information and verification when a client or transaction is classified as high risk for Money Laundering/Terrorist Financing (ML/TF).

Money Laundering: An activity likely to conceal or disguise the nature, source, location, disposition, or movement of the proceeds of unlawful activity, including any activity that constitutes an offense under Section 64 of FICA or Sections 4, 5, and 6 of POCA.

PEP's (Politically Exposed Persons): High-risk clients with more opportunities than ordinary nationals to gain assets through illegal means like bribery and money laundering. PEPs can be foreign, domestic, or International Organization PEPs, each carrying different risk levels.

POCA: The Prevention of Organized Crime Act, 121 of 1998, which provides for money laundering offenses and forfeiture of proceeds of crime.

Proceeds of Crime: Any financial benefit that a criminal derives from criminal activity.

Proceeds of Unlawful Activities: Property, service, advantage, benefit, or reward acquired, received, or retained, directly or indirectly, connected with unlawful activity carried on by any person.

Single Transaction: A transaction other than one in the course of a business relationship, with a value not less than R 5000.00, except for Section 20A cases.

Smurfing, Splitting, Structuring: Money laundering methods involving the splitting of proceeds of crime into smaller amounts to evade detection.

Suspicious Activity Reporting: A report submitted by the Accountable Institution (AI) in terms of Section 29(1) of the Act concerning proceeds of unlawful activities or money laundering. It applies to activities involving multiple parties or inquiries about a transaction under Section 29(2).

STR (Suspicious or Unusual Transaction Report): A report submitted by the AI in terms of Section 29(1) of the Act concerning proceeds of unlawful activities or money laundering related to a transaction or series of transactions between multiple parties.

Transaction: A transaction concluded between a client and an AI in line with the institution's business type, including transactions beyond money flow.

Unlawful Activity: Conduct constituting a crime or violating any law, whether before or after the commencement of POCA, in the Republic of South Africa or elsewhere.

Verification: A process where an AI investigates and collects documentation providing sufficient proof of requested client information and compares it with confirming documentation.

4. AML Compliance Officer

VaultFunder a product of Fintech Focused designates an AML Compliance Officer responsible for implementing and overseeing the AML program. The AML Compliance Officer will:

Email: support@vaultfunder.trade

Address: 605 Touchstone House, 7 Bree Street, Cape Town, South Africa



- Develop and maintain AML policies and procedures.
- Ensure employees are trained on AML requirements.
- Monitor and report suspicious activities.
- Conduct periodic risk assessments.
- Stay updated on changes in AML laws and regulations.

5. Customer Due Diligence (CDD) Identification and Verification

VaultFunder a product of Fintech Focused will perform customer due diligence on all customers, including:

- Identifying and verifying customer identities, including full name, date of birth, identity number (for South African citizens) or passport number (for non-South African citizens), residential address, email address, and telephone number.
- Maintaining records of customer information.
- Conducting ongoing monitoring of customer transactions.

6. Verification Methods

- Individuals: Verify identity by reviewing original identity documents such as a South African driver's license, passport, or identity card. For non-South African persons, a passport is used.
- Businesses: Verify identity by reviewing original registration documents, including the certificate of incorporation or business registration certificate.
- Other organizations: Verify identity by reviewing the original constitution or trust deed.
- Beneficial Owner Identification and Verification: Identify and verify individuals who ultimately own or control the customer or exercise significant influence over the customer.
- Politically Exposed Person (PEP) Screening: Screen customers and beneficial owners against lists of PEPs using internal systems. PEPs are individuals holding or having held prominent public positions or functions or being close associates of such individuals.
- Using third-party data sources: Employ third-party data sources, such as public records and commercial databases, to verify the identity of beneficial owners.

7. Reporting Suspicious Activities

All employees must promptly report suspicious activities to the AML Compliance Officer. VaultFunder a product of Fintech Focused (Pty) Ltd will submit Suspicious Activity Reports (SARs) to relevant authorities as required by law.

8. Record Keeping

Email: support@vaultfunder.trade

Address: 605 Touchstone House, 7 Bree Street, Cape Town, South Africa



VaultFunder a product of Fintech Focused (Pty) Ltd will maintain records of customer identification and transactions for the required period as per applicable laws and regulations.

9. Employee Training

VaultFunder a product of Fintech Focused (Pty) Ltd will provide regular AML training to all employees to ensure awareness and compliance with AML policies and procedures.

10. Sanctions Screening

VaultFunder a product of Fintech Focused (Pty) Ltd will screen customers and transactions against applicable sanctions lists to prevent engagement with prohibited entities.

11. Independent Review

The AML program will undergo periodic independent reviews to assess its effectiveness and compliance with regulations.

12. Non-Retaliation

VaultFunder a product of Fintech Focused (Pty) Ltd prohibits retaliation against employees who report AML concerns in good faith.

13. Penalties for Non-Compliance

Failure to comply with this AML policy may result in disciplinary action, including termination of employment or contractual relationship.

14. Reporting

Any violations of this AML policy or suspicions of money laundering should be reported to the AML Compliance Officer immediately.

15. Commitment

VaultFunder a product of Fintech Focused (Pty) Ltd is committed to preventing money laundering and terrorist financing. The company will implement and enforce anti-money laundering and counter-terrorist financing policies and procedures to ensure its products and services are not used to facilitate these crimes. VaultFunder a product of Fintech Focused (Pty) Ltd is dedicated to complying with all applicable KYC requirements and will regularly review KYC procedures to ensure they are effective and up-to-date.

16. Amendments

This AML and KYC policy may be amended as necessary to remain compliant with changing laws and regulations.

17. Contact Us:

If you have any questions about this policy, please contact us at support@vaultfunder.trade.

Email: support@vaultfunder.trade

Address: 605 Touchstone House, 7 Bree Street, Cape Town, South Africa