

PUBLIC OFFER AGREEMENT

FOR THE ISSUANCE AND SERVICING OF ELECTRONIC MONEY IN THE "MONET" SYSTEM

This document constitutes an official public offer (Public Contract) of the Payment System Operator – "MePay" LLC – addressed to capable natural persons, individual entrepreneurs, and legal entities, to enter into an agreement on the terms and conditions established herein, the System Rules, and the applicable legislation of the Republic of Armenia.

■ 1. DEFINITIONS AND CORE CONCEPTS USED IN THE AGREEMENT

1.1. Public Offer Agreement (Public Agreement) – the agreement concluded between the System Operator and the User governing the opening and top-up of the Accounting Account for the issuance and servicing of electronic money through the System, as well as the execution of electronic money settlements for services rendered within the System.

1.2. "Monet" Electronic Money – monetary value accounted for in the operating system and via specialized software on a computer or other electronic device based on the "Monet" computer system. Such value is represented as pre-acquired virtual/network funds (prepaid electronic value), hereinafter referred to as "Monet units", entitling the User to make payments for services in the System, execute redemptions, conversions (including via converters), and transfers in accordance with this Public Agreement and the System Rules.

1.3. General-Purpose Electronic Money (Electronic Money) – monetary value (prepaid electronic value) stored on a microprocessor (chip) or within the centralized database of the "Monet" Internet Payment System (IPS), which supports subsequent replenishment (balance increase).

1.4. User – a legally capable natural person who has attained at least 16 (sixteen) years of age under the laws of the Republic of Armenia, a legal entity, or an individual entrepreneur that has entered into this Public Agreement with the System Operator to acquire electronic money and execute settlements for services using electronic money under the terms and rules established by the Operator.

1.5. System or "Monet" IPS (Internet Payment System "Monet") – the settlement system in "Monet" units, comprising the "Monet" IPS, Users, Service Providers, Distributors, and/or Agents (hereinafter collectively the "Participants"), as well as the rules, hardware-software complex, and technological processes that ensure the issuance and servicing of electronic money.

1.6. System Operator – "MePay" Limited Liability Company (state registration number: 264.110.1122587, Taxpayer Identification Number [TIN]: 00219684), responsible for the operations of "Monet" IPS and serving as the operator of the mutual settlement system in "Monet" units.

1.7. Service Provider (Merchant) – a legal entity or individual entrepreneur that has entered into an agreement with the System Operator to accept electronic money issued by the Operator from Users as a means of payment for sold goods, performed works, rendered services, and/or civil or administrative transactions under the System Rules.

1.8. Agent – a financial institution distinct from the System Operator that, pursuant to an agreement with the Operator, executes the redemption or top-up of electronic money in accordance with the System Rules.

1.9. Financial Institution – an entity licensed to perform money (remittance) transfers, a bank operating within the territory of the Republic of Armenia, or a branch of a foreign bank established in Armenia.

1.10. System Rules – the aggregate of rules, procedures, and standards governing settlements and mutual interaction among Participants during the servicing and use of electronic money.

1.11. Accounting Account ("Monet" ID) – a unique identification number and virtual account opened in the name of the User or Service Provider within the centralized database of the System Operator, maintained and managed by the Operator, on which "Monet" units are credited and accounted for.

1.12. User Registration – the technical and legal onboarding procedure of creating an Accounting Account in the System in the User's name.

1.13. Top-Up of Accounting Account – the operation allowing the User, against non-cash payment (including via linked bank cards [vPOS], the unified ArCa processing system, partner banks/payment systems, or payment terminals) or through conversion of electronic money of third-party systems, to acquire electronic value in "Monet" units against equivalent funds and credit the Accounting Account.

■ 1. DEFINITIONS AND CORE CONCEPTS (CONTINUED)

1.14. Servicing of Electronic Money — ensuring the settlement process among Participants during electronic money transactions, whereby the User is enabled to pay for services of Service Providers, execute transfers to other persons, and, where provided by the Agreement, top up the Accounting Account and convert third-party electronic money.

1.15. Redemption of Electronic Money — an operation whereby the equivalent monetary amount is paid to the User or a designated recipient by transfer to a bank account and/or payment card (including instant payouts via the ArCa Pay system), or whereby electronic money is converted into other electronic money.

