MINT

# Anti-Money Laundering, Counter-Terrorist Financing and Proliferation Financing

MINT PLATFORMS (PTY) LTD

INVEST | BORROW | PROTECT

FSP 55118 | NCRCP22892

# MINT PLATFORMS (PTY) LTD

## PUBLIC STATEMENT ON

## Anti-Money Laundering, Counter-Terrorist Financing and Proliferation Financing

## 1. FOREWORD FROM THE BOARD

1.1. MINT Platforms (Pty) Ltd ("**MINT**") is a South African fintech business that operates a regulated, technology-enabled investment and digital assets platform. MINT is authorised as a Financial Services Provider under the Financial Advisory and Intermediary Services Act 37 of 2002 and is registered as an accountable institution under the Financial Intelligence Centre Act 38 of 2001 ("**FIC Act**") and as a Crypto-Asset Service Provider under the applicable Financial Sector Conduct Authority Conduct Standard.

1.2. This Public Statement on Anti-Money Laundering, Counter-Terrorist Financing and Proliferation Financing ("**Statement**") is issued by the Board of Directors of MINT to communicate MINT's approach, commitments, and obligations in relation to the prevention of money laundering, terrorist financing, and proliferation financing (collectively "**ML/TF/PF**") to its customers, counterparties, regulators, investors, and the public.

1.3. This Statement is issued in accordance with MINT's obligations as a regulated financial services business and reflects MINT's policy position as at June 2026. It should be read together with MINT's Terms and Conditions, Privacy Policy, and Complaints Policy, all of which are available at www.mymint.co.za.

## 2. REGULATORY AND LEGAL FRAMEWORK

MINT's AML/CTF/PF framework is governed by, and must be read in the context of, the following principal legislation, regulatory instruments, and international standards:

2.1. The FIC Act and all regulations, directives, guidance notes, and public compliance communications issued thereunder. The FIC Act is the primary South African statute governing the obligations of accountable institutions in relation to ML/TF/PF. MINT is registered with the Financial Intelligence Centre ("**FIC**") as an accountable institution under the applicable category of Schedule 1 to the FIC Act.

2.2. The Financial Intelligence Centre Amendment Act 1 of 2017, which introduced a risk-based approach to compliance as the governing framework for accountable institutions in South Africa.

2.3. Guidance Note 7A issued by the FIC, which provides the definitive regulatory guidance on the risk-based approach to combating ML/TF/PF and which informs the structure and calibration of MINT's internal compliance programme.

2.4. The Financial Advisory and Intermediary Services Act 37 of 2002 ("**FAIS Act**") and the General Code of Conduct for Authorised Financial Services Providers and Representatives, under which MINT holds FSP Licence Number 55118.

2.5. The Financial Sector Regulation Act 9 of 2017 ("**FSR Act**") and any Conduct Standards and directives issued by the Financial Sector Conduct Authority ("**FSCA**") applicable to MINT's regulated activities, including its crypto-asset services.

2.6. The Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004 ("**POCDATARA**") and the Charter of the United Nations Act 69 of 1962, which domesticate the United Nations Security Council Resolutions on targeted financial sanctions and proliferation financing into South African law.

2.7. The Currency and Exchanges Act 9 of 1933 and the Exchange Control Regulations published thereunder, which govern cross-border flows of funds and crypto-assets involving South African resident customers.

2.8. The standards and recommendations of the Financial Action Task Force ("**FATF**"), of which South Africa is a member. MINT's compliance programme is calibrated to meet FATF standards in addition to domestic legal requirements.

2.9. The Protection of Personal Information Act 4 of 2013 ("**POPIA**"), which governs the processing of personal information collected by MINT in the course of performing its AML/CTF/PF obligations.

## 3. MINT'S AML/CTF/PF COMMITMENTS

MINT's AML/CTF/PF framework is founded on the following nine commitments, each of which reflects a specific obligation under the FIC Act and applicable regulatory standards. Together, these commitments constitute MINT's public undertaking to its customers, regulators, and the South African financial system:

3.1. MINT maintains a zero-tolerance position toward money laundering, terrorist financing, and proliferation financing across all products, services, and markets in which it operates. No commercial consideration justifies the facilitation of financial crime, and MINT's internal policies, systems, and training programmes are designed to give effect to this position without exception.

