ADRIATIC BANK AD PODGORICA

GENERAL TERMS
FOR THE USE OF PAYMENT CARDS AND ELECTRONIC BANKING SERVICES

VERSION 1.1

Podgorica, 22.07.2026

CONTENTS

1. INTRODUCTORY PROVISIONS

These General Terms and Conditions govern the manner of contracting, establishing, using, modifying, limiting and terminating payment card and electronic banking services of Adriatic Bank AD Podgorica, with its registered office in Podgorica, Bulevar Georga Washingtona br. 98, registered with the Central Register of Business Entities under number 40009471, registration number 03087158 (hereinafter: the Bank), by the user of services (hereinafter: the User).

These General Terms and Conditions constitute the legal basis for the use of:

- payment cards, including debit, credit and business cards;
- digital Cards and digital wallets;
- Adriatic Web Bank and Adriatic Mobile Bank;
- Office Banking servisa;
- SMS/Email service info;
- other related payment and digital services made available by the Bank.

These General Terms and Conditions apply in conjunction with:

- the Framework Agreement and individual agreements concluded between the Bank and the Beneficiary;
- application forms, applications, authorizations and other documentation for contracting individual products and services;
- the Bank's Tariff;
- A schedule for the execution of payment transactions, where applicable;
- other acts of the Bank that are available to the User;
- applicable laws and regulations.

The Bank reserves the right to amend these General Terms and Conditions in accordance with the applicable regulations, of which the User will be notified in the prescribed manner.

Operational issues related to the receipt and processing of requests, personalization, distribution, storage, delivery, delivery, activation, blocking, deactivation, cancellation and destruction of payment instruments, as well as the technical method of activating, administering and shutting down electronic banking services, are regulated by the Bank's internal acts and procedures. Internal acts may not diminish the rights of the User established by regulations, contractual documentation and these General Terms and Conditions.

1.1. SANCTIONS

The Bank operates in accordance with applicable regulations, international restrictive measures, sanction regimes and internal acts of the Bank that regulate the area of sanctions, restrictions and prohibitions on doing business with certain persons, countries, territories, goods, services, activities or transactions.

The Bank has the right, in accordance with applicable regulations and internal acts, to carry out verification of the User, authorized persons, beneficial owners, users of additional Cards, payee, payee, merchant, country of origin or destination of funds, as well as other participants in the transaction, in order to determine whether there are sanctions, regulatory or other restrictions on the establishment, continuation or execution of a business relationship, product, service or transaction.

The Bank may refuse to establish a business relationship, refuse to issue or use the Card, refuse to activate or use electronic banking, Office Banking services, digital wallets or other services, as well as refuse, postpone, block, suspend or limit the execution of an individual transaction, if its execution would be contrary to applicable regulations, international restrictive measures, rules of card organizations, rules of correspondent banks, rules of payment system or internal acts of the bank.

The Bank shall not be liable for damages, costs, delays or other consequences that may arise for the User or third parties as a result of the Bank's actions in accordance with the regulations, sanction regimes, requirements of the competent authorities, rules of payment systems, rules of card organizations, rules of correspondent banks or internal acts of the Bank in the field of sanctions and restrictions.

The Beneficiary is obliged to provide the Bank with accurate, complete and up-to-date data and documentation necessary to carry out the checks referred to in this paragraph. If the User fails to provide the required data or documentation, or if the Bank determines that there are sanction or other regulatory restrictions, the Bank may refuse or limit the provision of the service, i.e. terminate the business relationship, in accordance with the regulations and contractual documentation.

1.2. PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

The Bank implements measures to know and monitor Users, prevent money laundering, terrorist financing and proliferation financing of weapons of mass destruction, in accordance with the applicable regulations and internal acts of the Bank.

In order to implement the measures referred to in the previous paragraph, the Bank has the right and obligation to request from the User, legal representative, authorized person, beneficial owner, Card user, additional Card user, authorized user of electronic banking or Office Banking service the data and documentation necessary for:

- identification and verification;
- establishing and verifying beneficial ownership;
- determining the purpose and nature of the business relationship;
- determining the origin of funds and/or the origin of assets;
- monitoring of business relationships and transactions;
- assessing the risk of the User, product, service, usage channel or transaction;
- Compliance with other legal and regulatory obligations of the Bank.

The Bank may request additional data, statements, evidence and documentation from the User prior to the establishment of the business relationship, during the duration of the business relationship, before the execution of an individual transaction or after the execution of the transaction, when it is necessary to comply with the legal, regulatory or internal obligations of the Bank.

The User is obliged to provide the Bank with accurate, complete and up-to-date data and documentation, as well as to notify the Bank without delay of any change in data relevant to the business relationship, including changes in identification data, contact data, authorized persons, beneficial owners, activities, sources of funds, purpose of use of products or services and other data that the Bank considers relevant.

The Bank may refuse to establish a business relationship, refuse to execute a transaction, postpone the execution of a transaction, block or limit the use of a product or service, terminate a business relationship or take other measures prescribed by law and internal acts of the Bank if:

- The User fails to provide the requested data or documentation;
- the documentation provided is not complete, credible or sufficient to establish the purpose, basis, nature or origin of the funds;
- The Bank may not implement the prescribed measures of knowledge and monitoring of the User;
- there are grounds for suspicion or suspicion of money laundering, terrorist financing, financing of proliferation of weapons of mass destruction or other illegal activity;
- the execution of the transaction or the provision of the service would be contrary to the regulations, internal acts of the Bank or the requirements of the competent authorities.

In the case of deposits, withdrawals, transfers of funds, card transactions, cash-in transactions, bank deposits, international payments, Office Banking orders and other transactions, the Bank may request additional information about the payer, the payee, the purpose of the payment, the basis of the transaction, the origin of the funds and the accompanying documentation, regardless of the amount of the transaction, when it results from the risk assessment, applicable regulations or internal acts of the Bank.

In the case of cash deposits, withdrawals and other cash transactions, including Cash-in transactions, deposits or withdrawals via ATMs, Bank counters or other channels facilitated by the Bank, in the amount of EUR 10,000 or more, or the equivalent of that amount in another currency, as well as in the case of several interconnected transactions that in total reach or exceed the specified amount, the Bank may request additional information and documentation on the origin of the funds, the basis and purpose of the transaction, as well as prior approval or additional verification in accordance with applicable regulations, internal acts of the Bank and risk assessment.

The Bank, in accordance with the regulations, collects, verifies, processes, stores and submits to the competent authorities data on the User, authorized persons, beneficial owners, payer, payee and transactions, when necessary for the implementation of measures to prevent money laundering and terrorist financing.