1.16. Password — a confidential combination of characters created by the User consisting of at least 8 (eight) characters (strictly containing at least one uppercase Latin letter, one lowercase Latin letter, one digit, and one special character), utilized by the System as the primary authentication credential.

1.17. PIN Code — a personal 6 (six) digit security code created by the User, recognized by the System as the User's simple electronic signature, utilized to authenticate payments, remittances, and other financial operations, as well as to modify passwords and personal profile data.

1.18. Mobile Phone Verification Code (SMS OTP) — a one-time numeric code transmitted by the Operator via SMS to the Armenian mobile operator phone number (+374) entered by the User to verify phone number ownership.

1.18.1. Email Verification Code (Email OTP) — a one-time alphanumeric code transmitted by the Operator to the email address specified by the User to verify its validity and ownership.

1.19. Customer Agreement — an agreement or contract entered into between the User and a Service Provider.

1.20. Customer / Subscriber Account — the unique personal account of the User in the information system of a Service Provider.

1.21. Remittance and Transfers — the transfer and payout of funds expressed in "Monet" units or linked payment cards upon the User's order to a Recipient designated by the User under the System Rules. Transfer types include:

- **1.21.1. Monet P2P Transfers:** between Users by Monet ID, mobile phone number, or QR code;
- **1.21.2. ArCa Pay Transfers:** between Armenian banks participating in the unified processing system of "Armenian Card" CJSC by phone number;
- **1.21.3. Transfers to Armenian Bank Cards and Bank Accounts;**
- **1.21.4. International Top-Ups and Transfers** (including via partner remittance systems).

Mandatory transfer parameters comprise the unique transaction identification code, the Idempotency Key, the transfer amount in units, and the identity details of the User and Recipient.

1.22. Recipient — a natural or legal person designated by the User's order as the beneficiary of a remittance or transfer.

1.23. Service Point — a dedicated physical or electronic location for servicing operations (Operator branches, financial institution branches, ATMs, self-service kiosks, etc.).

1.24. Official Website of the Operator — the Internet domain located at www.mepay.am. The Operator bears sole responsibility for information published thereon, which carries official legal force.

1.25. Commission Fee — the remuneration charged to Users in accordance with the tariffs published on the Operator's website and in the Mobile Wallet.

1.26. Payment — the fulfillment by the User of a monetary obligation; an operation executed by the Operator based on the User's payment order debiting the Accounting Account.

1.27. Payment Acceptance — the moment of debiting funds from the User's account and generating the corresponding electronic settlement document.

1.28. Payment Execution — the moment of actual receipt of funds or electronic settlement registers by the payment destination.

1.29. Mobile Wallet (Monet Wallet) — the mobile software application developed for smart devices (iOS, Android) through which the Operator provides remote services to Users.

1.30. Monet ID Account Statuses — the technical and legal modes of accounts set forth in Annex No. 2 to this Agreement.

1.31. User Statuses in the System — the identification tiers and profiles set forth in Annex No. 3 to this Agreement.

1.32. Data Recovery Procedure — the procedure for restoring access in the event of lost Passwords/PIN codes or changes of phone numbers.

1.33. Qualified Assignee — an authorized third party holding all requisite licenses and permissions to deliver the services offered by the Operator.

1.34. Completed Transaction — a transaction where the obligation to transfer funds under the User's order has been fully finalized.

1.35. Uncompleted Transaction — a transaction whose execution has not been finalized by the Operator.

■ 2. SUBJECT MATTER OF THE AGREEMENT

2.1. Under this Public Agreement, the System Operator undertakes, upon the User's order and through the User's Accounting Account, to execute electronic money payments, redemptions, conversions (including via converters), and electronic money transfers in connections between the User and Service Providers, while the User undertakes to accept properly rendered services pursuant to the "Procedure on the Application of Limits on Electronic Money Transactions".

2.2. The catalog of services available through "Monet" IPS is accessible on the Operator's official website and in the Mobile Wallet.

2.3. All money transfers within the System are executed strictly within the limits of the positive balance of the User's Accounting Account or linked payment cards. The transaction amount, including commission fees, shall not exceed the available balance. For an identified User, the general system transaction limit is **AMD 2,000,000 (two million Armenian Drams)**, and the single-transaction limit for ArCa Pay transfers ranges from **AMD 1,000 to AMD 400,000**.

