AML, CFT AND SANCTIONS COMPLIANCE POLICY

TPay AML, CFT and Sanctions Compliance Policy

Entity	TPPPAY (Pty) Ltd
Trading Name	TPay Africa
Shortened Brand Reference	TPay
Registration Number	2025/544950/07
Website	www.tppp.africa
Version	Version 1.0
Effective Date	15 May 2026
Classification	Financial Crime Compliance Governance Document
Scope	Public-facing AML, CFT, CPF and sanctions compliance summary

Publication Note: This document explains TPay's public-facing approach to anti-money laundering, counter-terrorist financing, counter-proliferation financing and sanctions compliance.

DOCUMENT CONTROL

Document Title	AML, CFT AND SANCTIONS COMPLIANCE POLICY
Alternative Name	TPay AML, CFT and Sanctions Compliance Policy
Entity	TPPPAY (Pty) Ltd
Trading Name	TPay Africa
Shortened Brand Reference	TPay
Registration Number	2025/544950/07
Website	www.tppp.africa
Contact Email	support@tppp.africa
Physical Address	122 Beech Street, Northcliff, Johannesburg, 2195
Version	Version 1.0
Effective Date	15 May 2026
Review Cycle	Annual or as required
Document Owner	Ronald Gwenzi
Approved By	Board
Classification	Financial Crime Compliance Governance Document

Purpose: This document explains TPay's public-facing approach to anti-money laundering, counter-terrorist financing, counter-proliferation financing, sanctions compliance and financial crime risk management. It forms part of TPay's website and service policy framework and should be read together with TPay's Terms of Website Use, Payment Service Terms, Privacy Policy, PAIA Manual and Complaints Process, where applicable.

LEGAL IDENTITY AND BRAND REFERENCES

Legal Entity	TPPPAY (Pty) Ltd
Registration Number	2025/544950/07
Trading Name	TPay Africa
Shortened Brand Reference	TPay
Website	www.tppp.africa

TPPPAY (Pty) Ltd, registration number 2025/544950/07, conducts business under the trading name ‘TPay Africa’.

For convenience and branding purposes, TPPPAY (Pty) Ltd may use ‘TPay’ as a shortened brand reference to TPay Africa on the Website and in its forms, notices, communications, product materials, templates and other documents.

Where ‘TPay’ appears together with the existing TPay logo, the Website address www.tppp.africa, or the legal details of TPPPAY (Pty) Ltd, it must be understood as a reference to TPay Africa, with TPPPAY (Pty) Ltd remaining the relevant legal entity, unless the relevant document expressly states otherwise.

The use of ‘TPay’ as a shortened brand reference does not create a separate legal entity or contracting party. Any agreement concluded under the TPay brand is concluded with TPPPAY (Pty) Ltd, trading as TPay Africa, unless expressly stated otherwise.

Nothing in this document asserts ownership of, affiliation with, endorsement by, or responsibility for any unrelated person or business using ‘TPay’, ‘T Pay’ or a similar name in South Africa or elsewhere.

Contracting party: TPPPAY (Pty) Ltd, Registration No. 2025/544950/07, trading as TPay Africa and using ‘TPay’ as a shortened brand reference.

TABLE OF CONTENTS

AML, CFT AND SANCTIONS COMPLIANCE POLICY

TPay AML, CFT and Sanctions Compliance Policy

Public-Facing Compliance Notice: This policy is a public-facing compliance summary. It does not disclose TPay's confidential internal control framework, monitoring thresholds, detection rules, investigation methods or risk scoring logic.

1. Introduction and Scope

1.1 This AML, CFT and Sanctions Compliance Policy applies to TPPPAY (Pty) Ltd, registration number 2025/544950/07, trading as TPay Africa.

1.2 The official TPay website is www.tppp.africa.

1.3 This policy describes TPay's public-facing approach to anti-money laundering, counter-terrorist financing, counter- proliferation financing, sanctions compliance, financial crime risk management, merchant due diligence, transaction- related risk monitoring, suspicious activity identification and escalation, and cooperation with banks, payment partners, regulators and lawful authorities, where applicable.

1.4 This policy is a public-facing compliance statement. It does not replace TPay's internal risk management and compliance procedures, confidential control framework, merchant agreements, bank arrangements or applicable legal obligations.