The Bank shall not be liable for damages, costs, delays or other consequences that may arise for the User or third parties due to refusal, delay, blocking, restriction or non-execution of a transaction or service, when the Bank acts in accordance with regulations, requirements of competent authorities or internal acts in the field of prevention of money laundering and terrorist financing.

2. DEFINITIONS AND TERMS

The terms used in these General Terms and Conditions have the following meanings:

2.1. GENERAL TERMS

Banka – Adriatic Bank AD Podgorica, the issuer of these General Terms and Conditions and the provider of services governed by these General Terms and Conditions.

General Terms and Conditions – These General Terms and Conditions for the use of payment cards and electronic banking services of Adriatic Bank AD Podgorica.

User – A natural or legal person who uses one or more of the Bank's services on the basis of a contract, application form, request, authorization and these General Terms and Conditions.

Account – A common name for a transaction account, card account, payment account or credit lot, depending on the product and service.

Transaction Account – a payment account opened and maintained by the Bank for the User and used to execute payment transactions.

Card Account – An account or record showing financial transactions made using the basic or additional Cards, with the associated commissions, fees and interest.

Credit lot – An account or record of the Bank on which the approved credit limit, used and available amount, due and overdue liabilities, interest, fees and other elements of the loan product are recorded.

Tariff – A valid act of the Bank that defines fees, commissions, membership fees, costs and other financial conditions for the use of the Bank's products and services.

Schedule – An act of the Bank defining the time of receipt, processing deadlines and execution time of payment orders and transactions.

Durable medium – A means that allows the User to store information addressed personally to him, so that it is available for future use and can be reproduced in an unmodified form.

Sanctions – Restrictive measures, prohibitions or restrictions arising from applicable regulations, international sanctions regimes, decisions of competent authorities, rules of payment systems, card organizations or correspondent banks.

Beneficial owner – A natural person who, in accordance with the applicable regulations, directly or indirectly owns or controls the User, i.e. a person in whose name or on whose behalf a business relationship is established or a transaction is made.

Origin of funds – Data and documentation confirming the source of funds, the basis of the transaction and the purpose of using the Bank's product or service.

2.2. USERS AND AUTHORIZATIONS

Card User – a natural person to whom the Bank has issued a Card and whose name is stated on the Card or in the corresponding digital record.

Basic User – A natural person to whom the basic Card has been issued and who is the owner of the account to which the Card is linked, i.e. the user of the approved credit limit.

Additional Card User – a natural person to whom an additional Card has been issued at the request of the Basic User or the account holder, whereby the obligations arising from its use are debited from the account of the Basic User or the account holder.

Electronic Banking User – A natural or legal person who uses one or more of the Bank's electronic banking services.

Authorized User – A natural person who has been granted the right to use a certain service of the Bank by the account holder, legal representative or other authorized person.

Legal representative – A person authorized to represent a legal entity in accordance with the registration documentation and applicable regulations.

Authorized User of the Office Banking Service – A natural person authorized by the Business User to review, enter, verify, sign, send or administer orders within the Office Banking Service, within the framework of the assigned rights.

Access Rights – A set of functionalities assigned to the User, including viewing, entering, modifying, verifying, signing, sending orders or administering the User.

Signature Rights – Authorization to authorize an order individually or in combination with another signatory, in accordance with the documentation submitted to the Bank.

2.3. ELECTRONIC BANKING

Electronic Banking – Payment service with the use of means of distance communication that enables the User to access accounts, make payments and use other banking services through electronic channels.

Web Bank – An electronic banking service used through a web application to view accounts, enter and authorize accounts and other available functionalities.

Mobile Bank – An electronic banking service that is used through a mobile application and that may contain mToken, biometric authentication and other functionalities.

Office Banking – Desktop/Enterprise multibank service intended for legal entities, entrepreneurs and other business users, which enables viewing and managing accounts, preparing, signing, sending and monitoring orders, downloading statements and exchanging data and documentation.

tag. Info Service is a service that defines the manner and framework through which the Bank delivers to its Clients notifications, information and other communications related to the business relationship with the Bank, including, but not limited to, changes and activities on transaction accounts and payment cards, through one or more electronic communication channels, in accordance with applicable regulations, these General Terms and Conditions and the Bank's business policy.

User Profile / Digital Banking Profile – A unique digital profile of the User associated with his/her master data and one or more contracted services and accounts.

Webcontract – An application record of the Bank that records the contracted electronic banking service, assigned accounts, rights and status of the service.

Service status – Application status of the user or service, which can be created, activated, blocked, deactivated or other status defined by the technical solution.

Digital certificate – Electronic confirmation of the holder's identity that is used for secure authentication and electronic signing in the Office Banking service.

External certificate – A valid digital certificate issued to the user by another eligible issuer or another bank, which can be used in Office Banking after technical and identity verification.

Certification Authority – An authorized entity that issues, renews, suspends, and revokes digital certificates in accordance with its certification policy.

USB token – A physical security device on which the User's digital certificate and private key can be stored.

mToken - Functionality of the Bank's mobile application for account authentication and authorization

2.4. PAYMENT CARDS AND CARD BUSINESS

Card Organization – Visa Inc., Mastercard or other card organization with which the Bank has established cooperation.

Payment Card (Card) – A payment instrument that enables the payment of goods and services, withdrawal and, when enabled, payment of cash, as well as the use of other services through ATMs, POS terminals, self-service devices and electronic channels.

Debit Card – A card with which the User has funds up to the amount of the available balance on the transaction account to which the Card is linked.

Credit Card – a card with which the User has funds up to the amount of the approved credit limit, in accordance with the request, the credit limit agreement and other relevant acts of the Bank.

Business Debit Card – Debit Card issued to a legal entity, entrepreneur or other business entity, used by a natural person authorized by a business User.

Basic Card – A card issued to the Basic User, i.e. the Account Holder or the Credit Limit User.

Additional Card – A card issued to another person at the request of the Basic User or the account holder to which the Card is linked.

Digital Card – a digital payment instrument based on a Card issued by the Bank to the User and stored and used through a digital wallet or other supported digital channel.

Digital Wallet – An application or service that allows you to add and use a Digital Card through a compatible mobile or other device.

Digital Token – A unique digital identifier that replaces the data of a physical Card in a digital wallet and is used to execute and secure digital transactions.

Unclaimed Card – a Card created or personalized by the Bank, which the User has not collected within the period specified in these General Terms and Conditions.