2.4. Payment Card Binding and Ownership Verification:

1. To access full payment and settlement functionality, the User may link an active bank card of Armenian or international payment systems (ArCa, Visa, MasterCard) to the Account.
2. The linked card must be issued *strictly in the name of the User*. The System automatically matches the cardholder's first name, last name, and Public Services Number (PSN/SSN, where available) against the verified identity data of the User. Binding third-party cards is strictly prohibited and automatically rejected.
3. For card verification and ownership validation, a zero-cost test pre-authorization may be initiated via the vPOS processing engine, which is immediately canceled by the System without incurring any fees or charges.
4. Upon successful card linking and verification, the User's account is assigned the status **PaymentVerified**.
5. If the User removes their last linked bank card, the account status reverts from PaymentVerified to **DocumentVerified**. Passport verification remains intact, and full payment capabilities resume upon linking a new valid card.

2.5. 1 (one) "Monet" unit is equivalent to 1 (one) Armenian Dram (AMD).

2.6. Self-Service Blocking (Stop Services) and Unblocking Procedure:

1. For financial self-protection or fraud defense, the User has the right at any time via the Mobile Wallet to independently block individual service categories or all services simultaneously: Money Transfers, Bank Card Operations, Credit Services, Utility Payments, Telecom Services, and Top-Up.
2. **Security Cooldown Period:** To safeguard the User against social engineering, coercion, or theft, submitting a remote unblocking request activates an administrative security verification period of **up to 24 (twenty-four) hours**. During this timeframe, services remain in the pending state (**UnblockPending**) while safety verifications are conducted.
3. Upon expiration of the Cooldown Period and confirmation by the Operator, the services are fully reactivated (**Unblocked**).
4. The User reserves the right to undergo accelerated in-person unblocking by presenting a valid identity document at the Operator's office.

2.7. Duplicate Transaction Elimination Guarantee (Idempotency): All financial API requests are accompanied by a unique **Idempotency Key**. If a duplicate request enters the System due to network drops or multiple clicks, the System does not perform a secondary debit, but returns the cached result of the original transaction.

■ 3. CONCLUSION AND EXECUTION OF THE AGREEMENT

3.1. A prerequisite for concluding this Public Agreement is User registration in the System and receipt of a Monet ID. The Agreement is deemed entered into in electronic form from the moment the Monet ID is generated.

3.1.1. During registration via the Mobile Wallet, the User enters an Armenian mobile operator phone number (+374), email address, completes verification via SMS OTP and Email OTP, enters identity document details (RA Passport or ID Card) for real-time online verification against the State Population Register of Armenia (EKENG / Migration and Citizenship Service of the MIA RA), uploads document photographs (KYC), and creates a compliant Password and 6-digit PIN code.

3.2. By entering into this Public Agreement, the User confirms full awareness, acceptance, and understanding of the System Rules, warrants that service utilization is in their legitimate interest, does not infringe third-party rights, and will cause no detriment to any party.

3.3. The Operator reserves the right to amend the provisions of this Public Agreement unilaterally by publishing a notification on its official website at least 1 (one) day prior to the effective date. In such case, the User may terminate the Agreement unilaterally. Continued use of the System constitutes unconditional acceptance of the amendments.

3.4. The User is obligated to undergo mandatory identification under Annex No. 3.

3.5. By becoming a customer of partner financial institutions, the User obtains remote banking capabilities (online/mobile banking) to open/manage deposit and savings accounts, apply for and manage loans, grant data processing consent, and provide ACRA credit bureau inquiry consent.

