DRAFTING NOTE

PAYMENT SYSTEMS AND DIGITAL FINANCE ACT 2026

1. Status and purpose of this note

This drafting note is explanatory and is not part of the proposed Assembly Act. It identifies the legislative need, the relationship with earlier Eritrean law, the principal matters retained, the modernization choices made and the place of the draft within the emerging constitutional statute book. The instrument remains a consultation draft and should be finalized only after legal, institutional, fiscal and public review.

2. Legislative need and prior law

Earlier financial legislation did not anticipate interoperable payments, electronic money, mobile services, fintech, digital identity, automated compliance and cyber risk.

3. What the draft retains

The draft retains central-bank oversight, settlement finality, licensing, safeguarding of customer funds, financial integrity and operational reliability.

4. What the draft updates and modernizes

It establishes technology-neutral authorization, open and fair access, e-money and payment-provider rules, consumer and data protection, interoperability, cyber and outsourcing standards, innovation testing, agent networks, digital inclusion and due process.

5. Constitutional, code and treaty fit

The draft is framed under the Constitution of Eritrea 1997 and must be read with the Civil Code, Penal Code, Civil Procedure Code and Criminal Procedure Code of Eritrea 2015 where those Codes govern. It is also coordinated with the other institutional, financial, commercial, land, labour, administrative and sectoral drafts in this collection. References to international or regional standards guide compatibility and implementation; they do not bypass the Treaty-Making Act or convert an unincorporated instrument into domestic law.

6. Scope and organization

The principal divisions address preliminary provisions; national payment system and public oversight; licensing of operators and providers; payment-system governance and finality; payment services and customer funds; electronic money; fast payments, interoperability and open finance; users, merchants and payment liability; agents, identity and inclusive delivery; data, technology and operational resilience; and the concluding enforcement, transitional and final provisions.

7. Transition, implementation and consultation

The draft preserves lawful accrued rights, completed transactions, pending proceedings and institutional continuity where appropriate, while preventing temporary savings from preserving unconstitutional coercion or indefinite executive discretion. Before enactment or issuance, authentic predecessor instruments and amendments should be verified, cross-references and fiscal capacity confirmed, implementing regulations and digital systems prepared, and affected institutions, professions, communities and the public given a practical opportunity to comment.

CONSULTATION DRAFT — NOT ENACTED LAW

ACT NO. ___ OF 2026

PAYMENT SYSTEMS AND DIGITAL FINANCE ACT 2026

(ASSEMBLY ACT)

AN ACT TO GOVERN PAYMENT SYSTEMS, PAYMENT SERVICES, ELECTRONIC MONEY AND DIGITAL FINANCIAL SERVICES; PROVIDE FOR LICENSING, SETTLEMENT FINALITY, SAFEGUARDING, INTEROPERABILITY, CUSTOMER PROTECTION, OPERATIONAL RESILIENCE AND OVERSIGHT; FACILITATE INCLUSIVE DOMESTIC AND CROSS-BORDER PAYMENTS; AND PROVIDE FOR RELATED MATTERS.

PREAMBLE

WHEREAS Articles 8, 21, 23 and 56 of the Constitution of Eritrea support economic development, property protection, efficient financial institutions and lawful management of the national currency;
WHEREAS Eritrea requires reliable, affordable and interoperable payment infrastructure capable of serving households, businesses, government, rural and pastoral communities and Eritreans abroad;
WHEREAS digital finance can reduce distance, delay, cash-handling cost and exclusion, but requires protection against loss, fraud, surveillance, monopoly, cyber failure and misuse of customer funds;
WHEREAS payment regulation must preserve market choice, cash access, privacy, competition, technological neutrality, transparent exchange and effective remedies;
NOW, THEREFORE, the National Assembly of Eritrea, acting under Articles 32 and 56 of the Constitution, enacts as follows:

CHAPTER I
PRELIMINARY PROVISIONS

Article 1 — Short title

This Act may be cited as the “Payment Systems and Digital Finance Act 2026”.

Article 2 — Objects

1. to establish safe, efficient, inclusive and interoperable national payment arrangements;
2. to permit responsible banks, non-bank providers, technology firms, cooperatives and agents to provide payment services under proportionate rules;
3. to protect customer funds, payment data, transaction finality and continuity of critical services;

4. to support fast payments, electronic money, digital identity, open finance, remittances and innovation without abolishing cash or private choice;
5. to prevent political surveillance, forced exchange, hidden charges, anticompetitive control and unaccountable automated decisions; and
6. to assign clear oversight and enforcement powers consistent with the Constitution and related Assembly Acts.

Article 3 — Constitutional limits

1. The National Bank's constitutional responsibility for currency and financial institutions supports oversight of the national payment system as detailed by Assembly legislation.
2. No digital form of payment becomes legal tender, public money or a compulsory means of payment except under an Assembly Act and lawful National Bank action.
3. No authority may use this Act to appropriate money, impose tax, compel political monitoring, confiscate foreign currency or abolish reasonable cash access.
4. A limitation of privacy, property, expression, movement or administrative justice shall satisfy Articles 26 and 28 of the Constitution.

Article 4 — Application of Act

1. This Act applies to a payment system, payment-system operator, payment-service provider, electronic-money issuer, agent and digital-finance activity conducted in or materially directed to Eritrea.
2. It applies to the National Bank when it owns or operates payment infrastructure, subject to constitutional monetary functions and equivalent public accountability.
3. It applies to government payments, public revenue collection and public disbursement to the extent they use regulated payment services.
4. A foreign provider is subject to this Act when it targets Eritrean users, holds their funds or data, or connects materially to Eritrean payment infrastructure.

Article 5 — Interpretation

1. "agent" means a person authorized to provide specified payment services on behalf of a licensed provider;
2. "Bank" means the National Bank of Eritrea;
3. "customer funds" means money or monetary value received from or for a user for execution of payment or issuance of electronic money;
4. "digital finance" means regulated financial service initiated, delivered, recorded or supported primarily through electronic technology;
5. "electronic money" means monetary value stored electronically, issued on receipt of funds, accepted by a person other than the issuer and redeemable at par;
6. "fast payment system" means a system that makes funds available to a payee in near real time on a continuous or broadly available basis;
7. "operator" means a person responsible for rules and operation of a payment system;
8. "payment account" means an account used to execute payment transactions;

9. “payment instrument” means a personalized device, procedure or agreed means used to initiate a payment order;
10. “payment service” includes account operation, cash placement or withdrawal, transfer, direct debit, card or device payment, acquiring, payment initiation, account information, money remittance and electronic-money service;
11. “payment-service provider” means a person authorized under this Act to provide one or more payment services;
12. “payment system” means rules, participants and arrangements for transfer, clearing or settlement of funds;
13. “settlement” means discharge of obligations by transfer of funds or another settlement asset;
14. “systemically important payment system” means a system designated under Article 15;
15. “user” means a payer, payee, account holder, merchant or other person using a payment service; and
16. “virtual asset” means a digital representation of value that may be transferred or used for payment or investment but is not fiat currency, electronic money or another financial asset already governed by law.

Article 6 — Relationship with other laws

1. The National Bank Act governs central-bank status, currency and monetary authority, while this Act governs payment infrastructure and services.
2. The Financial Institutions Act governs prudential licensing and supervision of banks and credit institutions, including when they provide payment services.
3. The Commercial and Civil Codes govern contracts, electronic transactions, agency, negotiable instruments, insolvency and private remedies except where this Act provides a specific payment rule.
4. The Data Protection and Privacy Act, Competition and Consumer Protection Act, Interpretation and General Provisions Act, Anti-Money Laundering legislation and applicable tax, public-finance and cybersecurity laws remain applicable within their fields.
5. The Deposit Protection Act does not insure electronic money or safeguarded payment funds unless that Act expressly provides otherwise.