Card Personalization – The process of entering personal data and security elements on the card plastic and chip, in accordance with the rules of the Bank and card organizations.

PIN-mailer – A security document or other secure channel through which the PIN is delivered to the User.

Processor – Provider of card data and transaction processing services with whom the Bank has contracted cooperation.

Personalization Center – An authorized service provider who performs personalization of Cards and/or preparation of PIN-mailers for the Bank.

Confirmation of receipt of the Card and PIN – A document by which the User confirms the receipt of the Card and/or PIN and familiarization with the obligations of their protection.

Urgent Card Creation – Creation of the Card by an accelerated procedure, when such a service is available and for a fee determined by the Tariff.

Delivery of the Card to the address – Delivery of the Card to the User via an authorized postal or courier service to the address accepted by the Bank for delivery.

Retained Card – A card held by an ATM or other device for technical, security, or other reasons.

Damaged Card – A card that cannot be used properly due to physical damage, technical malfunction or other reason.

Deactivation of the Card – Temporary or permanent disabling of the use of the Card in the Bank's systems.

Cancellation and destruction of the Card – The process by which the Card is permanently decommissioned and physically destroyed.

2.5. DOCUMENTATION FOR PRODUCTS AND SERVICES

Application form for the issuance of a Card – the Bank's Form, in paper or electronic form, by which the User requests the issuance of a debit or other Card for which a special credit limit agreement is not concluded.

Credit Card Application – User's request for approval of the Credit Card and the associated credit limit.

Credit Limit Agreement – the Agreement by which the Bank approves the credit limit for the use of the Credit Card and regulates the terms of its use and repayment.

Application form/application for electronic banking – Form or other contractual documentation by which the User requests the activation, modification or shutdown of Adriatic Web Banka, Adriatic Mobile Banka, Office Banking or SMS/Email info service.

Authorization – A document or record by which an account holder, legal representative, or other authorized person grants another person the right to use a product or service.

Framework Agreement – A contractual framework between the Bank and the User, which, together with individual contracts, application forms, requirements, authorizations, General Terms and Conditions, Tariff and Term Plan, regulates the use of the Bank's payment and other services.

2.6. SECURITY, AUTHENTICATION AND AUTHORIZATION

Authentication – A procedure that allows the Bank to verify the identity of the User or the validity of the use of a payment instrument.

Trusted Client Authentication (SCA) – Authentication based on at least two mutually independent elements from the categories of knowledge, possession, and ownership.

Personalized Security Data – Personalized features or data assigned or enabled by the Bank to the User for the purpose of identification, authentication and authorization.

Personalized Card Security Features – Data required to complete a card transaction, including PAN, expiration date, CVV/CVC and other data required to accept the Card.

Sensitive payment information – Information that can be used to commit fraud, including personalized security information.

PIN – A personal identification number known exclusively to the User, which is used for authentication and/or authorization.

mToken – is a function within the Bank's mobile application that enables secure authentication (identification) of the User, i.e. authorization (signature) of given orders remotely. The application is activated by entering the registration code (identification and activation), after which the user further determines the PIN for further use.

3D Secure (3DS) – A security standard for additional authentication of internet card transactions, which the Bank supports through Adriatic Mobile Banka and mToken, when additional authentication is required.

Authorization – the User's consent to execute the transaction, given in the manner agreed with the Bank, including PIN, signature, biometrics, mToken, one-time password, Card data or other accepted security element.

Biometric data – Unique physical properties of the User, such as a fingerprint or facial appearance, which are stored on the User's device and can be used for authentication or authorization.

One-Time Password (OTP) – A one-time security code used for authentication or authorization.

Push Notification – A message delivered through a mobile app to notify, authenticate, or authorize a transaction.

User Identification – The username, customer number, digital profile, or other identifier used to access the Service.

User credentials – A set of data and security elements used by the User for login, authentication and authorization.

Activation code – A one-time code used to activate an application, mToken, or other security element.

Identification Code – Code or other element used to identify the User when activating or using the Service.

2.7. TRANSACTIONS AND PAYMENTS

Payment transaction – payment, withdrawal or transfer of funds, initiated from the payer, on his behalf or by the payee, regardless of the obligations between the payer and the payee Distance payment transaction (electronic payment transaction) – a payment transaction that is initiated via the Internet or a device that can be used for distance communication

Card Transaction – Payment of goods or services, withdrawal or payment of cash, internet or MOTO payment or other operation performed using the Card.

Payment order – a payment order is an instruction submitted by a payer or payee to a payment service provider requesting the execution of a payment transaction.

Payer - a natural or legal person who has a payment account and gives an order or consent for payment from that account, or a natural or legal person who does not have a payment account and provides a payment order

Payee - a natural or legal person to whom the funds that are the subject of a payment transaction are intended;

Payment service user is a legal entity, state administration body and part of a foreign company (hereinafter: legal entity), entrepreneur and other person who performs activities in accordance with the regulations (hereinafter: entrepreneur) and natural person who uses payment services as a payer and/or payee;

National Payment Transaction – is a payment transaction in the execution of which the payment service provider of the payer and/or the payment service provider of the payee who provide payment services in the territory of Montenegro participate.

International payment transaction – is a payment transaction in which one payment service provider provides a payment service in the territory of Montenegro and another payment service provider in the territory of a third country, as well as a payment transaction in which the same payment service provider provides a payment service for one payment service user in the territory of Montenegro, and for the same or another payment service user in the territory of a third country, and payment transactions are executed via SWIFT or SEPA payment scheme.

Credit transfer – is a payment service by which the payee's payment account is credited for a payment transaction or a series of payment transactions debited from the payer's payment account, by the payment service provider with which the payer's payment account is maintained, based on a payment order provided by the payer.

Instant credit transfer is a credit transfer that is executed immediately and continuously, 24 hours a day on any calendar day, whereby the payment transaction is executed and the funds are made available to the payee within 10 seconds of receipt of the payment order, and relates exclusively to national credit transfers in euro;

Payment Initiation Service (PIS) – Payment service for initiating a payment order at the request of a payment service user relating to a payment account maintained by another payment service provider.

A payment initiation channel is any method, device or procedure through which a payer delivers a payment order to a payment service provider for the execution of a credit transfer, including internet banking, mobile banking application, ATM or by any other means at the premises of the payment service provider

Account Information Service (AIS) – is a payment service provided with an online connection, which provides consolidated information on one or more payment accounts held by a payment service user with another payment service provider or with several payment service providers.