3.2. MINT applies a formal risk-based framework calibrated to the specific ML/TF/PF risks presented by its customers, products, delivery channels, and geographic exposure, in

accordance with the FIC Act and FATF standards. Controls are applied in proportion to the level of risk identified and are not applied uniformly regardless of risk.

3.3. MINT verifies the identity of every customer before establishing any business relationship or processing any transaction. Verification covers identity, residential address, source of funds, and, where applicable, beneficial ownership. Ongoing monitoring ensures that customer profiles remain current and accurate throughout the duration of the relationship.

3.4. MINT continuously monitors all transactions for indicators of suspicious activity, including unusual patterns, high-risk flows, and behaviours inconsistent with a customer's known profile and stated purpose of the relationship. Automated monitoring systems generate alerts that are reviewed by MINT's compliance function.

3.5. MINT screens all customers, beneficial owners, and counterparties against applicable targeted financial sanctions lists on an ongoing basis, including United Nations Security Council designations, domestic FIC lists, and other applicable international lists. No transaction is processed with or for a designated person or entity.

3.6. MINT files all required reports with the Financial Intelligence Centre, including suspicious transaction reports, unusual transaction reports, cash threshold reports, and terrorist property reports, within the timeframes prescribed by the FIC Act. Reporting is overseen by the Compliance Officer.

3.7. MINT retains customer due diligence records and transaction records for a minimum of five years from the termination of the relationship or the date of the transaction, in compliance with sections 22 and 23 of the FIC Act. All records are stored securely in a manner that permits timely retrieval by regulatory authorities on request.

3.8. All MINT employees, officers, and agents receive mandatory AML/CTF/PF training at onboarding and at least annually thereafter. Training covers the applicable regulatory framework, red-flag indicators, internal reporting obligations, the tipping-off prohibition, and the personal legal consequences of non-compliance.

3.9. MINT's Board of Directors retains ultimate accountability for the AML/CTF/PF framework. The Board-appointed Risk and Compliance Committee provides ongoing oversight and receives quarterly compliance reports from the Compliance Officer. An independent audit of the AML/CTF/PF framework is conducted at least annually.

## 4. GOVERNANCE STRUCTURE

MINT has established a governance structure that ensures clear accountability for AML/CTF/PF compliance at every level of the organisation:

4.1. The Board of Directors of MINT bears ultimate responsibility for ensuring that MINT maintains an effective AML/CTF/PF compliance framework. The Board approves MINT's Risk Management and Compliance Programme ("**RMCP**"), applies its mind to the adequacy of the RMCP at least annually, and satisfies itself that sufficient resources, systems, and controls are in place to implement the RMCP effectively. This responsibility cannot be delegated away.

4.2. The Board has constituted a Risk and Compliance Committee ("**RCC**") as a Board sub-committee. The RCC receives quarterly AML/CTF/PF compliance reports from the Compliance Officer, oversees the adequacy and effectiveness of MINT's compliance framework, reviews the findings of internal and external audits, and escalates material compliance matters to the full Board.

4.3. MINT has appointed a suitably qualified and senior-level Compliance Officer in terms of section 43A of the FIC Act. The Compliance Officer's appointment is registered with the FIC. The Compliance Officer is responsible for the design, implementation, maintenance, and continuous improvement of MINT's AML/CTF/PF framework, for the filing of all required reports with the FIC, and for reporting to the RCC and the Board on all compliance matters. The Compliance Officer's reporting line is independent of MINT's operational and commercial functions.

4.4. MINT has appointed a Deputy Compliance Officer to act in the absence or incapacity of the Compliance Officer, ensuring continuity of the AML/CTF/PF function at all times.

4.5. MINT arranges for an independent review or audit of its AML/CTF/PF framework at least annually. The findings of each review are reported to the RCC and the Board, and all deficiencies identified are remediated within agreed timeframes under the oversight of the RCC.

## 5. RISK-BASED APPROACH

MINT adopts a risk-based approach to AML/CTF/PF compliance as required by section 42 of the FIC Act and the FIC's Guidance Note 7A. Under this approach, MINT's compliance measures are calibrated to the specific ML/TF/PF risks presented by its business rather than applied uniformly across all customers and transactions:

5.1. MINT conducts a formal institutional ML/TF/PF risk assessment that identifies and assesses the inherent risks to which MINT is exposed across five dimensions: customer risk, product and service risk, delivery channel risk, geographic risk, and emerging risk typologies. The risk assessment is reviewed and updated at least annually and whenever a material change in MINT's business model, product offering, or risk environment occurs. The institutional risk assessment is approved by the Board.