■ 4. RIGHTS AND OBLIGATIONS OF THE SYSTEM OPERATOR

4.1. The System Operator undertakes to:

- 4.1.1. Ensure the User's unhindered and continuous access to and utilization of the System.
- 4.1.2. Top up the User's Accounting Account in accordance with the channels and terms published in the "Top-Up" section.
- 4.1.3. Perform proper User identification pursuant to the Law of the RA "On Combating Money Laundering and Terrorism Financing", Central Bank of Armenia (CBA) regulations, and Annex No. 3.
- 4.1.4. Take all statutory organizational and technical measures to preserve data confidentiality and prevent unauthorized third-party access, alteration, or disclosure.
- 4.1.5. Upon receipt of the User's electronic redemption order, transfer equivalent funds in AMD (less applicable commission) to the User's designated bank account or card within a reasonable timeframe (via ArCa Pay – *instantly*; for transfers requiring interbank clearing – *within up to 3 banking days*).
- 4.1.6. Facilitate credential recovery and reissue Passwords/PIN codes in the event of loss, in accordance with the Data Recovery Procedure.
- 4.1.7. Ensure continuous technical maintenance and flawless operation of software and hardware facilities.
- 4.1.8. Provide Users with comprehensive information regarding available services, tariffs, and technical features.
- 4.1.9. Issue electronic settlement documents (electronic receipts in the "Transaction History" section) confirming completed payments in compliance with Armenian legislation.
- 4.1.10. Upon the User's request, provide hard-copy documentary receipts confirming completed payments.
- 4.1.11. Enable Users to receive monthly account statements via email and maintain 24/7 access to real-time transaction history within the System.
- 4.1.12. In the event of technical errors or disruptions occurring through the Operator's fault, immediately notify Users and restore system operability within a maximum of **24 (twenty-four) hours**, or otherwise compensate documented actual damages upon verified User demand.
- 4.1.13. Promptly notify the User of all circumstances of material importance for the performance of this Agreement.
- 4.1.14. **Offline Mode Operation:** If the User's device experiences loss of internet connectivity or unstable signal, the Mobile Wallet automatically suspends financial transactions and displays an offline status banner. For security reasons, no financial orders are accepted or executed in offline mode until full network connectivity and server synchronization are re-established.

4.2. The System Operator has the right to:

4.2.1. Reject a User's transaction if:

- (i) The User has not completed the required identification procedure;
- (ii) Reasonable grounds exist to suspect illegality or AML/CFT violations;
- (iii) The User enters an incorrect PIN code or verification OTP;
- (iv) The transaction amount exceeds the limits established for the given account type or service;
- (v) Rejection is stipulated by other provisions of this Agreement, Operator policies, or Armenian law.

4.2.2. Establish and unilaterally adjust minimum and maximum transaction limits for account top-ups, transfers, and withdrawals.

4.2.3. Deny transaction cancellation requests if cancellation is precluded by System Rules, Service Provider terms, or lack of recipient consent.

4.2.4. Retain charged commission fees on Completed Transactions upon cancellation requests, unless the cancellation resulted directly from Operator error.

4.2.5. Temporarily suspend System operations for scheduled upgrades, maintenance, or security hardening with prior notice to Users.

4.2.6. Unilaterally amend the terms and conditions of this Public Agreement in accordance with the established notification procedure.

■ 4. RIGHTS AND OBLIGATIONS OF THE OPERATOR (CONTINUED)

4.2.7. Unilaterally terminate this Public Agreement in the event of contractual breaches by the User.

4.2.8. Engage authorized third parties (processing centers, payment agents, technical providers) at its own expense and discretion to fulfill contractual obligations.

4.2.9. Request and receive all mandatory identification documents and data from the User.

4.2.10. Require supplementary documentation in circumstances stipulated by Armenian legislation and CBA regulations.

4.2.11. Block the User's Monet ID in the following instances:

- (i) Upon the User's verified request, provided identity is adequately confirmed;
- (ii) Upon detecting unauthorized access attempts or cyber security breaches;
- (iii) By initiative of the Operator's Information Security Department to safeguard account funds;
- (iv) Upon reasonable suspicion or detection of AML/CFT infractions or CBA regulatory violations;
- (v) In other instances established by this Public Agreement and Armenian legislation;
- (vi) Upon receiving official information regarding the User's death, declaration of death, missing person status, bankruptcy, or business suspension – pending determination of legal successors;
- (vii) Upon receiving official notice of the User being declared legally incapacitated.

4.2.12. Unilaterally terminate the Agreement and cease business relationships if the User is classified as an undesirable customer, including refusing future contract execution.

■ 5. RIGHTS AND OBLIGATIONS OF THE USER

5.1. The User undertakes to:

5.1.1. Duly perform obligations arising under this Public Agreement and the published System Rules.

5.1.2. Provide accurate and true personal and registration data required for identification and service delivery.

5.1.3. Immediately notify the Operator of any doubts regarding the validity or execution of any transaction.

5.1.4. Strictly adhere to all System Rules and security standards when executing operations.

5.1.5. Maintain strict confidentiality regarding all information acquired within the scope of System utilization.

5.1.6. Bear full personal responsibility for balance losses or adverse consequences resulting from disclosure of Monet ID credentials, Passwords, or PIN codes to third parties, whether due to negligence, imprudence, or fault.