Account Payment Service Provider – Payment Service Provider that opens and maintains a payment account for the User.

List of trusted payees – A list of recipients marked as trusted by the User, according to which, when the prescribed conditions are met, an exemption from trusted authentication can be applied.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a global network that enables secure, standardized and reliable exchange of financial messages between financial institutions. Through the use of SWIFT codes and messages in accordance with international standards, it enables the transfer of information about payment transactions regardless of the location of banks or other participants in the system.

SEPA (Single Euro Payments Area) payments are all types of credit transfers that are made as international payments in the Single Euro Payments Area through SEPA payment schemes according to standardized and defined rules according to SEPA member states

BBAN – Payment account number in national format.

IBAN – International Payment Account Number.

BIC/SWIFT code – *Unique identifier* of a bank or other financial institution in international payment transactions.

RTGS (Real-Time Gross Settlement) system is a system of the Central Bank in which individual payment transactions between participants are executed on a gross basis in real time;

A Deferred Net Settlement (DNS) system is a system in which interbank payment transactions are executed on a net basis over a deferred period of time.

TIPS Clone system (TARGET Instant Payment Settlement Clone) is an instant payment system within Montenegro that enables the execution of payment transactions between the payer and the payee in real time, continuously (24/7/365), according to standardized and defined rules and technical standards of the SCTInst scheme, but without direct connection to its infrastructure;

The limit per transaction for the execution of an instant credit transfer represents the maximum amount of the user's instant credit transfer, and the user can independently manage the specified limit via electronic banking, provided that the specified limit is not higher than the predefined limit;

The predefined limit is the maximum amount per individual transaction for the execution of an instant credit transfer, which is defined by the Central Bank of Montenegro or alternatively set at the client level by the Bank;

The daily limit for making an instant credit transfer represents the maximum daily amount of all instant credit transfers of the user, and the limit can be independently defined or changed by the user via electronic banking.

Cancellation – is a procedure for reversing a payment order in which the payer withdraws a previously set payment order that has not yet been authorized.

Revocation of an order/transaction – A request for the withdrawal of an authorized order before execution, i.e. a request for the revocation of an international transaction after execution, in accordance with the rules of the respective system.

2.8. CARD OPERATIONS AND CALCULATION

Available balance – The amount of funds on the account available to the User, minus active reservations and other recorded debits.

Reservation – Temporary reduction of the available balance on the basis of an authorized card transaction for which the Bank has not yet received the final financial confirmation.

Credit Limit – The maximum amount of credit granted by the Bank per credit lot or credit card.

Spending and transaction limits – Maximum amounts and/or number of transactions that the User can make in a given period and per specific channel.

Daily Limit Profile – A set of predefined daily ATM and POS limits assigned to the Card.

Accounting period – The period for which the Bank makes a cross-section of transactions and calculates liabilities, fees, commissions and interest.

Card Organization Exchange Rate – The exchange rate of the Visa or Mastercard system applied to the conversion of transactions made in a currency other than the currency of the account, on the day of processing the transaction in the card system.

DCC (Dynamic Currency Conversion) – A service by which the ATM owner or merchant may offer the User to make a transaction in the currency of the Card or another currency offered, according to the exchange rate and fees displayed before the transaction is confirmed.

Monthly statement – Overview of transactions, fees, commissions, interest and other data for the billing period.

Minimum amount to be paid – The minimum monthly amount of obligations on the credit Card that the User must settle within the agreed period.

Deadline for settling the due debt – The date by which the Credit Card User must settle the due obligations.

Card Validity Period – The period until which the Card may be used, until the last day of the month specified on the Card.

Renewal/re-issuance of the Card – Issuance of a new Card upon the expiry of the validity period of the previously issued Card.

Card Replacement – Issuance of a new Card due to damage, loss, theft, change of data, compromise or other justified reason.

PIN re-creation – Re-assigning, printing or delivering a PIN to the User, when such a service is enabled.

Turnover Card – Overview of changes in the account or credit lot linked to the Card.

2.9. CARD INFRASTRUCTURE AND ACCEPTANCE NETWORK

Point of Sale – A legal or natural person who accepts the Card as a means of payment for goods and/or services.

ATM – A self-service device for cash withdrawal, balance checking, PIN change, cash deposit, and other services provided.

Cash-in transaction – Depositing cash into an account using the Card at an ATM or other device that supports payment.

Payment device – A self-service device intended for cash payment to the account of a business User, in accordance with the technical possibilities and conditions of the Bank.

POS terminal / EFTPOS – A device at a point of sale, bank counter or other acceptance point used for electronic card transactions.

Cash advance – Cash withdrawal using the Card at a counter POS terminal or other acceptance point.

CVV/CVC – A security number on the Card used for internet and other transactions without the physical presence of the Card.

PAN – Card number that uniquely identifies the Card in the card system.

MOTO transaction – A transaction without the physical presence of the Card, in which the User submits card data to the merchant by mail, e-mail, telephone or other similar channel.

Contactless payment – A transaction made by bringing a Card or mobile device to a POS terminal that supports contactless technology.

NFC technology – Technology that enables the exchange of data between the Card or device and the POS terminal without physical contact.

3. GENERAL RULES OF USE

The User is obliged to use the Bank's products and services in accordance with the contractual documentation, these General Terms and Conditions, applicable regulations, rules of card organizations and instructions of the Bank.

The User is obliged to keep the Card, devices, digital certificates, tokens and personalized security data and not to give them to third parties.

The User is obliged to notify the Bank without delay of suspected loss, theft, compromise or unauthorized use of the Card, electronic banking, digital certificate, token, device or security data.

A bank may temporarily limit or disable the use of a product or service when there are security, regulatory, credit, operational or other objectively justified reasons.

4. SERVICE USERS

Users of services are natural and legal persons, residents and non-residents, who have an account with the Bank or meet other conditions prescribed for a specific product.

Users can be account holders, proxies, legal representatives, users of basic and additional Cards, as well as other persons who have been assigned the rights to use a particular service.

For minors from 14 to 18 years of age, the Card can be issued with the participation and consent of a parent or guardian, or under the conditions applied by the Bank in accordance with the regulations and type of account.

The user is responsible for the accuracy, completeness and up-to-dateness of data on identity, contacts, authorizations, access rights, signature rights and limits.

5. SELECTION AND CONTRACTING OF SERVICES

The user chooses the service in accordance with the Bank's offer and the conditions for a specific product.

For a debit Card, the User submits an application form or other appropriate application. The User submits an application for a Credit Card, and the approval and use of the credit limit is regulated by the Credit Limit Agreement and other relevant acts of the Bank.