5.2. MINT applies a documented Customer Risk Scoring Model to every customer at onboarding and on an ongoing basis throughout the relationship. The model assigns a risk score based on a weighted assessment of customer type, jurisdiction, product usage, transaction patterns, source of funds plausibility, delivery channel, and the results of screening processes. Each customer is classified as Low, Medium, or High risk. The risk classification determines the applicable level of customer due diligence, the frequency of ongoing monitoring, and applicable transaction limits.

5.3. Compliance resources and controls are applied in proportion to assessed risk. Low-risk customers are subject to simplified due diligence measures. Customers assessed at standard risk are subject to full customer due diligence. High-risk customers, including all politically exposed persons and their associates, are subject to enhanced due diligence, senior management approval, and more frequent review.

5.4. MINT treats proliferation financing as a distinct risk category requiring specific assessment and controls, separate from money laundering and terrorist financing. MINT's institutional risk assessment includes a standalone proliferation financing component. Screening against all applicable targeted financial sanctions lists extends to proliferation-related designations under the UNSC Resolutions and POCDATARA.

## 6. CUSTOMER DUE DILIGENCE

MINT applies a comprehensive customer due diligence framework in accordance with sections 21 to 21E of the FIC Act. The purpose of customer due diligence is to establish and verify the identity of customers and their beneficial owners before a business relationship is established or a transaction is processed, and to maintain a current and accurate understanding of the customer relationship throughout its duration:

6.1. Every customer must be identified and verified before MINT establishes a business relationship or processes any transaction. For individual customers, MINT collects and verifies full legal name, date of birth, identity number or passport number, nationality, and residential address, using reliable and independent sources including, where

available, electronic verification against the Department of Home Affairs National Population Register. For juristic entity customers, MINT verifies the entity's registration details, constitutional documents, directorship, and beneficial ownership structure.

6.2. MINT identifies and verifies the natural persons who ultimately own or control every juristic entity, trust, and partnership customer. MINT does not rely solely on a fixed percentage ownership threshold for this purpose. Any natural person who exercises effective control over an entity through ownership, voting rights, contractual arrangements, or other means must be identified as a beneficial owner, regardless of the size of their interest in the entity.

6.3. All individual customers and the beneficial owners of all juristic entity customers are screened against MINT's politically exposed persons ("**PEP**") database at onboarding and on a continuous basis throughout the relationship. Every PEP relationship is subject to enhanced due diligence, including verification of source of funds and source of wealth, senior management approval before the relationship is established or continued, and more frequent review. No PEP relationship may be established without the approval of the Compliance Officer and a member of MINT's Executive Committee.

6.4. MINT monitors all customer relationships and transactions continuously throughout the duration of the relationship. Monitoring encompasses transaction volumes, values, frequencies, geographic counterparties, and consistency with the customer's known profile, stated purpose, and source of funds. Customer risk classifications are reviewed periodically and updated where circumstances change or where monitoring identifies indicators of heightened risk.

6.5. Where MINT is unable to complete the required identification and verification steps, or where information provided by a customer is false, misleading, or incapable of verification, MINT will decline to establish the business relationship or will terminate an existing relationship in accordance with section 21E of the FIC Act. MINT will not process any further transactions through the relevant account and will assess whether the circumstances give rise to a reportable suspicion.

## 7. TRANSACTION MONITORING AND SANCTIONS SCREENING

7.1. MINT operates automated transaction monitoring systems that analyse transaction volumes, values, frequencies, and counterparty geographies against defined risk thresholds and alert parameters. All alerts generated by MINT's monitoring systems are reviewed by MINT's compliance function and escalated to the Compliance Officer where required. Transaction monitoring parameters are reviewed and updated at least

annually in line with MINT's institutional risk assessment and current ML/TF/PF typologies.

7.2. MINT screens all customers, beneficial owners, directors, and counterparties against the following sanctions lists at onboarding and on a continuous basis throughout the relationship:

7.2.1. the targeted financial sanctions lists published by the United Nations Security Council pursuant to the Charter of the United Nations Act 69 of 1962;

7.2.2. the domestic targeted financial sanctions lists published by the FIC pursuant to section 26A of the FIC Act;

7.2.3. the OFAC Specially Designated Nationals and Blocked Persons List and the EU Consolidated Financial Sanctions List, to the extent that MINT has exposure to relevant jurisdictions; and

7.2.4. such other lists as may be required by applicable law or as directed by the FIC or FSCA from time to time.