5.1.7. Promptly inform the Operator of any technical errors, credential compromises, or fraudulent attempts.

5.1.8. Immediately notify the Operator of any changes in passport details, residence, phone number, or email.

5.1.9. **Not utilize** the Accounting Account for commercial or entrepreneurial purposes (such as unauthorized business payment collection by natural persons) and never transfer account access to third parties.

5.1.10. Disclose Beneficial Owners and legitimate sources of funds upon the Operator's first request.

5.1.11. Use the Monet ID strictly in a personal capacity.

5.1.12. Maintain and operate only **one Accounting Account**, unless opening an additional account is formally justified in writing and pre-approved by the Operator.

5.2. The User has the right to:

5.2.1. Access all System services in accordance with their assigned verification status and limits;

5.2.2. Request redemption of accumulated "Monet" units under the terms of the Agreement and Tariffs;

5.2.3. Request account recovery and reissuance of PIN codes or Passwords;

5.2.4. Update verified mobile phone numbers pursuant to established security verification procedures;

■ 5. RIGHTS OF THE USER (CONTINUED)

5.2.5. Submit applications, inquiries, and complaints electronically or in hard copy. Electronic complaints are accepted *strictly from the verified email linked to the Monet ID accompanied by a certified copy of the identity document*. In-person complaints require presentation of the original identity document.

5.2.6. Submit proposals regarding enhancements to service quality and operational procedures;

5.2.7. Access financial partner products (including remote loans and deposits) subject to proper identification and acceptance of the respective bank's customer agreements;

5.2.8. Independently block specific service categories or the entire account at any time via Stop Services, and modify Passwords, PIN codes, and biometric authentication settings.

■ 6. LIABILITY OF THE PARTIES

6.1. The Parties bear statutory liability for non-performance or improper performance of contractual obligations under the laws of the Republic of Armenia.

6.2. The Operator bears financial liability for prepaid funds solely upon presentation of an official payment document (bank receipt, cash order, terminal receipt) verifying the deposit, and provided the depositor's identity corresponds to the Account holder.

6.3. The Operator is not liable for technical failures of hardware, communication channels, or third-party networks beyond its reasonable control resulting in temporary unavailability of services, provided the Operator promptly alerts Users via accessible channels.

6.4. The Operator is not liable for lawful service denials executed pursuant to this Agreement, System Rules, Armenian law, or partner financial institution requirements.

6.5. The Operator bears no liability for the confidentiality or compromise of data stored on the User's personal hardware devices (smartphones, personal computers).

6.6. Complaints concerning service delivery are reviewed under "MePay" LLC's Dispute and Complaint Resolution Procedure.

6.7. The User bears sole responsibility for adverse outcomes resulting from the loss, disclosure, or transfer of Passwords, PIN codes, or account numbers. Transfer encompasses both intentional sharing and the selection of weak or predictable credentials.

6.8. The Operator is fully released from liability for balance debiting if such debiting resulted from credential compromise on the part of the User.

6.9. Legal relationships concerning banking and loan services arise exclusively between the User and the respective Financial Institution. The Operator is not a party to such transactions and assumes no liability thereunder.

■ 7. FORCE MAJEURE

7.1. The Parties are released from liability for partial or complete non-performance of obligations under this Public Agreement if such failure resulted from force majeure events occurring after contract execution that could not be reasonably foreseen or prevented (earthquakes, floods, acts of war, martial law, state of emergency, blockades, acts of the CBA or state authorities, global network shutdowns). If force majeure conditions persist for more than 2 (two) consecutive months, either Party may terminate the Agreement upon written notice to the other Party.

■ 8. SETTLEMENT OF FRAUD, UNAUTHORIZED TRANSACTIONS, AND TECHNICAL ERRORS

8.1. Upon discovering signs of unauthorized debits, fraud, or technical errors, the User is entitled to inform the Operator via established notice procedures, and is obligated to do so immediately, but **no later than 5 (five) calendar days** from the date when the User became aware or should have become aware of such occurrence.