1.5 This policy forms part of TPay's website and service policy framework and should be read together with TPay's Terms of Website Use, Payment Service Terms, Privacy Policy, PAIA Manual, Complaints Process, merchant agreements, applicable bank or payment partner terms and any other commercial agreement concluded with TPay, where applicable.

1.6 If there is any inconsistency between this policy and another TPay document, the document that specifically governs the relevant subject matter will apply to that subject matter, unless otherwise stated in writing.

2. Definitions and Interpretation

2.1 In this policy, unless the context indicates otherwise, the following words and expressions have the meanings set out below.

applicable to TPay's business model, payment arrangements, banks, payment partners or legal obligations. Suspicious Activity means activity, conduct, information or transaction behaviour that may indicate financial crime, sanctions risk, fraud, unlawful conduct or misuse of TPay's services. TPay means the shortened brand reference used by TPPPAY (Pty) Ltd, registration number 2025/544950/07, trading as TPay Africa. Transaction means a payment-related transaction or payment instruction supported through the Payment Service. User means a consumer, payer, merchant, authorised representative, website user or other person who interacts with TPay or uses TPay's services. we, us, our means TPay. you, your means the relevant User, Merchant or other person interacting with TPay, as the context requires. 2.2 References to laws include those laws as amended, replaced or re-enacted from time to time. Headings are for convenience only and do not affect interpretation.

3. Who We Are

3.1 TPPPAY (Pty) Ltd, registration number 2025/544950/07, trading as TPay Africa, operates a fintech payment services business.

3.2 TPay provides payment service-related functionality and supports payment instructions through approved payment flows and relevant payment ecosystem arrangements, where applicable.

3.3 TPay is not a bank. Banking services, bank account access, bank authentication, clearing and settlement processes remain subject to the relevant banks, payment system participants, payment rules and applicable legal frameworks.

3.4 Nothing in this policy should be read as a claim that TPay holds a particular licence, approval, registration, certification, bank sponsorship, payment system status or regulatory approval unless such status is separately and expressly confirmed by TPay in writing or in a formal public statement.

4. Compliance Commitment

4.1 TPay is committed to supporting a safe, transparent and compliant payment environment and to maintaining controls proportionate to its business model, operational role and risk profile.

4.2 TPay's compliance commitment includes preventing misuse of its services for money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud and other financial crime.

• applying a risk-based approach to financial crime controls; • cooperating with banks, payment partners, regulators and lawful authorities where required; • protecting the integrity of payment-related services and systems; • supporting appropriate due diligence, risk monitoring and escalation processes; and • reviewing its approach as laws, risks, payment arrangements and regulatory expectations develop.

5. Applicable Legal and Regulatory Framework

5.1 To the extent applicable to TPay's business model, role, contractual arrangements and regulatory position, TPay's AML, CFT, CPF and sanctions controls may be informed by South African legal and regulatory requirements and relevant payment ecosystem obligations.

• the Financial Intelligence Centre Act, 38 of 2001, as amended; • the Protection of Constitutional Democracy against Terrorist and Related Activities Act, where applicable; • applicable sanctions requirements and restricted-party requirements; • applicable payment system, banking, sponsor bank, payment partner, merchant due diligence or payment-

processing requirements; • applicable data protection and privacy requirements; and • other laws, rules, directives, guidance notes, contractual obligations or regulatory expectations that may apply to

TPay's business model. 5.2 This policy does not make a determination that TPay is an accountable institution or regulated entity for every purpose. Applicable obligations must be assessed with reference to TPay's current business model, role, contracts and regulatory position.

6. Risk-Based Approach

6.1 TPay may apply a risk-based approach to financial crime compliance. This means that controls are designed and applied in a manner that is proportionate to the nature and level of risk presented by a relationship, transaction, activity or service.

6.2 Risk factors that may be considered include customer or merchant profile, business activity, transaction nature, payment method, geographic exposure, product or service type, delivery channel, source of funds indicators where relevant, sanctions exposure, adverse media or reputational risk where relevant, fraud indicators, transaction behaviour and regulatory or payment partner requirements.

6.3 Higher-risk relationships or activities may require enhanced due diligence, additional information, restrictions, refusal, suspension or termination.