Article 7 — Technological neutrality and equivalence

1. Equivalent payment functions and risks shall receive equivalent legal treatment regardless of device, network, code, ledger, token, biometric or business name.
2. A law shall not require paper, wet signature, physical branch or proprietary technology where a reliable electronic method performs the legal function.
3. Innovation shall remain open to different technical standards where interoperability, security, audit and user rights are maintained.
4. A technology shall not be approved merely because it is new or rejected merely because it is foreign, open-source or decentralized.

Article 8 — Proportionality and inclusion

1. A requirement shall reflect service, funds held, transaction value, operational dependence, customer vulnerability and systemic importance.
2. Simplified licensing, customer due diligence and reporting may apply to low-risk, low-value services subject to transparent limits and safeguards.
3. Proportionality does not excuse misuse of funds, deceptive pricing, unlawful discrimination, weak security or denial of remedy.
4. Rules shall account for rural distance, pastoral mobility, disability, low literacy, intermittent electricity, basic phones and limited connectivity.

CHAPTER II
NATIONAL PAYMENT SYSTEM AND PUBLIC OVERSIGHT

Article 9 — National payment system

1. The national payment system consists of public and private systems, providers, instruments, rules, infrastructure and users serving payments in Eritrea.
2. It shall support safety, efficiency, competition, inclusion, interoperability, innovation and monetary and financial stability.
3. No single operator or public institution owns the national payment system merely because it provides a component.
4. The Bank shall coordinate development without directing ordinary commercial choice or excluding lawful entrants.

Article 10 — Functions of the Bank

1. The Bank shall license and oversee payment systems, operators, providers and electronic-money issuers according to this Act.
2. It shall adopt technical and prudential standards, monitor risk, collect data, facilitate cooperation and enforce compliance.
3. It may own or operate core infrastructure where public need justifies doing so and governance separates operator and oversight roles.
4. It shall publish policy, decisions, statistics, fees and assessments subject to lawful confidentiality.

Article 11 — Operational separation within the Bank

1. A unit operating a payment system shall be operationally separate from the unit overseeing that system.
2. Oversight standards shall apply to a Bank-operated system to the same extent as to a comparable private system, subject to lawful central-bank functions.
3. Conflicts, pricing, access and performance shall be documented and independently audited.
4. The Bank shall not use regulatory information to give its operating unit an unfair competitive advantage.

Article 12 — National payments council

1. The Bank shall convene a National Payments Council representing providers, operators, government, businesses, consumers, workers, technology, rural communities and persons with disabilities.
2. The Council shall advise on strategy, interoperability, standards, inclusion, competition, resilience and cross-border development.
3. It has no power to license, sanction, fix private prices or decide an individual dispute.
4. Membership, conflicts, minutes and recommendations shall be public.

Article 13 — National payment strategy

1. The Bank shall publish a five-year national payment strategy after public consultation.
2. The strategy shall assess cash, account access, fast payments, government payments, remittances, identity, merchant acceptance, infrastructure, competition and cyber risk.
3. It shall state measurable actions, responsible institutions, costs, dependencies and review dates.
4. Progress shall be reported annually to the National Assembly and public.

Article 14 — Recognition of payment systems

1. An operator shall register or obtain a licence before operating a payment system in Eritrea as prescribed by scale and risk.
2. The Bank shall recognize low-risk closed or limited systems through simplified notice where public funds and stability are not materially exposed.
3. Recognition shall state authorized functions, participants, settlement arrangements and material conditions.
4. A system shall not be represented as guaranteed or operated by the Bank unless true.

Article 15 — Designation of systemically important system

1. The Bank may designate a payment system as systemically important based on value, volume, substitutability, interconnectedness, critical users and disruption impact.
2. The operator shall receive notice, evidence, opportunity to respond and a reasoned decision.
3. A designated system shall comply with enhanced governance, financial, operational, recovery and disclosure standards consistent with applicable international principles.
4. Designation shall be reviewed at least every two years and may be removed when criteria no longer apply.

Article 16 — Public register

1. The Bank shall maintain a free searchable register of systems, operators, providers, electronic-money issuers, agents and licence status.

2. The register shall identify authorized services and material restrictions and support reliable electronic verification.
3. Historical status shall be preserved and a pending application shall not appear as licensed.
4. Protected personal and security information shall not be published unnecessarily.

Article 17 — Oversight cooperation

1. The Bank shall cooperate with financial, competition, data-protection, communications, cybersecurity, consumer, tax and law-enforcement authorities according to law.
2. A memorandum may allocate operational tasks but shall not create coercive power or override an Assembly Act.
3. Information sharing shall have defined purpose, necessity, security, retention and accountability.
4. Cooperation shall avoid duplicate licensing and contradictory standards.

Article 18 — International cooperation

1. The Bank may cooperate with foreign and regional payment, supervisory and resolution authorities.
2. An arrangement shall protect confidentiality, reciprocity, legality, customer rights and Eritrean financial stability.
3. It shall comply with the Treaty-Making Act and shall not create an unauthorized international obligation.
4. Cross-border cooperation shall support remittances and trade without permitting foreign political surveillance.

CHAPTER III
LICENSING OF OPERATORS AND PROVIDERS

Article 19 — Licence requirement

1. No person shall operate a regulated payment system, provide a payment service or issue electronic money without the required licence or authorization.
2. A bank licensed under the Financial Institutions Act shall obtain or hold the payment authorization appropriate to its service, through a coordinated process without duplicate prudential review.
3. A licence is personal, states authorized services and is not transferable.
4. An agent acts under the provider's licence and does not receive an independent licence unless it also conducts business on its own account.

Article 20 — Licence classes

1. The Bank shall establish published licence classes for system operators, account-servicing providers, remittance providers, merchant acquirers, payment initiators, account-information providers and electronic-money issuers.

2. A combined licence may cover several services where governance and financial safeguards are adequate.
3. A limited licence may impose value, customer, product, geographic or functional limits appropriate to risk.
4. Classification shall not favor banks over competent non-bank providers without a risk basis.

Article 21 — Licence application

1. An application shall identify the legal person, beneficial owners, controllers, directors, managers, proposed services, agents, technology, outsourcing and funding.
2. It shall include governance, safeguarding, risk, cyber, fraud, data, business-continuity, wind-down and customer-protection plans.
3. The Bank shall accept secure electronic applications, publish a checklist and identify missing material once reasonably practicable.
4. An application shall be assessed on substance, not political relationship or ownership nationality.

Article 22 — Legal form and local presence

1. A licensed provider shall be a legal person capable of bearing full responsibility under Eritrean law.
2. The Bank may authorize a foreign branch or require a local subsidiary according to customer funds, supervision, resolution and systemic risk.
3. A provider shall maintain a responsible local contact, accessible records and customer-redress arrangements.
4. A digital-only model is permitted where lawful service, supervision and continuity do not require a retail branch.

Article 23 — Capital and financial resources

1. An applicant shall maintain paid-up, unencumbered and transparent capital proportionate to its services and risk.
2. Customer funds, safeguarded assets and borrowed circular funds do not count as own capital.
3. The Bank shall publish minimums and a method for additional institution-specific capital.
4. A provider that holds no customer funds and presents low risk shall not bear unnecessary bank-level capital.