Web Bank, Mobile Bank, Office Banking and SMS/Email info are agreed upon by means of an appropriate application, application form, Framework Agreement or other documentation prescribed by the Bank.

By submitting a request, signing the contractual documentation or activating the service, the User confirms that the General Terms and Conditions and the Tariff have been made available to him and that he accepts the rules of use of the contracted product.

6. PAYMENT CARDS – ISSUANCE, COLLECTION AND USE

6.1. Card issuance

The Card is issued by the Bank on the basis of a duly submitted application form, application and other documentation, depending on the type of Card and product.

The decision on the issuance of the Card is made by the Bank according to internal criteria, type of product and applicable regulations. The bank may request additional information and documentation and verify the information provided.

The card is tied to the relevant account or credit lot and can only be used up to the amount of available balance, credit limit and applicable transaction limits.

6.2. Documentation for the issuance and use of the Card

The documentation, depending on the product, consists of:

- application form or application for the issuance of a debit or Business Debit Card;
- application for a Credit Card and a credit limit agreement;
- these General Terms and Conditions and the applicable Tariff;
- confirmation of receipt of the Card and PIN, where applicable;
- other documentation required by the Bank in accordance with the regulations and the type of product.

6.3. Ownership, collection and delivery of the Card

All issued Cards remain the property of the Bank and must be returned at the request of the Bank.

The card can be picked up in person at the Bank's branch office or, when the service is available and selected, delivered to the User's address via an authorized postal or courier service.

The Bank will send the card via courier service through a reliable courier/delivery company with an indication for the mandatory personal delivery of the shipment, at the explicit written request of the User to a precisely defined address in the request.

By signing the request for sending cards and PIN via courier service, the User accepts and assumes all the risks of this type of delivery and agrees that the Bank is not responsible for any abuse or damage due to this method of delivery.

The Bank charges a fee for sending the card and PIN via courier service in accordance with the Tariff valid on the day of submitting the application.

The Bank will activate the card only after receiving a notification from the User that it has received the card and the corresponding PIN code, delivered via e-mail or SMS message from the e-mail address, i.e. phone number registered for a specific client in the Bank's Core Banking Application

In the case of personal collection, the Bank identifies the User and, where applicable, obtains a Confirmation of Takeover. The card can also be taken over by another person on the basis of an appropriate authorization certified by the competent authority, if the Bank accepts such a method of collection.

When delivering to the address, the Card is handed over to the person and in the manner specified by the request, the rules of the Bank and the rules of the authorized courier. The user is obliged to provide the correct address and conditions for proper identification and delivery.

The PIN is delivered separately from the Card or through another secure channel provided by the Bank. The bank may charge for delivery in accordance with the Tariff.

If the delivery fails, the Card is returned to the Bank and treated as an unclaimed Card. The Bank may repeat the delivery or make the Card available at the branch, in accordance with its rules and with the possibility of charging additional costs.

6.4. Unclaimed cards

If a natural person does not take over the Card within 90 days from the date of creation/personalization, the Bank has the right to deactivate, cancel and destroy the Card without additional consent of the User.

For users of the Private Banking service, the deadline for collection is six months from the date of creation/personalization of the Card.

The above deadlines also apply to Cards returned to the Bank after unsuccessful delivery, as well as to unclaimed reissued or replacement Cards.

For re-issuance, the User submits a new application form or application, and the costs are calculated in accordance with the Tariff.

6.5. Additional cards

At the request of the Basic User or Account Holder, the Bank may issue one or more additional Cards, in accordance with the Bank's offer.

The main user or account holder is responsible for all transactions, fees, commissions, interest and other obligations arising from the use of additional Cards.

The Additional Card User is obliged to comply with these General Terms and Conditions and the Bank's security rules.

6.6. Ways to use the Card

The card can be used:

- for payments at POS terminals and other acceptance devices;
- for online payments and, where enabled, MOTO transactions;
- for cash withdrawals at ATMs and counter POS terminals;
- to deposit cash at ATMs and devices that support Cash-in;
- for digital payments through a digital wallet;
- for other services provided by the Bank and the Receiving Network.

The card may only be used by the person whose name it is called. The user is obliged, at the request of the merchant or other acceptance point, to show an identification document.

The card may not be used for illegal transactions, nor should it be left as collateral or security.

6.7. Cash deposits at ATMs and cash deposit machines

When the Bank enables the Cash-in functionality, the User may use the Card to deposit cash to the account to which the Card is linked, at a technically trained ATM or a market payment device.

The device can only accept supported currencies, denominations, and types of cash. Supported amounts, the number of banknotes or coins per deposit and daily limits may be limited by the technical characteristics of the device, regulations and internal rules of the Bank.

The user is obliged to check the amount recognized by the device before confirming. By confirming the payment, the User accepts the displayed amount, except in the case of a proven technical error.

The machine may hold a suspicious, damaged, unacceptable or unrecognised banknote for verification. The bank will act in accordance with the regulations and the results of cash post-processing.

For individual or related payments exceeding the amounts defined by the regulations, internal acts and rules of the Bank, the Bank may require prior approval and documentation on the origin and basis of the payment.

If the invoice is not credited with the expected amount or the device does not issue an appropriate confirmation, the User is obliged to report the problem to the Bank without delay and save all available payment information.

6.8. Daily limits on the use of the card.

In order to ensure the safe use of the Card, the Bank sets daily limits for cash withdrawals at ATMs (ATM limit) and for other card transactions (POS limit).

POS limit includes payments at POS terminals, internet payments and other card transactions that are not ATM withdrawals, unless the Bank sets a special limit for a particular type of transaction.

Cards are initially assigned an LP2 limit profile, which is EUR 1,000 per day for ATM transactions and EUR 5,000 per day for POS and other transactions, unless another profile is approved for a specific product, User or request.

The user can request a change in the limit by submitting a request to the Bank or independently through Adriatic Web Banka/Adriatic Mobile Banka, if the functionality is available. The bank may approve, reject or limit the requested amendment in accordance with the risk assessment, available balance, credit limit and internal rules.

A change in the limit takes effect after confirmation in the Bank's system. The limits do not affect the amount of available funds and do not constitute an obligation for the Bank to approve the transaction if other conditions are not met.