7.3. Where a sanctions screening match is confirmed, MINT will immediately freeze all funds and assets associated with the relevant customer, file the required report with the FIC, and notify the relevant competent authority, all in accordance with the FIC Act and POCDATARA. MINT will not process any transaction that would result in a payment to or from a designated person or entity.

7.4. Given the heightened ML/TF/PF risks presented by crypto-asset transactions, MINT applies enhanced controls to all crypto-asset activities. These include blockchain analytics screening of transaction flows and wallet addresses, risk assessment of external wallet addresses before transfers are permitted, transaction monitoring calibrated to crypto-asset-specific typologies including mixer and tumbler detection, and compliance with the FATF Travel Rule requirements for virtual asset transfers above the applicable reporting threshold.

## 8. REGULATORY REPORTING OBLIGATIONS

MINT is subject to the following reporting obligations under the FIC Act and discharges each of them in accordance with the prescribed requirements:

8.1. MINT files a Suspicious Transaction Report ("**STR**") with the FIC in terms of section 29 of the FIC Act whenever MINT knows or suspects, or has reasonable grounds to know or suspect, that funds involved in a transaction represent the proceeds of unlawful activities, are connected to terrorist financing or proliferation financing, or where information becomes available in the course of MINT's business that may be relevant to an investigation of an unlawful activity.

8.2. MINT files an Unusual Transaction Report ("**UTR**") with the FIC in terms of section 28A of the FIC Act in respect of transactions that are unusual or appear to have no apparent business or lawful purpose, even in the absence of a specific suspicion of ML/TF/PF.

8.3. MINT files Cash Threshold Reports ("**CTRs**") with the FIC in terms of section 28 of the FIC Act in respect of all cash transactions above the prescribed reporting threshold.

8.4. MINT files Terrorist Property Reports ("**TPRs**") with the FIC in terms of section 28A of the FIC Act whenever MINT knows or suspects that it has possession or control of funds or property owned or controlled by, or on behalf of, a person involved in terrorist activities or proliferation financing.

8.5. MINT strictly observes the tipping-off prohibition under section 29(2) of the FIC Act. No employee, officer, director, contractor, or agent of MINT may disclose to any person that a report has been, is being, or will be submitted to the FIC, or that a person is the subject of any such report. Violation of this prohibition constitutes a criminal offence under the FIC Act.

## 9. EXCHANGE CONTROL

9.1. MINT implements controls to ensure that all cross-border transfers of funds and crypto-assets comply with the Currency and Exchanges Act 9 of 1933 and the Exchange Control Regulations published thereunder. Before facilitating any cross-border transfer or externalisation of funds for a South African resident customer, MINT verifies the applicable exchange control allowance available to that customer, including the Single Discretionary Allowance and the Foreign Investment Allowance, and applies system controls that prevent a transfer from being processed where it would cause a customer to exceed their available allowance without South African Reserve Bank approval.

9.2. All cross-border transfers and crypto-asset externalisation transactions are logged in MINT's cross-border transfer register, which records the customer's identity, the amount, the currency, the destination, the date, the exchange control category applied, and the outcome of MINT's AML/CTF/PF risk review. This register is available to the South African Reserve Bank, FSCA, and FIC on request.

## 10. YOUR OBLIGATIONS AS A CUSTOMER

MINT's AML/CTF/PF framework places certain obligations on customers. By opening an account with MINT and using MINT's Services, every customer acknowledges and agrees to the following:

10.1. You must provide accurate, complete, and current information at all times. This includes identity information, proof of residential address, declarations regarding source of funds and source of wealth, and beneficial ownership information. You must promptly notify MINT of any change in your personal or business circumstances that may affect your identity, risk profile, or eligibility to use MINT's Services.

10.2. MINT may at any time request additional documentation or information from you in connection with its customer due diligence, enhanced due diligence, or ongoing monitoring obligations. You must respond to such requests within the timeframe specified by MINT. Failure to respond may result in MINT restricting, suspending, or terminating your account.