Article 24 — Fitness and propriety

1. A beneficial owner, significant owner, controller, director and senior manager shall be honest, competent, financially sound and capable of responsible payment-service governance.
2. Assessment shall consider role, evidence, seriousness, recency, rehabilitation and response.

3. Political belief, ethnicity, religion, gender, disability, region or former national-service status is irrelevant.
4. Material change shall be reported and reassessed fairly.

Article 25 — Operational readiness

1. Before launch, the applicant shall demonstrate secure functioning, reconciliation, settlement, safeguarding, customer support, incident response and record integrity.
2. Testing shall cover peak load, outage, compromised credential, erroneous payment, agent failure, cyberattack and recovery.
3. The Bank may authorize controlled pilot operation with limits and disclosure.
4. Pilot status shall not be used to hold customer funds without safeguards.

Article 26 — Licensing decision

1. The Bank shall decide a substantially complete application within one hundred twenty days unless complexity is explained and a final date stated.
2. Approval, condition or refusal shall state material facts, law, risk and review rights.
3. A condition shall address an identified risk and shall not secretly allocate customers, fix prices or protect an incumbent.
4. Silence does not grant a licence, but unreasonable delay is reviewable.

Article 27 — Commencement, lapse and renewal

1. A licensee shall commence within twelve months or another stated period after final readiness approval.
2. A licence continues unless surrendered, revoked or made time-limited for a justified pilot or restricted activity.
3. Administrative renewal shall not interrupt a timely compliant provider.
4. Lapse does not extinguish customer claims, safeguarding, records or investigation.

Article 28 — Material changes

1. Prior approval is required for control change, merger, material new service, significant outsourcing, system-rule change affecting finality or transfer of substantially all business.
2. Ordinary product, price, address or technical updates may proceed by notice unless a published risk threshold requires approval.
3. The Bank shall provide clear thresholds and decision periods.
4. A customer shall receive fair notice of a material contractual change.

Article 29 — Suspension and revocation

1. The Bank may suspend, restrict or revoke a licence for material breach, unsafe operation, misuse of funds, false licensing information, insolvency or persistent failure to remedy.
2. The provider shall receive notice, evidence, response and reasons except where an urgent interim restriction is necessary to prevent loss.

3. An interim restriction shall preserve customer access and settlement as far as safely possible and receive prompt review.
4. Exit shall be coordinated with safeguarding, transfer, wind-down and court remedies.

Article 30 — Voluntary surrender and wind-down

1. A licensee may surrender only after approval of a plan for customer funds, pending payments, claims, records, agents and system connections.
2. Users shall receive reasonable notice and free means to redeem or transfer value.
3. Customer funds shall not be used for wind-down costs.
4. Surrender does not prevent liability or enforcement for earlier conduct.

CHAPTER IV
PAYMENT-SYSTEM GOVERNANCE AND FINALITY

Article 31 — Operator governance

1. An operator shall have transparent governance supporting system safety, efficiency, users, financial stability and public interest.
2. Owners, board, committees, management, conflicts and accountability shall be documented.
3. Major participants shall not control access, pricing or rules to exclude competitors unfairly.
4. A systemically important operator shall include independent and user perspectives appropriate to its role.

Article 32 — System rules

1. An operator shall maintain clear enforceable rules governing participation, payment orders, acceptance, clearing, settlement, default, collateral, fees, disputes and exit.
2. Rules and material amendments require Bank approval or notice according to systemic importance.
3. Participants and users shall have access to applicable rules in understandable form.
4. An unpublished operational instruction shall not alter legal finality or customer rights.

Article 33 — Legal basis

1. A payment system shall have a well-founded, clear and enforceable legal basis for every material aspect in each relevant jurisdiction.
2. The operator shall assess conflict of laws, insolvency, netting, settlement, collateral and electronic-record validity.
3. A material legal uncertainty shall be disclosed to the Bank and addressed before scale increases.
4. Contract shall not override mandatory customer, competition or financial-stability law.

Article 34 — Acceptance of payment order

1. System rules shall state the point at which a payment order is accepted and may no longer be revoked unilaterally.
2. Acceptance shall be determined by objective recorded events and reliable time.
3. A provider shall inform users of cut-off, rejection and pending status relevant to their transaction.
4. A payment entered after cut-off shall be treated according to the next applicable cycle unless a fast-payment rule provides otherwise.

Article 35 — Settlement finality

1. A transfer order, netting result and settlement that has become final under approved system rules is legally enforceable and shall not be unwound solely because a participant later enters insolvency.
2. Finality shall not validate fraud by the protected participant or a transaction not accepted under the rules.
3. The finality point shall be certain, public and no later than the end of the value date absent exceptional arrangement.
4. A court may grant monetary and personal remedies without disturbing system finality where stability and innocent participants require it.

Article 36 — Netting

1. Bilateral and multilateral netting under approved system rules is enforceable according to its terms, including against an insolvent participant.
2. Only claims properly included before the applicable finality or default point receive protection.
3. Netting shall not be used to conceal an unlawful preference, sham transaction or customer-asset misuse.
4. The operator shall calculate, reconcile and retain an auditable net obligation.

Article 37 — Settlement assets

1. A systemically important system shall settle in central-bank money where practical and available.
2. Use of commercial-bank or another settlement asset requires assessment of credit, liquidity, legal and concentration risk.
3. An operator shall disclose the settlement asset and associated material risk.
4. No private settlement asset becomes legal tender by system rule.

Article 38 — Settlement accounts

1. The Bank may provide settlement accounts to eligible regulated participants under objective published criteria.

2. Access may require capital, liquidity, technical, governance and operational readiness appropriate to risk.
3. Denial, restriction and price shall be reasoned, proportionate and reviewable.
4. A settlement account shall not be used for ordinary commercial lending except as authorized by the National Bank Act.

Article 39 — Participant default

1. System rules shall provide tested procedures for participant default, loss allocation, liquidity, collateral, communication and continued service.
2. The operator shall act promptly, consistently and without favoring an owner participant.
3. Loss allocation shall be transparent, contractually grounded and subject to statutory safeguards.
4. The Bank and affected systems shall coordinate where default may spread.

Article 40 — Collateral

1. Collateral pledged to a designated system or the Bank for settlement obligations shall be identifiable, valued, controlled and legally enforceable.
2. Approved realization after participant default is not stayed by insolvency except for fraud or failure of the security interest.
3. Excess collateral shall be returned promptly after obligations are satisfied.
4. Collateral arrangements shall not take customer property without lawful authority.

Article 41 — Liquidity and credit risk

1. An operator shall measure and control participant credit and liquidity exposure in real time or at a frequency appropriate to the system.
2. A systemically important system shall maintain sufficient resources to complete settlement under severe but plausible participant failure.
3. Limits, collateral, prefunding, loss sharing and emergency liquidity shall be transparent and tested.
4. The operator shall not assume discretionary public rescue.

Article 42 — Access and participation

1. Participation criteria shall be objective, risk-based, publicly available and permit fair access by qualified banks and non-bank providers.
2. A restriction shall relate to safety, efficiency, settlement or legal risk and not merely business model or ownership.
3. A participant shall receive reasons and review for denial, suspension or termination.
4. Indirect access shall not be structured to permit discriminatory gatekeeping.