Overview of limit profiles:

LIMIT PROFILE	DNEVNI ATM LIMIT	DAILY POS LIMIT
LP0	100 EUR	300 EUR
LP1	500 EUR	1.000 EUR
LP2	1.000 EUR	5.000 EUR
LP3 - Initial profile	2.000 EUR	10.000 EUR
LP4	5.000 EUR	20.000 EUR
LP5	10.000 EUR	50.000 EUR
LP6	15.000 EUR	100.000 EUR
LP7	Up to the technical maximum of the system, the available balance and the limit approved by the Bank	Up to the technical maximum of the system, the available balance and the limit approved by the Bank
L12	800 EUR	5.000 EUR
L13	800 EUR	10.000 EUR
L14	800 EUR	20.000 EUR

The Bank may change the available profiles, their amounts or the method of application in accordance with regulations, rules of card organizations, risk assessment and technical possibilities, with appropriate notification to the User when necessary.

6.9. Reservation and final posting of card transactions

When the Bank approves a card transaction, the amount of the transaction and any associated fees may be reserved and immediately reduce the available balance, even if the transaction has not yet been finalized.

The final amount credited may differ from the reserved amount due to exchange rate conversion, tip, surcharge, partial cancellation, post-processing or other justified reason in accordance with the rules of the merchant and the card organization.

In the case of hotels, rent-a-car companies, gas stations and other activities, the merchant can reserve an estimated or increased amount in order to secure future billing.

The reservation is released upon receipt of the final financial confirmation, cancellation or expiration of the deadline defined by the rules of the card organization and the technical system. The bank cannot always release the reservation immediately on its own without confirmation from the merchant or the acquiring bank.

If the final transaction is delivered after the release of the reservation or without prior reservation, the Bank has the right to debit the account for the duly submitted transaction, in accordance with the regulations and rules of the card organization.

6.10. Transactions in foreign currency and DCC

A card transaction made in a currency other than the currency of the account is converted according to the exchange rate of the Visa or Mastercard system valid on the day of processing the transaction in the relevant card system, with the application of the Bank's conversion fee, when provided for by the Tariff.

The transaction processing date may be different from the date of purchase or cash withdrawal. Therefore, the amount reserved and the amount finally credited may differ due to changes in exchange rate and processing times.

A merchant or ATM owner abroad may offer the User DCC, i.e. the choice to make the transaction in EUR or another currency offered. Prior to confirmation, the User should be shown the selected currency, exchange rate and possible fee.

If the User accepts DCC at a terminal or ATM of another bank, the exchange rate and fees are determined by the DCC service provider, the merchant or the owner of the device, and not by Adriatic Bank. The bank is not responsible for the exchange rate, additional fees or the method of display applied by the other provider.

Cash withdrawals at an ATM of another bank may include an additional fee charged by the ATM owner, regardless of the Adriatic Bank fee defined by the Tariff.

6.11. Security measures when using the Card

The User is obliged to keep the Card and security data with due care. In particular, it is obliged to:

- knows where the Card is at all times;
- He does not give the card to another person and does not leave him unattended;

- check the amount, currency and merchant details before confirming;
- Remember the PIN, keeps it separate from the Card and protects the PIN entry from the view of other persons;
- does not communicate PIN, CVV/CVC, passwords, activation codes or the content of push messages to third parties;
- immediately report a loss, theft, compromise or unknown transaction.

7. AUTHORISATION OF CARD TRANSACTIONS

7.1 POS, ATM and counter transactions

The User gives consent to the transaction by entering a PIN, signing, bringing a contactless Card or device, confirmation on the screen or other means supported by the receiving device and the Bank.

Cash withdrawals and deposits at ATMs are authorized by entering a PIN. After the prescribed number of erroneous entries, the Card may be blocked or held in the device.

7.2 Internet payments, 3D Secure and mToken

When making online payments, the User enters the Card data required by the merchant, including the Card number, the expiry date and the CVV/CVC, making sure that the data is entered only on a reliable website or application.

When 3D Secure or reliable authentication is required for a transaction, the User confirms or rejects the transaction through Adriatic Mobile Banka, in which the registered mToken is embedded.

The user is shown transaction data via push notifications or in the app, in particular the merchant, amount and currency. The user is obliged to verify the data before confirming it with a PIN or biometrics.

If Adriatic Mobilna Banka or mToken is not activated, if the device is blocked or if the User does not confirm the transaction within the stipulated period, the transaction may be rejected.

Certain transactions may be executed without additional confirmation in the mobile application when permitted by regulations, rules of card organizations or the nature of the transaction, including certain low-risk, recurring or merchant-initiated transactions.

> The Bank will never ask the User to provide the full PIN, CVV/CVC, password for the application or to send a photo of the Card by phone, e-mail or message in order to authorize the payment.

7.3. MOTO transactions

MOTO transactions are carried out without the physical presence of the Card, by providing data to the merchant by telephone, e-mail, mail or other similar channel. The merchant may require a signed letter of authorization or other proof of consent.

The user is obliged to use MOTO transactions only at trusted merchants and not to submit a PIN or other data that is not required for this type of transaction.

7.4. Contactless payments

For certain contactless transactions, no PIN entry or signature is required, in accordance with the rules of card organizations, regulations and security parameters of the Bank and the acceptance device.

Contactless payments without entering a PIN can be enabled up to EUR 50 for Visa Cards and up to EUR 40 for Mastercard Cards, with a cumulative limit of EUR 150 or a maximum of five consecutive transactions since the last reliable authentication, unless different terminal, country or card organization limits apply.

The bank or acceptance device may also ask for a PIN for a smaller amount for security verification.

8. DIGITAL CARDS AND DIGITAL WALLETS

8.1. Adding a Card to a Digital Wallet

The User can add a supported Card to the digital wallet according to the instructions of the Bank and the digital wallet provider. Adding may require additional identity verification and verification via the mobile app, SMS, Contact Center, or other channel.

The use depends on the compatibility of the device, the operating system, the availability of the digital wallet and the technical limitations of the Bank and the service provider. The number of devices or digital tokens may be limited.

8.2. Use and Crediting of the Digital Card

The Digital Card can be used at points of sale, ATMs and online points of sale that support the appropriate form of digital payment.

Transactions with a Digital Card are debited from the same account and are credited under the same basic conditions as transactions with a physical Card. The same limits, fees, exchange rate conversions and complaint rules apply, unless otherwise stated for the specific service.

The Bank does not charge for the installation of a digital wallet, unless otherwise specified in the Tariff. The wallet provider or telecommunications operator may charge for its own services in accordance with its terms and conditions.

8.3. Device protection and loss management

The user is obliged to protect the device with a PIN, password or biometrics, not to register biometric data of other persons on the device and not to leave the device unlocked or unattended.