8.2. The Operator is obligated to undertake all technically viable measures to cancel unauthorized operations, rectify errors, conduct a thorough internal investigation, and notify the User of the investigation findings.

8.3. If errors or disruptions occurred through the Operator's fault and resulted in a loss of "Monet" units, the Operator shall restore the balance, except where more than 2 (two) months have elapsed since the incident, or where the User failed to notify the Operator within the mandatory 5-day period.

■ 9. APPLICABLE LAW AND DISPUTE RESOLUTION

9.1. This Public Agreement is governed by and construed in accordance with the substantive and procedural laws of the Republic of Armenia.

9.2. Any disputes or controversies shall be subject to pre-trial settlement under the "Dispute, Error, and Complaint Resolution Procedure of 'MePay' LLC" published on the Website.

9.3. Pursuant to the Law of the RA "On the Financial System Mediator", property disputes of natural persons may be submitted to the Office of the Financial System Mediator of Armenia.

■ 10. MISCELLANEOUS PROVISIONS

10.1. Matters not regulated herein are governed by the rules published on the Operator's website, or, in their absence, by applicable laws of the Republic of Armenia.

10.2. Execution of this Agreement in electronic form is recognized as legally equivalent to a paper contract executed under wet-ink signatures.

10.3. Service delivery terms and conditions are published on the Operator's official website.

10.4. This Agreement enters into legal force upon creation of the User's Monet ID.

10.5. Either Party may terminate this Agreement by serving a **15 (fifteen) calendar days** prior notice to the other Party.

10.6. Account Deletion: When submitting an account deletion/closure request, the balance of the Accounting Account must be strictly **0 (zero) AMD**. If a positive balance exists, account deletion is blocked (**BalanceNot0**). The residual balance must be redeemed, spent, or transferred prior to deletion.

■ 11. NOTICES AND COMMUNICATIONS

11.1. Formal notices are delivered electronically: via email, website publications, Push Notifications in the Mobile Wallet, or SMS messages.

■ 12. ASSIGNMENT OF RIGHTS

12.1. The Operator has the right to assign and transfer all contractual rights and obligations to a Qualified Assignee, and the User hereby provides irrevocable consent to such transfer, provided all User rights and protections are preserved.

12.2. The assignment includes personal data processing rights and transaction histories under the Privacy Policy (Annex No. 1). The User gives unconditional consent to such transfer to the Qualified Assignee under identical terms.

ANNEX NO. 1 TO THE PUBLIC OFFER AGREEMENT
PRIVACY AND DATA PROTECTION POLICY (PRIVACY POLICY)

A. General Provisions: The System Operator guarantees confidentiality and protection of User personal data. By accepting this Policy, the User provides consent to the collection, processing, storage, and transfer of personal data as set forth herein.

B. Collection and Processing of Personal Data: To register and service Users, the Operator processes: first name, last name, registration/residence address, phone number, email address, date of birth, passport/ID card details, Public Services Number (PSN/SSN), and document copies. The Operator is authorized to submit online inquiries to the State Population Register of the RA (via EKENG / Migration and Citizenship Service of the MIA RA) to verify the authenticity of identity data.

C. Cryptographic Protection and Security Standards: "MePay" LLC protects personal and financial data using industry-leading technical standards:

1. Encrypted Channels: All communication between the Mobile Wallet and server infrastructure operates strictly over **TLS 1.3 (Transport Layer Security)**, preventing eavesdropping and Man-in-the-Middle (MitM) attacks.

2. Sensitive Data Storage: Identity, personal, and payment records are encrypted on secure servers using **AES-256-GCM and RSA-4096** algorithms.

3. Credential Hashing: Passwords and PIN codes are *never stored in plaintext* and undergo salted, irreversible cryptographic hashing based on **PBKDF2 / Argon2** standards.

D. Policy Amendments: The Operator may update this Policy with mandatory prior notice to Users at least 15 (fifteen) calendar days before changes take effect.