Article 43 — Fees and pricing

1. Operator fees shall be transparent, cost-aware, competitively neutral and approved through governance appropriate to the system.
2. A Bank-operated monopoly infrastructure shall publish costs, methodology and cross-subsidy.
3. Interchange and access fees may be regulated where market failure or exclusion is demonstrated after evidence and consultation.
4. A rule shall not prohibit legitimate discount, surcharge or commercial negotiation unless customer harm or competition requires it.

Article 44 — Recovery and orderly wind-down

1. A systemically important operator shall maintain plans to recover from financial, operational and business stress and to wind down without disrupting critical services.
2. Plans shall identify governance, loss and liquidity tools, replenishment, service continuity, communication and implementation barriers.
3. Tools shall be transparent to participants and shall not allocate unlimited or unknowable liability.
4. The Bank shall review and require remediation and may coordinate a transfer or bridge arrangement under law.

CHAPTER V
PAYMENT SERVICES AND CUSTOMER FUNDS

Article 45 — Payment accounts

1. A licensed provider may open and maintain payment accounts within its authorized class.
2. The account shall state ownership, permitted use, balance status, fees, interest if any, safeguarding and withdrawal rights.
3. A non-bank payment account shall not be represented as a bank deposit.
4. A user shall receive reliable access to balance and transaction history.

Article 46 — Execution of payment order

1. A provider shall execute an authorized payment accurately, securely and within the disclosed time.
2. It shall validate required information and reject or query an order that cannot be executed reliably.
3. The payer shall receive confirmation, amount, fees, exchange, date and reference on a durable medium.
4. A provider shall not delay a payment to obtain undisclosed float or commercial advantage.

Article 47 — Unique identifiers and name check

1. A payment may rely on a prescribed unique identifier, but the provider shall offer reasonable confirmation of payee name or other recipient information where technically feasible.
2. A material mismatch shall generate a clear warning and opportunity to correct or consciously proceed.
3. The system shall protect recipient privacy and shall not expose unnecessary account data.
4. Provider responsibility for error shall reflect the information and warning actually supplied.

Article 48 — Payment initiation

1. A licensed payment-initiation provider may initiate payment from a user's account with explicit authorization.
2. The account-servicing provider shall provide secure nondiscriminatory access through approved interfaces and shall not require disclosure of reusable credentials to an unauthorized person.
3. The initiation provider shall not hold funds unless separately licensed and shall use data only for the requested service.
4. The user shall receive clear confirmation and equivalent refund and complaint protection.

Article 49 — Account-information service

1. A licensed account-information provider may access and consolidate information with the user's explicit consent.
2. Access shall be limited to designated accounts, data and duration and may be withdrawn readily.
3. The provider shall not modify transactions, infer unrelated sensitive traits or sell data without separate lawful basis.
4. A user shall receive access logs and means to report misuse.

Article 50 — Merchant acquiring

1. An acquirer shall contract fairly with merchants, disclose settlement time, fees, reserves, chargebacks, security and termination.
2. Funds shall be settled promptly and shall not be withheld beyond risk reasonably connected to the merchant.
3. A reserve or rolling hold shall be proportionate, recorded and released when risk ends.
4. Dispute rules shall protect both merchant and payer from duplicate recovery.

Article 51 — Money remittance

1. A remittance provider may receive funds for transfer without maintaining a continuing payment account where licensed.

2. The sender shall receive amount, fee, exchange rate, delivery time, collection conditions and cancellation rights before payment.
3. The provider shall trace a delayed transfer and refund promptly where delivery fails.
4. Remittance funds are customer funds and shall be safeguarded from receipt until payout or refund.

Article 52 — Cash services

1. A provider and agent may offer cash-in and cash-out under security, liquidity, receipt and reconciliation controls.
2. Cash conversion to or from electronic value shall ordinarily occur at par except a disclosed reasonable service charge.
3. A user shall not be denied lawful cash solely to force digital adoption.
4. Counterfeit, safety and anti-financial-crime controls shall be proportionate and respectful.

Article 53 — Recurring payments and direct debit

1. A recurring payment or direct-debit mandate shall state payee, amount or calculation, frequency, duration and cancellation method.
2. The payer may withdraw future authorization through an accessible channel without unreasonable fee.
3. A material variable debit shall receive advance notice unless the payer knowingly waives it for a defined transaction class.
4. An unauthorized or incorrectly executed debit is subject to refund and investigation.

Article 54 — Cards, devices and tokenized credentials

1. A provider may issue a physical or virtual card, device credential or token under secure and transparent terms.
2. Tokenization shall not change the underlying user rights, funding source or dispute process.
3. Loss, theft, compromise and replacement channels shall be continuously available for material services.
4. A provider shall not impose liability merely because a device or credential was used.

Article 55 — Safeguarding of customer funds

1. A non-bank provider holding customer funds shall segregate them from its own money in a trust, custodial or equivalent insolvency-protected arrangement.
2. Funds shall be reconciled at least daily, held in safe liquid assets and used only for execution, redemption or lawful charges.
3. The provider and its creditors have no beneficial claim to safeguarded funds.
4. The Bank may prescribe diversification, permitted custodians, insurance, guarantees and audit according to risk.

Article 56 — Safeguarding audit

1. An independent auditor shall verify safeguarding, reconciliation, asset eligibility and customer liabilities at prescribed intervals.
2. A material shortfall or control failure shall be reported immediately to the board and Bank.
3. The provider shall restore a shortfall from its own resources without waiting for fault determination.
4. Audit does not transfer management responsibility.

Article 57 — Treatment on insolvency

1. Safeguarded customer funds do not form part of the provider's free insolvency estate.
2. An administrator or liquidator shall identify, reconcile and return or transfer funds promptly, subject only to necessary administration cost prescribed by law.
3. A shortfall is shared proportionately among affected customers after application of provider capital, guarantee, insurance and responsible-person claims as lawful.
4. The Bank may arrange transfer to a sound provider to preserve access.

CHAPTER VI
ELECTRONIC MONEY

Article 58 — Electronic-money licence

1. No person shall issue electronic money without an electronic-money licence or express authorization under a bank licence.
2. The licence shall state value limits, distribution channels, permitted investments, redemption, safeguarding and interoperability.
3. Electronic money is a claim on the issuer and is not legal tender or a bank deposit merely by issuance.
4. Interest or credit linked to electronic money requires separate lawful authorization.

Article 59 — Issuance at par

1. Electronic money shall be issued only on receipt of funds and at equal nominal value in the same currency.
2. An issuance or cash-conversion fee shall be disclosed separately and shall not disguise a value haircut.
3. The issuer shall record the corresponding safeguarded liability immediately.
4. Credit creation through unfunded electronic-money issuance is prohibited.

Article 60 — Redemption at par

1. A holder may redeem electronic money at par at any time during the contract and for a reasonable period after termination.
2. A fee may reflect a genuine disproportionate redemption cost only when disclosed and permitted by regulation.

3. No minimum balance, political clearance, forced exchange or unrelated debt may prevent redemption.
4. The issuer shall provide cash or account transfer options reasonably available to the user.

Article 61 — Electronic-money reserves

1. The issuer shall maintain safeguarded high-quality liquid assets at least equal to outstanding electronic-money liabilities.
2. Permitted assets, concentration, maturity, currency matching and custodians shall be prescribed conservatively.
3. Investment income belongs to the issuer unless contract states otherwise, but investment loss shall not reduce customer value.
4. Customer reserves shall not secure the issuer’s own borrowing.