If the device is lost, stolen or compromised, the User must immediately notify the Bank and, where possible, the digital wallet provider, in order to suspend or remove the digital token.

The Bank may suspend or delete the Digital Token without shutting down the physical Card, when technically possible and justified by security reasons.

8.4. Re-issuance, exchange and removal of the Card

In the case of regular re-issuance, the User may be obliged to update the data on the new validity period in the digital wallet, depending on the functionality of the digital wallet and the card organization.

A replacement Card with a new number is considered a new Card and must be re-added to the digital wallet.

Removing a Digital Card from a digital wallet does not shut down the physical Card or terminate the contractual relationship with the Bank. The bank will execute duly authorized transactions that occurred before the tokens are removed.

8.5. Data exchange and protection

For the purpose of registering and using the Digital Card, the Bank, the card organization, the digital wallet provider and other persons involved in tokenization may process and exchange the data necessary for the identification of the User, the creation and management of the Digital Token, authentication, execution of transactions and the prevention of misuse, in accordance with the applicable regulations.

9. ELECTRONIC BANKING

9.1. Types of services and available functionalities

Electronic banking includes Adriatic Web Bank, Adriatic Mobile Bank, Office Banking and SMS/Email info. The Bank may change or improve the functionalities of the service, while respecting contractual and legal obligations.

Depending on the type of User, assigned rights and technical availability, Web and Mobile Bank may enable:

- overview of balances, turnover and account statements;
- national, international and SEPA payments;
- view and manage Cards;
- changing the daily limits of the Card;
- temporary blocking and unblocking of the Card, when the functionality is enabled;
- overview of loans, liabilities and other products;
- exchange of messages and notifications with the Bank;
- overview of branch and ATM locations;
- other functionalities that the Bank makes available.

9.2. Adriatic Web Banka and Adriatic Mobile Bank

The service is activated after the identification of the User, verification of the account, authorization, contact data and receipt of the appropriate contractual documentation.

Through a single digital banking profile, the user can have access to their own accounts and the accounts of legal entities or other entities for which they are duly authorized.

The user can only use the accounts and functionalities for which he has been assigned rights. The right of review does not include the right to enter, verify or sign an order.

9.3. Office Banking

Office Banking is intended for business users who need to work with one or more accounts, banks, users and signature levels.

The service is activated based on the request of the Business User. For each Authorized User, special documentation is submitted and individual credentials, rights and a security element are assigned. The number of Authorized Users is not limited in advance, subject to compliance with the technical and contractual conditions.

Rights may include reviewing, preparing, entering, modifying, verifying, individual or collective signature, and sending orders. A user without the appropriate right cannot finally authorize or send an order.

The authorized user may use a digital certificate issued through the Bank or a supported external certificate, after appropriate verification. The digital certificate and USB token are personal and may not be shared with another person.

Loss of tokens, suspicion of compromise of certificates or termination of authorization must be immediately reported to the Bank for blocking, revocation or modification of rights.

Deletion of the application from the computer, termination of use, or absence of transactions does not constitute a cancellation of the service. Fees are calculated until the service or the Authorized User is formally deactivated in accordance with the request and rules of the Bank.

9.4. Info service (SMS, e-mail, Viber or other communication channel)

Info services can be arranged individually or together.

The messages are for informational purposes only and do not replace the statement, turnover overview or other official records of the Bank. Non-delivery or delay of the message does not affect the execution, validity, or posting of the transaction.

The Bank is not responsible for delays or non-delivery of messages caused by a problem with the mobile operator, internet provider, e-mail service, the User's device or other circumstances beyond the control of the Bank.

The user is obliged to report the change of phone number or e-mail address without delay. Activation, modification and deactivation of the service are carried out on the basis of the User's request, and the fees are calculated according to the Tariff.

9.5. Technical Conditions, Availability and Interruptions

The User is obliged to provide the device, Internet connection, supported operating system and other equipment necessary for the use of the Service.

The services are generally available 24 hours a day, seven days a week, but may be temporarily unavailable due to maintenance, upgrades, security incidents, outages with third-party providers, or force majeure.

The bank will announce planned outages when possible and when the notification does not jeopardize the security of the system.

10. ACTIVATION, AUTHENTICATION AND SECURITY FEATURES

10.1. Activation of the Service

After approving the service, the Bank provides or provides the User with a username, activation codes, mToken, digital certificate or other security elements, depending on the service.

Initial credentials are one-time or time-limited. The user is obliged to perform the activation according to the instructions of the Bank and to define their own PIN or password when it is provided.

10.2. Authentication and authorization

The user can access the service only after successful authentication. Orders and other actions that require consent are authorized with an mToken, PIN, biometrics, digital certificate, or other supported element.

Accounts and users without the right to confirm or sign are not granted the option of final authorization of the order.

A bank can block access after exceeding the number of erroneous entries or when there is a suspicion of abuse.

10.3. Alteration or loss of the device

When changing the mobile device, the User may be obliged to reactivate Adriatic Mobile Banka and mToken. Before stealing or handing over the old device to another person, the User is obliged to remove the application and the data that allow access to the service.

The User must immediately report any loss, theft or compromise of the device to the Bank. The bank may block the user's profile, mToken or other security elements until they are re-identified and activated.

10.4. Digital certificates and tokens for Office Banking

A digital certificate is issued and renewed on the basis of an appropriate request and is valid for the period specified in the certificate. The fees for issuance, renewal and USB tokens are determined by the Tariff.

The user is obliged to keep the token, private key, PIN and certificate and to use them exclusively within the scope of the assigned authorizations. A bank may require the revocation or replacement of a certificate when the authorizations cease to exist, when the certificate is compromised, or for other justified reason.

11. EXECUTION OF THE TRANSACTION

All forms of use of electronic banking, including the entry of payment orders from the user's account, which are entered electronically with the application of the prescribed user identification, are equated with handwritten signing and are binding on the user.

Electronic banking services will be available to the User 24 hours a day, seven days a week. Received payment orders will be processed every working day from 08:00 to 15:30. Orders received after this time will be processed on the next business day. Notwithstanding the above, orders for instant credit transfers are processed continuously, 24 hours a day every calendar day, and are executed within 10 seconds.

A payment transaction is considered authorized only if the payer has given consent to execute the payment transaction. Consent may be given before or, if agreed between the Client and the Bank, after the execution of the payment transaction. Consent to execute a payment transaction or a series of payment transactions must be given in the manner agreed between the payer and his payment service provider, and may also be given through the payee or payment initiation service provider, otherwise the payment transaction is considered not authorised.