7. Merchant Due Diligence

7.1 TPay may conduct due diligence on merchants before onboarding and during the business relationship, where applicable.

• verifying legal entity information; • identifying directors, beneficial owners or authorised representatives, where applicable; • understanding the merchant's business model; • reviewing the merchant's products or services; • assessing prohibited or restricted activities; • verifying bank account or settlement-related information, where applicable; • screening against sanctions or watchlists, where appropriate and lawful; • assessing fraud and reputational risk; • requesting supporting documents; and • performing ongoing review where required. 7.2 This public policy does not disclose TPay's internal scoring models, screening methods, escalation thresholds or sensitive control logic.

8. User and Transaction Risk Controls

8.1 TPay may apply user and transaction-level risk controls where appropriate and lawful.

• transaction monitoring; • fraud detection; • velocity and behavioural monitoring; • review of suspicious indicators; • payment status checks; • review of transaction references; • screening or risk review, where applicable; • escalation of unusual or suspicious activity; and • transaction delay, refusal, suspension or restriction where reasonably necessary. 8.2 TPay does not publish transaction thresholds, detection triggers, monitoring rules or internal control logic because disclosure of such information could undermine the effectiveness of financial crime controls.

9. Sanctions Compliance

9.1 TPay seeks to comply with applicable sanctions obligations and restricted-party requirements to the extent applicable to its business model, contractual arrangements and payment ecosystem role.

9.2 TPay may screen merchants, counterparties, users, beneficial owners, representatives, transactions or other relevant parties against applicable sanctions lists, where appropriate and lawful.

9.3 TPay may refuse, suspend, block, escalate or terminate a relationship, transaction or service access where sanctions risk is identified or reasonably suspected.

9.4 TPay may cooperate with banks, payment partners, regulators, law enforcement authorities or other lawful authorities in relation to sanctions-related matters, subject to applicable law and privacy requirements.

10. Prohibited and Restricted Activities

10.1 TPay's services may not be used for unlawful activity, prohibited financial crime, sanctions evasion or activity prohibited by applicable payment partner, bank or TPay requirements.

• money laundering; • terrorist financing; • proliferation financing; • sanctions evasion; • fraud, scams, identity theft or unauthorised payment activity; • illegal goods or services; • stolen goods; • unlawful gambling; • unlawful adult services; • illegal drugs or controlled substances; • weapons or prohibited goods, where unlawful; • human trafficking, exploitation or abusive conduct; • corruption, bribery or tax evasion; • cybercrime or misuse of systems; • any activity prohibited by law, payment partner requirements, bank requirements or TPay's policies. 10.2 TPay may restrict, suspend, refuse or terminate access where prohibited or restricted activity is identified or reasonably suspected.

11. Suspicious Activity Identification and Escalation

11.1 TPay may identify and escalate suspicious activity where appropriate. Suspicious activity may include unusual transaction behaviour, inconsistent merchant activity, suspected fraud, unauthorised payment activity, sanctions indicators, false information, unusual payment patterns or conduct inconsistent with the stated business purpose.

11.2 Where appropriate, TPay may request further information, place a transaction or relationship under review, restrict access, delay or refuse processing, escalate internally to compliance or risk functions, engage banks, payment partners or merchants, or report to relevant authorities where legally required.

11.3 This policy does not disclose internal suspicious activity typologies, rules, thresholds or investigation methods.

12. Reporting Obligations

12.1 Where TPay is legally required or contractually required to report or escalate a financial crime concern, TPay will do so through the appropriate reporting, bank, payment partner, regulatory or lawful authority channel.

12.2 Reportable matters may include suspicious or unusual activity, sanctions concerns, suspected fraud, unlawful activity or other matters that require escalation under applicable law, payment partner requirements or contractual arrangements.

12.3 TPay may be restricted by law or by the integrity of an investigation from disclosing the details of a report, escalation or investigation to a user or merchant.

13. Recordkeeping

13.1 TPay may maintain records relating to due diligence, merchant onboarding, transaction information, payment instructions, risk reviews, screening results where applicable, complaints, investigations, suspicious activity escalations, compliance decisions and supporting documents.

13.2 Records will be retained for periods required by applicable law, contract, payment partner requirements, regulatory expectations, business requirements or legitimate risk management purposes.