Article 62 — Limits and tiered accounts

1. The Bank may prescribe graduated balance and transaction limits based on identity assurance, risk and inclusion.
2. A user may move between tiers through accessible verification and shall receive notice of limits.
3. A limit shall not discriminate unlawfully or require documents unavailable to a genuine low-risk user when reliable alternatives exist.
4. Aggregation across related accounts may prevent evasion while preserving family and business separation.

Article 63 — Agents and distributors

1. An electronic-money issuer may distribute, redeem and service electronic money through registered agents under written authority.
2. The issuer is responsible for agent liquidity, conduct, records, security, training and customer complaints.
3. An agent shall display the issuer, authorized services, fees and complaint channels.
4. An exclusive-agent term that materially restricts competition or access is prohibited unless objectively justified.

Article 64 — Dormant value

1. Electronic value becomes dormant only after a published period without user-initiated activity and reasonable contact attempts.
2. Dormancy shall not permit confiscation, expiry or unreasonable erosion by fees.
3. Unclaimed value shall be transferred to a lawful custodian while preserving the user’s reclaim right.
4. The issuer shall maintain searchable privacy-protective recovery procedures.

Article 65 — Electronic-money failure

1. The Bank shall maintain plans for transfer, redemption and orderly wind-down of a failing issuer.
2. Customer reserves shall be insulated and used first for holders.
3. The issuer’s owners and creditors bear business losses before public resources are considered.
4. Public support requires specific Assembly authority and shall not be implied by licensing.

CHAPTER VII
FAST PAYMENTS, INTEROPERABILITY AND OPEN FINANCE

Article 66 — National fast payment capability

1. The Bank shall facilitate at least one safe, competitive and broadly accessible fast-payment capability for the Nakfa.
2. Qualified banks and non-bank providers shall receive fair direct or indirect access under published criteria.
3. The system shall support person, business and government payments and function across providers.
4. Public investment and procurement shall be transparent and avoid unnecessary proprietary dependence.

Article 67 — Availability and speed

1. A fast-payment system shall provide near-real-time processing and prompt payee availability on a broadly continuous basis.
2. Planned maintenance and service limitations shall be disclosed and designed around essential user needs.
3. A transaction shall show clear pending, completed, rejected or reversed status.
4. Speed shall not remove proportionate fraud, sanctions or error controls.

Article 68 — Interoperability

1. The Bank may require interoperability among payment accounts, electronic-money systems, agents, merchants and infrastructure where it improves access and competition safely.
2. A standard shall be open, secure, governable and available on fair reasonable and nondiscriminatory terms.
3. Interoperability shall preserve provider responsibility, consent, privacy and transaction traceability.
4. A proprietary system may coexist where users can transfer value without unreasonable barrier.

Article 69 — Common identifiers and aliases

1. A system may use telephone number, account number, business identifier or another alias to route payment with user consent.
2. Alias directories shall minimize disclosed data, verify changes and prevent unauthorized reassignment.
3. A user may port, correct or remove an alias without losing the underlying account.
4. No alias directory shall become a general population-surveillance database.

Article 70 — Quick-response and acceptance standards

1. The Bank may recognize common quick-response, near-field or other acceptance standards after consultation.
2. A merchant shall not require multiple proprietary devices where a secure interoperable standard is reasonably available.
3. Fees, routing choice and merchant information shall be transparent.
4. A technical standard shall accommodate basic phones, printed codes and accessibility where practicable.

Article 71 — Open application interfaces

1. An account-servicing provider shall offer secure standardized interfaces for licensed payment-initiation and account-information services where prescribed.
2. Interface performance, authentication and data shall be equivalent to the provider's own comparable channel.
3. Access may be limited for specific documented security risk and shall be reported and reviewable.
4. A provider shall not screen-scrape or require reusable credentials where a safer interface is available.

Article 72 — Consent dashboard

1. A user shall have an accessible dashboard showing active third-party payment and data permissions.
2. Consent may be narrowed or withdrawn prospectively without unreasonable procedure.
3. Withdrawal shall not invalidate a completed payment or lawful record retention.
4. The dashboard shall show access history and a channel to report misuse.

Article 73 — Portability and switching

1. A user may switch payment provider and transfer standing instructions, aliases and available balance through a reasonable standardized process.
2. The former provider shall cooperate securely and shall not impose a punitive exit fee.
3. Portability shall not transfer disputed debt or data beyond the user's authority.
4. The Bank may prescribe switching timeframes and liability.

Article 74 — Competition safeguards

1. An operator or dominant provider shall not tie access, discriminate, self-preference or degrade interoperability to exclude competitors.
2. Technical, risk and security distinctions remain lawful when objective and proportionate.
3. The Bank and Competition Authority shall investigate market-wide barriers and coordinate remedies.
4. A remedy shall preserve system safety and incentives to invest.

CHAPTER VIII
USERS, MERCHANTS AND PAYMENT LIABILITY

Article 75 — Fair treatment and accessibility

1. A provider shall treat users honestly, fairly, respectfully and without unlawful discrimination.
2. Services, instructions and support shall be accessible by principal Eritrean languages and reasonable disability accommodation.
3. A digital service shall provide effective human assistance for material problems.
4. A provider shall not exploit poverty, displacement, low literacy or urgent family remittance.

Article 76 — Pre-contract disclosure

1. Before service, the provider shall disclose identity, licence, functions, fees, exchange, execution time, limits, security, data use, liability, termination and complaints.
2. A concise key-facts statement shall be available on paper or durable electronic medium.
3. Material change requires advance notice and a reasonable right to terminate or reject where feasible.
4. Disclosure shall distinguish electronic money, bank deposit, virtual asset and other value accurately.

Article 77 — Pricing and receipts

1. Every fee, surcharge, commission and exchange spread shall be disclosed before authorization.
2. A user shall receive a receipt showing provider, parties, amount, currency, rate, charges, time, status and reference.
3. A provider shall not impose a hidden receiving fee or deduct value after the stated amount without authority.
4. Standard price information shall be comparable and publicly available.

Article 78 — Authorization

1. A payment is authorized only when the payer consents through the agreed reliable procedure.

2. Consent may be transaction-specific or cover a defined series and may be withdrawn prospectively.
3. Silence, possession of a device, family relationship or government instruction does not alone establish authorization.
4. The provider bears the burden of showing authentication and technically correct recording, without making authentication conclusive of consent.

Article 79 — Strong customer authentication

1. A provider shall use authentication proportionate to transaction, channel, device, behavior and fraud risk.
2. Higher-risk remote action shall ordinarily use independent factors or equivalent protection.
3. Accessible alternatives shall exist for a person unable to use a biometric, smartphone or particular credential.
4. Authentication data shall be protected and shall not be reused for unrelated surveillance.

Article 80 — Unauthorized payment liability

1. A provider shall refund an unauthorized payment promptly after notice unless it has reasonable evidence of user fraud.
2. A user may bear a limited amount for loss before notice caused by negligent credential protection, as prescribed, but not where the provider failed required security.
3. Gross negligence requires more than ordinary mistake and shall be proved by the provider.
4. A vulnerable user deceived by sophisticated impersonation shall receive an individualized fair assessment.

Article 81 — Incorrect or delayed execution

1. A provider responsible for incorrect, duplicate or delayed execution shall trace, correct, restore value and refund resulting charges promptly.
2. Liability among providers may be allocated by system rules without reducing the user's direct remedy.
3. The user shall cooperate with reasonable information needed to locate the payment.
4. Consequential loss is governed by the Civil Code and applicable limitation and causation rules.