10.3. You may not use MINT's platform, directly or indirectly, to launder money, finance terrorism or proliferation financing, evade sanctions, or engage in any other activity that contravenes applicable AML/CTF/PF legislation. MINT reserves the right to restrict, suspend, or terminate any account where prohibited use is detected or reasonably suspected.

10.4. South African resident customers are responsible for ensuring that their use of MINT's Services complies with applicable exchange control requirements. MINT's system controls assist customers in tracking their allowance utilisation but do not substitute for each customer's personal obligation to comply with the Currency and Exchanges Act and the Exchange Control Regulations.

10.5. Where a customer becomes aware of information that may indicate that funds involved in a transaction are connected to unlawful activity, the customer should not process the transaction and should contact MINT's Compliance Officer immediately at compliance@mymint.co.za.

## 11. CONSEQUENCES OF NON-COMPLIANCE

MINT takes non-compliance with its AML/CTF/PF obligations seriously and will take decisive action in all cases where a breach is detected or reasonably suspected:

11.1. Where a customer is found to be in breach of MINT's AML/CTF/PF requirements, to have provided false or misleading information, to be the subject of a sanctions designation, or to be using MINT's platform for prohibited purposes, MINT will, without prior notice where required by law or risk management, restrict, suspend, or terminate the account; freeze or block funds and assets in the account; decline to process any transaction; and report the matter to the FIC, FSCA, and other competent authorities as required by applicable law.

11.2. Any employee, officer, director, contractor, or agent of MINT who fails to comply with MINT's AML/CTF/PF framework is subject to disciplinary action up to and including summary dismissal. Violations that constitute criminal offences under the FIC Act or other applicable legislation are reported to the relevant law enforcement and regulatory authorities.

11.3. Non-compliance with the FIC Act may expose MINT as an institution to administrative sanctions under Chapter 7 of the FIC Act, including fines of up to the greater of R10 million or ten per cent of MINT's annual turnover, debarment or suspension of operations, and criminal prosecution of directors, officers, and employees. MINT's AML/CTF/PF framework is designed to ensure that MINT meets its obligations and avoids these outcomes.

## 12. DATA PROTECTION AND PRIVACY

12.1. MINT processes personal information collected in the course of its AML/CTF/PF activities strictly in accordance with POPIA and MINT's Privacy Policy. The processing of personal information for AML/CTF/PF purposes is necessary for MINT to comply with its legal obligations under the FIC Act and applicable financial services legislation. MINT minimises the personal information collected to that which is strictly necessary for compliance purposes, implements appropriate technical and organisational security measures to protect that information, and retains it only for the periods required by law.

12.2. Where MINT is required by law to disclose personal information to the FIC, FSCA, SARB, SARS, or other regulatory or law enforcement authorities, it does so in accordance with applicable law. MINT does not disclose personal information collected for AML/CTF/PF purposes to third parties for commercial purposes.

12.3. Data subjects have rights of access, correction, objection, and complaint under POPIA. These rights may be exercised by contacting MINT's Information Officer at compliance@mymint.co.za. Complaints regarding MINT's data processing activities may be referred to the Information Regulator of South Africa at www.inforegulator.org.za.

## 13. CONTACTING MINT

Customers, counterparties, and other stakeholders who have questions about this Statement or about MINT's AML/CTF/PF obligations and practices are welcome to contact MINT's Legal, Risk and Compliance function using the following contact details:

13.1. Compliance Officer: Kevin Pillay.

13.2. Email: compliance@mymint.co.za.

13.3. Telephone: +27 (10) 276-0531.

13.4. Physical Address: 3 Gwen Lane, Sandown, Sandton, 2031.

13.5. Website: www.mymint.co.za.

13.6. If you have information that may indicate that funds on MINT's platform are connected to money laundering, terrorist financing, proliferation financing, or other unlawful activity, please contact the Compliance Officer immediately at compliance@mymint.co.za or call +27 (10) 276-0531. You may also report directly to the Financial Intelligence Centre at www.fic.gov.za.

## 14. REVIEW AND AMENDMENT OF THIS STATEMENT

This Statement will be reviewed by MINT's Compliance Officer at least annually and updated to reflect material changes in applicable law, regulatory requirements, MINT's risk profile, or MINT's business model. Material amendments are approved by the Board of Directors. The current version of this Statement is published on MINT's website at www.mymint.co.za and constitutes the authoritative version.

**[END]**