13.3 Records containing personal information will be handled in accordance with TPay's Privacy Policy and applicable data protection requirements.

14. Ongoing Monitoring and Review

14.1 TPay may monitor relationships and transactions on an ongoing basis, proportionate to risk.

• periodic review of merchant information; • review of transaction behaviour; • review of suspicious or unusual activity; • updating due diligence information; • sanctions or watchlist screening, where applicable; • reassessing risk ratings; • reviewing compliance incidents or complaints; and • taking corrective action where required.

15. Training and Awareness

15.1 TPay supports financial crime awareness among relevant personnel, contractors or service providers, where applicable.

15.2 Training or awareness may cover AML and CFT obligations, sanctions risk, fraud indicators, merchant due diligence, suspicious activity escalation, privacy and confidentiality, complaints and incident reporting, and responsible handling of payment-related information.

16. Governance and Accountability

16.1 TPay's financial crime compliance approach is overseen through appropriate governance structures proportionate to its business size, risk profile and operational role.

16.2 Governance responsibilities may include board or senior management oversight, compliance ownership, operational implementation, risk escalation, periodic review of policies, audit or assurance review where applicable, and corrective action tracking.

16.3 TPay may update governance arrangements as its business model, operational scale, regulatory expectations or payment arrangements develop.

17. Cooperation with Banks, Payment Partners and Authorities

17.1 TPay may cooperate with banks, payment partners, merchants, payment system participants, regulators, law enforcement authorities, the Financial Intelligence Centre, the Information Regulator or other lawful authorities where appropriate and lawful.

17.2 Cooperation may include responding to lawful requests, supporting investigations, providing transaction-related information, restricting services or taking corrective action, subject to applicable law and privacy requirements.

17.3 TPay may also cooperate with merchants, service providers or advisers where reasonably required for compliance, fraud prevention, risk management or dispute resolution purposes.

18. Privacy and Confidentiality

18.1 AML, CFT, CPF, sanctions and financial crime compliance activities may involve the processing of personal information.

18.2 Personal information will be processed in accordance with TPay's Privacy Policy, POPIA and applicable law.

18.3 TPay may share information with banks, payment partners, merchants, service providers, regulators or lawful authorities where reasonably required for compliance, fraud prevention, risk management, investigation or legal purposes.

18.4 TPay will take reasonable steps to handle confidential information appropriately and to protect personal information against unauthorised access, loss, misuse, alteration or disclosure.

19. Service Refusal, Suspension and Termination

19.1 TPay may refuse, suspend, restrict or terminate access to its services where doing so is reasonably necessary for compliance, risk management, payment integrity, legal obligations or financial crime prevention.

• information is false, incomplete or misleading; • due diligence cannot be completed; • sanctions risk is identified or reasonably suspected; • suspicious activity is detected or reasonably suspected; • fraud risk is identified; • unlawful activity is suspected; • a bank, payment partner or regulator requires action; • the user or merchant breaches TPay's policies or agreements; or • continuing the relationship creates unacceptable legal, regulatory, operational, reputational or financial crime risk.

20. No Circumvention

20.1 Users and merchants must not attempt to evade, bypass or interfere with TPay's financial crime controls.

• providing false or misleading information;

• using another person's identity or bank account without authority; • structuring transactions to avoid controls; • concealing beneficial ownership or control; • using TPay for prohibited activities; • attempting to bypass sanctions controls; • providing misleading business information; or • refusing lawful or reasonable due diligence requests. 20.2 Attempts to circumvent controls may result in refusal, suspension, termination, investigation, escalation or reporting where appropriate and lawful.

21. Policy Review and Updates

21.1 TPay may update this policy from time to time.

21.2 The updated version will apply from the date it is published or from the effective date stated in the updated document.

21.3 TPay reviews its AML, CFT, CPF and sanctions approach periodically or when there are material changes to its business model, laws, risks, payment arrangements or regulatory expectations.

22. Contact Details

22.1 For compliance-related questions about this policy, please contact TPay using the details below.

Entity TPPPAY (Pty) Ltd Trading as TPay Registration Number 2025/544950/07 Website www.tppp.africa Compliance Contact Email support@tppp.africa Address 122 Beech Street, Northcliff, Johannesburg, 2195