Article 82 — Mistaken payment

1. A user who sends a payment to an unintended recipient may request immediate recovery assistance.
2. Providers shall notify the recipient, preserve disputed value where lawful and facilitate consent or court-ordered return.
3. The provider shall not reverse a final payment unilaterally merely on an unsupported allegation.
4. Unjust enrichment and ownership are determined under the Civil Code with expedited access to necessary identity through lawful process.

Article 83 — Fraud and scam response

1. Providers and operators shall share timely fraud indicators, confirmation tools and recovery requests under privacy and competition safeguards.
2. A credible urgent report shall trigger prompt hold or trace where lawful and operationally possible.
3. Liability shall consider provider controls, warnings, conduct, authorization and each party's contribution rather than assigning every loss automatically to the user.
4. Aggregate scam data and prevention outcomes shall be published.

Article 84 — Complaints

1. A provider shall maintain free, accessible and time-bound complaint channels with trained staff and secure evidence.
2. It shall acknowledge, investigate, explain, remedy and inform the user of external review.
3. An urgent complaint involving inaccessible livelihood funds, fraud or identity compromise shall receive accelerated handling.
4. Internal complaint use shall not bar court, Ombud or regulatory relief.

Article 85 — Payment dispute resolution

1. A Financial Services Ombud or other independent body established by law may determine eligible payment disputes and order correction, refund, interest and modest compensation.
2. The procedure shall be simple, inexpensive, fair and available electronically and in person.
3. A provider shall participate and preserve records.
4. Systemic issues shall be referred to the Bank without exposing protected complainant information.

Article 86 — Merchant rights and duties

1. A merchant shall disclose accepted payment methods and any lawful surcharge before purchase.
2. It shall protect payment credentials, give receipts and cooperate with valid disputes without retaining unnecessary data.
3. A provider shall not impose a rule preventing lawful price transparency or customer choice except to protect security and fair competition.
4. Small merchants shall receive proportionate onboarding, equipment and settlement terms.

Article 87 — Cash acceptance and choice

1. Cash remains a lawful and generally available means of payment according to the National Bank Act.
2. A government office providing an essential service shall maintain a reasonable nondigital payment option unless an Assembly Act provides an accessible equivalent.

3. A private merchant may choose payment methods subject to advance notice, competition and nondiscrimination law.
4. The Bank shall monitor cash access and may require essential withdrawal and deposit arrangements where market withdrawal creates serious exclusion.

CHAPTER IX
AGENTS, IDENTITY AND INCLUSIVE DELIVERY

Article 88 — Agent authorization

1. A provider may appoint an agent under written agreement and registration with the Bank or approved central register.
2. The agreement shall state services, limits, liquidity, records, security, fees, training, complaints and termination.
3. The provider remains responsible to the user for the agent's authorized conduct.
4. An agent shall not subcontract without authorization and equivalent oversight.

Article 89 — Agent transparency

1. An agent shall display the provider, registration status, authorized services, official fees and complaint channels.
2. It shall issue a verifiable receipt and shall not charge an undisclosed amount.
3. Customer funds shall be handled only through approved accounts and reconciliation.
4. A user may verify an agent through free digital or nondigital means.

Article 90 — Agent liquidity and conduct

1. A provider shall monitor agent cash and electronic liquidity and support safe predictable service.
2. An agent shall not retain identity documents, compel purchases, discriminate or misuse customer information.
3. Fraud, shortage and misconduct shall be investigated and remedied promptly.
4. Termination shall protect pending customer claims and public notice.

Article 91 — Digital identification

1. A provider may rely on a lawful national, private, community-assisted or foreign identity method that provides appropriate assurance.
2. The Bank shall coordinate tiered and interoperable identification standards with competent identity and data authorities.
3. Lack of a conventional street address or paper document shall not automatically exclude a genuine low-risk person where reliable alternatives exist.
4. Identity data shall not be repurposed for political control or unrelated surveillance.

Article 92 — Remote onboarding

1. A provider may onboard a customer remotely using document, database, video, biometric, trusted-agent or other reliable verification.
2. Controls shall assess impersonation, synthetic identity, coercion and exclusion risk.
3. The customer shall know what data are collected and receive a channel to correct error.
4. A higher-risk service may require stronger verification without making physical presence the default.

Article 93 — Simplified due diligence

1. Low-risk, low-value services may use simplified customer due diligence under anti-money-laundering law.
2. Limits shall address balance, transaction, geography and functionality and shall be reviewed against actual risk.
3. Simplification shall not permit anonymous high-risk use or bulk structuring.
4. Financial inclusion and financial integrity shall be treated as mutually supporting.

Article 94 — Pastoral and mobile users

1. A provider shall accommodate lawful mobile residence, seasonal movement and shared community infrastructure where identity and communication can be managed reliably.
2. An account shall not be closed solely because the customer moves between villages, provinces or across ordinary grazing routes.
3. Offline and agent-assisted services shall be developed with community consultation and safeguards against gatekeeper abuse.
4. Geolocation shall not be continuously collected without necessity and consent or other lawful basis.

Article 95 — Persons abroad and diaspora

1. An Eritrean abroad may open and operate an account remotely subject to lawful risk-based verification and tax and foreign-exchange law.
2. A provider may recognize reputable foreign identity, address, bank and digital-signature evidence.
3. Diaspora status shall not justify a punitive exchange rate, compulsory contribution or discriminatory service fee.
4. Cross-border data and dispute arrangements shall preserve effective Eritrean remedies.

Article 96 — Offline payments

1. A provider may offer limited offline payment where value, duration, device, reconciliation and double-spend risks are controlled.
2. The user shall know when payment is provisional or final and the consequences of delayed synchronization.
3. Loss allocation shall be fair and reflect provider design and user conduct.

4. Offline capability shall support resilience and inclusion without creating untraceable high-risk value.

CHAPTER X
DATA, TECHNOLOGY AND OPERATIONAL RESILIENCE

Article 97 — Payment-data governance

1. A provider and operator shall collect, use, retain and share payment data only under the Data Protection and Privacy Act and this Act.
2. Purpose, access, accuracy, minimization, retention, security and accountability shall be documented.
3. Transaction data shall not be sold, used for political profiling or disclosed to an unrelated official without lawful authority.
4. A user shall receive access, correction and complaint rights subject to lawful financial records.

Article 98 — Data localization and cross-border processing

1. Payment data may be processed outside Eritrea where the provider ensures equivalent security, access, continuity and legal protection.
2. The Bank shall retain timely lawful supervisory access without requiring unnecessary duplication.
3. Localization may be required only for a demonstrated necessary and proportionate financial-stability, security or legal-enforcement purpose.
4. A cross-border processor shall not expose Eritrean users to foreign political surveillance or inaccessible remedy.

Article 99 — Cybersecurity programme

1. A provider and operator shall maintain board-approved cybersecurity governance, secure architecture, identity control, encryption, monitoring, testing and response.
2. Critical systems shall follow secure development, patch, vulnerability and privileged-access controls.
3. Independent assessment shall occur according to risk and after a major incident.
4. Security shall include people, agents, vendors, physical facilities and social engineering.

Article 100 — Operational resilience

1. Critical payment service shall have defined impact tolerance, redundancy, backup, recovery and alternative communication.
2. Plans shall address electricity failure, telecommunications disruption, cyberattack, natural disaster, conflict spillover and key-provider failure.
3. A systemically important operator shall aim for rapid recovery appropriate to continuous settlement and test with participants.
4. A provider shall not conceal repeated outage through manual record alteration.