ANNEX NO. 2 TO THE PUBLIC OFFER AGREEMENT
"MONET ID" ACCOUNT STATUSES AND DESCRIPTIONS

Account Status	Legal and Technical Definition
Registered Registered	A newly opened account. Retained for a maximum of 90 (ninety) days. If the User does not bind a verified bank card in their name during this period, the account is converted to Deleted status.
Active Active	A fully functional, identified account through which at least 1 (one) transaction was completed within the preceding 365 calendar days.
Locked Locked	An account automatically locked by security systems following repeated erroneous entries of credentials or PIN codes. Restored upon proper identity verification.
Suspended Suspended	An account temporarily suspended automatically upon detection of suspicious transactions under AML/CFT laws and internal risk management procedures.
Stop Services Modes: ActiveBlocked UnblockPending Unblocked	ActiveBlocked: Services self-blocked by the User via the Mobile Wallet. UnblockPending: Status during the security <i>Cooldown Period (up to 24 hours)</i> following a remote unblock request (services remain unavailable). Unblocked: Full restoration of functionality after verification by the Operator.
Suspended by User Suspended by User	An account temporarily frozen upon the voluntary written or electronic request of the User.
Banned Banned	An account indefinitely blocked by the Compliance Monitoring Body upon detection of fraud, money laundering, or regulatory breaches.
Terminated / Deleted Terminated / Deleted	An account closed upon User request (with zero balance) or following 1 year of inactivity, with data archived pursuant to statutory retention requirements.

ANNEX NO. 3 TO THE PUBLIC OFFER AGREEMENT

USER IDENTIFICATION PROCEDURES AND SECURITY MEASURES

1. User Verification States in the System (UserState):

- **New** — freshly registered profile undergoing initial onboarding;
- **DocumentVerified** — User whose passport/ID details have been validated via the State Population Register (EKENG / Migration and Citizenship Service of the MIA RA) with photo copies uploaded;
- **PaymentVerified** — User who has linked and verified their own bank card (ArCa/vPOS). Enables full access to all payment, settlement, and transfer services;
- **Inactive** and **Deleted** — inactive and archived profiles.

2. Identification Procedure for Natural Persons:

2.1. Remote Identification via Mobile Wallet (Primary Method):

- Step 1:** Verification of Armenian mobile number (+374) via SMS OTP and email address via Email OTP;
- Step 2:** Selection of document type (RA Passport or ID Card) and entry of series and document number;
- Step 3:** Automated online validation query via EKENG / MIA RA database verifying valid document status ("PRIMARY_VALID"), absence of death records, age of at least 16 years, and sanctions/AML blacklist clearance;
- Step 4:** Photographing and uploading original document images (both sides of ID Card or passport spread);
- Step 5:** Binding and verification of personal bank card (ArCa / Visa / MasterCard) with automated name and PSN matching and instant pre-authorization reversal.

2.2. In-Person Identification at Operator Office: The User may complete verification in person at the Operator's office by presenting an original valid identity document.

3. Identification of Legal Entities and Individual Entrepreneurs:

Conducted upon submission of state registry extracts, charter, TIN certificate, bank details, and identity documents of the director or authorized attorney.

8. Authentication and Transaction Confirmation Security Standards:

8.1. PIN Code and Biometric Authentication:

1. During registration, the User establishes a personal 6-digit PIN code serving as their simple electronic signature.
2. Every outgoing financial transaction (payment, transfer) requires mandatory PIN code confirmation.
3. Where supported by the mobile device, the User may enable biometric authentication (Touch ID / Face ID) for convenience. Biometrics operate as a local convenience feature, while knowledge and secrecy of the PIN code remain mandatory.
4. **Rate Limiting:** Upon **5 (five) consecutive** erroneous entries of PIN code or Password, the System automatically locks access to protect the account from brute-force attacks.

8.2. Password Complexity Rules: Passwords must contain at least 8 characters, including at least one uppercase letter, one lowercase letter, one digit, and one special character (!@#%\$^&*).

■ CORPORATE DETAILS AND OPERATOR SIGNATURES

SYSTEM OPERATOR "MONET"

"MEPAY" LLC

Republic of Armenia, Yerevan 0033, Marshal Baghramyan Ave.,
53, Apt. 66

Registration Number: 264.110.1122587

TIN (Tax ID): 00219684

Official Website: www.mepay.am

24/7 Customer Support: +374 60 700 701

Email: support@mepay.am

OFFER ACCEPTANCE & LEGAL VALIDITY

This Public Agreement carries full legal force and is permanently accessible online at www.mepay.am.

The Agreement is deemed duly executed in electronic form upon the generation of the User's personal Monet ID.

Director of "MePay" LLC

[Seal / Electronic Signature]