Article 101 — Incident notification

1. A material operational, cyber, fraud, data or safeguarding incident shall be reported promptly to the Bank and other competent authority.
2. Affected users shall receive timely useful notice where action is needed or harm is likely, subject to security.
3. The report shall state impact, services, funds, data, response and recovery and shall be updated materially.
4. Good-faith timely notification is considered in enforcement but does not remove remedy obligations.

Article 102 — Outsourcing and critical providers

1. A licensee remains responsible for outsourced payment, cloud, telecommunications, identity, data and support functions.
2. Material outsourcing requires due diligence, contract, audit, security, continuity, subcontracting and exit rights.
3. The Bank may assess a critical service provider and coordinate with other authorities.
4. An outsourcing arrangement shall not prevent supervision, resolution, switching or user access.

Article 103 — Artificial intelligence and automation

1. A material automated system shall have documented purpose, data lineage, testing, validation, monitoring, explainability and accountable human ownership.
2. The provider shall assess bias, exclusion, fraud manipulation, hallucination, drift, cyber risk and operational dependency.
3. No system may make an unreviewable final decision on account access, transaction freeze, fraud liability or complaint remedy.
4. The Bank may require independent testing and correction while protecting lawful intellectual property.

Article 104 — Biometric technology

1. Biometric use shall be necessary, proportionate, accurate, secure and accompanied by a reasonable alternative.
2. A provider shall test demographic performance and presentation-attack risk and shall not infer unrelated traits.
3. Raw biometric templates shall receive enhanced protection and shall not be centralized without necessity.
4. Failure or disability shall not deprive a user of funds or essential service.

Article 105 — Records and audit trails

1. A provider and operator shall keep complete, accurate, tamper-evident records sufficient to reconstruct payment, authorization, routing, settlement, fees and access.
2. Records may be electronic and shall remain accessible through migration, outage, insolvency and resolution.
3. Retention shall satisfy applicable commercial, tax, anti-financial-crime, data and limitation law.
4. A correction shall preserve the original, reason, authority and time.

Article 106 — Electronic evidence

1. A payment record, message, signature, authentication and system log shall not be denied legal effect solely because it is electronic.
2. Reliability is assessed by integrity, identity, time, security, process, accessibility and other evidence.
3. A system-generated record is not conclusive where credible evidence shows error, compromise or lack of consent.
4. Courts and tribunals may require intelligible presentation and independent technical evidence.

CHAPTER XI
GOVERNMENT PAYMENTS AND PUBLIC INFRASTRUCTURE

Article 107 — Government payment principles

1. Government shall use payment arrangements that are lawful, transparent, efficient, inclusive, competitive and auditable.
2. A person shall not be compelled to open an account with a politically selected institution to receive an entitlement or pay a public obligation where reasonable alternatives exist.
3. Fees, procurement, data use and service standards shall be published.
4. Digitization shall not delay benefit, salary, refund or supplier payment.

Article 108 — Public revenue collection

1. A public body may accept tax, customs, fee and other lawful revenue through approved payment providers and cash channels.
2. The payer shall receive an official verifiable receipt and payment shall discharge the obligation at the legally defined time.
3. A provider shall transfer public funds promptly to the Treasury Single Account or other lawful account.
4. Revenue data shall be reconciled and auditable without granting the provider tax-enforcement power.

Article 109 — Public disbursements

1. Salary, pension, social benefit, procurement and other public payment may be made electronically with recipient choice among reasonably available providers.
2. The recipient shall not bear an undisclosed fee or forced currency conversion.
3. A person without digital access shall receive assisted or cash alternative without stigma.
4. Payment lists and identity systems shall prevent fraud while protecting privacy and appeal.

Article 110 — Treasury and central-bank infrastructure

1. The Treasury and Bank shall connect public accounts to reliable settlement, reporting and reconciliation systems under the Public Finance Management Act.
2. Access control shall separate authorization, execution, custody, accounting and audit.
3. A public payment shall identify appropriation, authority, beneficiary, amount and status.
4. No secret off-system account or political payment channel is authorized.

Article 111 — Procurement and public technology

1. Public payment infrastructure shall be procured under the Public Procurement Act with transparent requirements, interoperability, cybersecurity, data protection and exit rights.
2. Vendor lock-in, undisclosed beneficial ownership, political commission and unreviewable proprietary control shall be avoided.
3. Open standards and reusable public components shall be preferred where they provide value and security.
4. Source-code, escrow, documentation and continuity rights shall be proportionate to criticality.

Article 112 — Public digital currency

1. The Bank may research and pilot a central-bank digital form of the Nakfa within powers enacted by the National Bank Act and this Act.
2. General public issuance requires published design, legal basis, privacy, financial-stability, access, cybersecurity and fiscal assessment and any further Assembly authorization required by law.
3. A design shall preserve reasonable cash access and shall not permit routine political tracking of lawful transactions.
4. Programmability shall not allow an executive body to restrict lawful use of private money without specific legislative authority.

CHAPTER XII
CROSS-BORDER PAYMENTS, REMITTANCES AND DIGITAL ASSETS

Article 113 — Cross-border payment services

1. A provider may offer cross-border payment under its licence, foreign-exchange authorization and applicable anti-financial-crime law.

2. The user shall receive sending amount, receiving amount, rate, spread, fees, route, time and complaint rights before authorization.
3. The provider remains responsible for its correspondent and agent arrangements to the extent of law and contract.
4. A foreign-law term shall not eliminate mandatory Eritrean user protection.

Article 114 — Remittance competition and access

1. Banks, non-bank providers, post offices, cooperatives and technology firms may compete in remittances when licensed and safe.
2. Access to settlement, foreign exchange, identification and agent infrastructure shall be fair and risk-based.
3. An exclusivity arrangement that closes a material corridor or community to competitors is prohibited unless objectively necessary.
4. The Bank shall publish corridor cost, speed and failure data.

Article 115 — Foreign-exchange treatment

1. Cross-border payment and electronic conversion shall use transparent market-consistent exchange under the National Bank Act.
2. No provider or public body shall confiscate value through compulsory conversion at an artificial rate.
3. A customer may hold and transfer foreign currency subject only to published, necessary and proportionate law.
4. Exchange error and unauthorized conversion require restoration of equivalent value.

Article 116 — International standards and messaging

1. The Bank may adopt interoperable messaging, identification and compliance standards facilitating regional and global payments.
2. A standard shall be open on fair terms and shall protect data minimization and security.
3. Migration shall be planned, tested and accessible to smaller providers.
4. Adoption shall not surrender legislative authority or make a private standard automatically binding law.

Article 117 — Virtual assets and payment use

1. A virtual asset is not legal tender, a deposit or electronic money merely because persons use it for payment.
2. A person providing exchange, transfer, custody or payment service involving virtual assets as a business shall obtain authorization under legislation or a regulatory framework issued under express Assembly delegation.
3. Marketing shall disclose volatility, custody, technology, legal, fraud and guarantee risks and shall not imply state backing.
4. Anti-financial-crime, consumer, tax, data and sanctions law applies according to function and risk.

Article 118 — Asset-referenced and stable-value arrangements

1. An arrangement representing stable value in Nakfa or foreign currency shall not be offered widely for payment without Bank authorization.
2. The issuer shall disclose legal claim, reserve assets, redemption, governance, technology and stabilization method.
3. A claim of one-to-one backing requires segregated high-quality reserves, independent assurance and redemption at stated value.
4. Designation as systemically important may subject the arrangement to payment-system standards.

Article 119 — Regulatory sandbox

1. The Bank may operate a transparent regulatory sandbox for limited testing of innovative payment and digital-finance services.
2. Admission shall use published criteria, time, customer limits, safeguards, disclosures, reporting and exit.
3. A sandbox does not waive criminal, safeguarding, privacy or fundamental consumer law.
4. Results and lessons shall be published in aggregate and successful participants receive no automatic licence or monopoly.

CHAPTER XIII
SUPERVISION, ENFORCEMENT AND FINAL PROVISIONS

Article 120 — Risk-based oversight

1. The Bank shall supervise according to funds held, transaction scale, operational dependence, conduct, interconnectedness and systemic impact.
2. It may use reporting, inspection, system access, testing, thematic review and supervisory technology under lawful safeguards.
3. A demand shall identify authority, purpose, scope, security and time and avoid needless duplication.
4. Oversight shall not grant access to unrelated private communication or political activity.

Article 121 — Inspection

1. An authorized examiner may inspect business premises, systems, records, safeguarding, agents and controls at a reasonable time.
2. A private home or unrelated device requires consent or court authority unless another Act expressly provides.
3. The examiner shall identify authority, protect confidentiality and avoid unnecessary disruption.
4. Material findings shall be provided for response and correction.

Article 122 — Corrective measures

1. The Bank may require a remediation plan, customer refund, safeguarding restoration, risk reduction, governance change, service restriction, transfer or orderly wind-down.
2. A measure shall state facts, authority, outcome, deadline and review and shall be proportionate to risk.
3. Urgent interim action may preserve customer funds or critical service and shall receive prompt independent review.
4. A measure shall not create a tax, criminal offence or confiscation beyond Assembly authority.

Article 123 — Administrative monetary penalty

1. The Bank may impose an administrative monetary penalty only where an Assembly Act defines the breach and liable person and enacts the applicable maximum.
2. The amount shall reflect harm, funds, duration, benefit, intent, cooperation, remediation, history and provider resources within Assembly-enacted maximums.
3. A penalty shall not be passed directly to affected users through a special charge.
4. No monetary penalty may be imposed until those statutory elements are in force; refund, compensation and criminal process remain available while double punishment is avoided.

Article 124 — Publication and review

1. A final material licensing, corrective or penalty decision shall be published with law, facts, outcome and reasons.
2. Redaction or delay is permitted only for compelling stability, security, investigation or privacy need.
3. A directly affected person may seek internal reconsideration and judicial review.
4. A court may grant suspension, correction, restoration, compensation and another effective remedy while preserving necessary finality and stability.

Article 125 — Unauthorized payment business offence

1. A person who intentionally operates a regulated payment system, holds customer funds or issues electronic money without required authorization commits a Class 8 serious offence under the Penal Code.
2. An employee performing a minor role without knowledge or control is not guilty merely by association.
3. A court may order preservation, restitution, disqualification and transfer of customer funds in addition to authorized sentence.
4. The Bank may seek immediate civil protection without awaiting conviction.

Article 126 — Misuse of safeguarded funds

1. A responsible person who intentionally uses safeguarded customer funds for the provider's own purpose commits a Class 7 serious offence under the Penal Code.

2. A temporary operational reconciliation error corrected promptly without dishonesty is not the offence but remains subject to remediation.
3. Restitution and tracing have priority over a fine.
4. Liability of the institution and natural person shall be determined separately.

Article 127 — False information, obstruction and retaliation

1. A person who knowingly submits materially false regulatory information, destroys a critical record or retaliates causing substantial harm to a protected reporter commits a Class 9 serious offence under the Penal Code.
2. Intentional obstruction without substantial harm is a Class 1 petty offence.
3. Peaceful legal challenge, correction, privilege claim and request for authority are not obstruction.
4. Employment, civil and constitutional remedies remain available.

Article 128 — Power to make regulations

1. The Bank may issue published regulations and technical standards necessary to administer this Act within authority delegated by the National Assembly.
2. Regulations may govern licensing, safeguarding, system rules, finality, interoperability, security, reporting, customer protection, digital assets and transition consistent with this Act.
3. A regulation shall not create a criminal offence, tax, appropriation, legal tender, forced currency conversion, general surveillance power or contradiction of an Assembly Act.
4. A material draft shall receive public consultation and a statement of authority, evidence, impact and proportionality.

Article 129 — Emergency standard

1. The Bank may issue an immediately effective temporary technical or protective standard where delay creates serious imminent threat to funds or system stability.
2. It shall publish authority, reason, scope and expiry as soon as compatible with protection.
3. Consultation shall follow and the standard expires after ninety days unless remade ordinarily.
4. Emergency power shall not authorize permanent shutdown, confiscation, censorship or public expenditure.

Article 130 — Guidance and technical specifications

1. The Bank may publish non-binding guidance and binding technical specifications within a regulation’s express scope.
2. Guidance shall be distinguished from law and permit an equivalent safe approach.
3. A technical specification shall address implementation and shall not change substantive rights or licence scope.
4. All generally applicable material shall be free, searchable and version-controlled.

Article 131 — Existing systems and providers

1. A person lawfully operating at commencement may continue temporarily subject immediately to safeguarding, user and integrity provisions.
2. The person shall register within ninety days and apply for the appropriate licence within twelve months.
3. The Bank shall classify legacy services transparently and provide proportionate remediation or exit periods.
4. Transition shall not validate unauthorized use of customer funds or forced exchange.

Article 132 — Existing contracts and value

1. A valid payment account, instrument, electronic value, merchant contract, mandate and pending payment continues notwithstanding transition.
2. A provider shall not use the new law to cancel value, impose a retroactive fee or compel conversion.
3. A term inconsistent with a mandatory protection is adjusted only to the necessary extent.
4. Pending complaints and claims continue under fair competent procedure.

Article 133 — Consequential amendment and repeal

1. A provision of Financial Institutions Proclamation 94/1997 governing payment services ceases to apply when this Act and the Financial Institutions Act commence.
2. A legacy directive or circular continues only to the extent consistent with this Act and until replaced lawfully.
3. An unpublished restriction, political payment instruction, forced exchange requirement or anticompetitive privilege has no continuing effect.
4. The Statute Law Revision, Repeals and Transitional Continuity Act shall identify technical consequential amendments without reviving superseded authority.

Article 134 — Periodic review

1. The National Assembly shall review this Act within three years after commencement and at least every five years thereafter.
2. Review shall examine access, cost, competition, cash, fraud, privacy, resilience, remittances, artificial intelligence, digital assets and public infrastructure.
3. The Bank shall provide public data and recommendations without exposing protected information.
4. Users, merchants, providers, workers, diaspora, rural and pastoral communities and independent experts shall have meaningful participation.

Article 135 — Commencement

1. This Act enters into force ninety days after publication in the Gazette except for protections made immediately applicable by an Assembly commencement schedule.

2. The Bank shall publish registration, licensing, safeguarding and system-transition timetables within thirty days after publication.
3. Safeguarding, redemption, transparent exchange, privacy, record access and complaint duties capable of direct application take effect immediately.
4. No delay in regulation, technology, appointment or budget postpones a direct right or protection.

Made at Asmara, this ___ day of __________ 2026.

THE NATIONAL ASSEMBLY OF ERITREA