The Bank is obliged to apply reliable authentication of the User when he initiates an electronic payment transaction.

Authorization or confirmation of the transaction is given in one of the following ways:

1) Authorization of payment transactions made through the Adriatic Web Banka service – is carried out in such a way that the user signs an order for payment with mToken using the dual authentication system (PIN + One time password). A one-time password is generated automatically via mToken after the User has identified himself by entering a PIN or logging in with biometric data.
2) Authorization of payment transactions submitted through the Adriatic Mobile Banka service – is carried out in such a way that the user signs a payment order by entering the PIN used for identification or with the use of biometric data.

12. PAYMENT ORDERS

Payment is made by initiating by the User to the telecommunications or network operator or information technology system operator.

The user is solely responsible for completing and controlling the correctness of the completed orders. The User undertakes to perform Electronic Banking services in accordance with the applicable legal regulations, acts of the Bank that regulate payment transactions. It also undertakes to initiate transactions in accordance with the law and guarantees the accuracy of the data entered into the order, and bears full responsibility in case of entering incorrect data.

The payment order will be executed within the deadline and in accordance with the Bank's business policy and practice, as well as in accordance with the applicable Law on Payment Systems.

The Bank will execute only authorized payment orders of the User relating to his account opened under the Agreement, exclusively within the available account balance. The Bank will manage the account and execute payment transactions, in accordance with the legal and other positive regulations applicable in Montenegro.

The Bank enables the Beneficiary to determine the maximum amounts of the limit for the purpose of executing instant credit transfers, i.e. to determine the maximum daily amount for the execution of all instant credit transfers or the maximum amount for each instant credit transfer, which cannot be higher than the limit set by the Central Bank of Montenegro or the Bank. The User may at any time, before initiating an instant credit transfer, change the above limits via electronic banking.Transactions from an account in the country to an account abroad are carried out in accordance with international standards and in accordance with the regulations and acts of the bank that regulate international payment transactions. The user is obliged to submit to the Bank the necessary supporting documentation that represents the basis of the transaction (invoice, pro-invoice, contract, order, etc.) via e-mail payments@adriaticbank.com with attached scanned copies of the above documentation TheUser is responsible for the identity of the data from the previously sent order and documentation and the later submitted documentation. In the event of disagreement or non-submission of the above-mentioned documentation, the Bank has the right to suspend the execution of the next order, until the submission of the documentation for the previously executed order.

Orders for the execution of national payment transactions are executed from the payer's BBAN account through the RTGS system or DNS system in accordance with the Decision on the minimum value of payment transactions that must be processed in the RTGS system, or through the TIPS Clone system in the form of an instant credit transfer.

A national payment order executed through the RTGS or DNS system must contain the following legally prescribed elements: the name of the payer, the payer's transaction account, the payee's name, the payee's transaction account, the purpose of the payment, the payment code, the model and reference number of the debit and payment authorisation, the amount of the payment and the currency of the payment.

An order for the execution of a national payment transaction executed through the TIPS Clone payment system, instant credit transfer, must contain the following elements: information about the payer, the payer's transaction account, the name of the payee, the payee's transaction account, the purpose of the payment, the payment code, the amount and currency of the payment, a description of the payment, and optionally additional data can be entered: Actual debtor, Final recipient and LEI code. When executing an instant credit transfer, the payee's payment service provider makes the funds available to the payee within 10 seconds and confirms the execution of the credit transfer. Instant credit transfer is made instantly, 24 hours a day every calendar day (24/7).

At the request of the User, the Bank enables the determination of limits related to the execution of instant credit transfers. Limits are defined in two groups:

- per transaction, and/or
- A daily limit for all instant credit transfers.

The User may define, amend or abolish the limits referred to in paragraph 1 of this Article via electronic banking or at a branch of the Bank at any time prior to initiating the instant credit transfer payment order. The user cannot set limits for making instant credit transfers above a predefined limit. The predefined limit is the maximum amount per individual transaction for the execution of an instant credit transfer, which is defined by the Central Bank of Montenegro or alternatively set at the client level by the Bank.

An international payment order is executed from the payer's IBAN account via the SWIFT or SEPA payment scheme and must contain the following elements: information about the payer, the payer's transaction account from which the payment is made, information about the payee, the payee's transaction account, the payment amount and currency, the purpose of the payment, the SWIFT (BIC) of the payee's bank and the applicable cost payment option. In the case of international payments made via the SEPA payment scheme, additional data can optionally be entered: Actual Debtor, Final Recipient and LEI code. The order must be signed by the client's authorized persons, with the appropriate documentation necessary for execution (e.g. contract, invoice/pro-invoice, decision, statement, etc.).

The Bank is not responsible for the User's orders that are rejected in the payment system, due to the User's error, nor is it responsible for the execution of an incorrectly completed order.

The Bank does not take responsibility for the unavailability of the Electronic Banking service that occurred as a result of technical problems on the user's computer equipment or phone, outages or interferences in telecommunication channels, power system failure or as a result of force majeure, i.e. for other circumstances beyond the Bank's control.

The Bank has the right, if it suspects that there is abuse, to temporarily block the provision of the remote access service to the Bank's accounts and to notify the User thereof. The Bank has the right to unilaterally suspend the provision of remote access to accounts if the User does not comply with all the provisions of the Agreement stipulating the use of electronic banking and other acts of the Bank. The User may request a temporary suspension of the provision of certain services of remote access to the Bank's accounts by submitting a written request at any branch of the Bank.

The Bank is not responsible for the User's orders that are rejected in the payment system, due to the User's error, nor is it responsible for the execution of an incorrectly completed order.

The Bank prescribes a time frame for sending orders during the banking day, and orders sent after the time frame will be processed with the currency of the next business day, unless the User chooses the currency of the transaction of his choice. Exceptionally, the time frame of the banking day does not apply to instant credit transfers, but such orders are executed within 10 seconds, regardless of the time of day they are initiated. A payment order that is sent electronically and received by the Electronic Banking service has legal force as well as a paper payment instrument signed by hand. The Bank guarantees that all properly sent orders are recorded and stored by computer in accordance with the law.

13. CANCELLATION AND REVOCATION OF PAYMENT ORDERS

The user cancancel the payment order through the Electronic Banking application in the part of the payment order review, provided that the account is not authorized. Authorized national accounts may be revoked by the user, i.e. the authorization may be withdrawn, provided that the Bank has not executed the payment order, that the order was placed via electronic banking and that it is not an instant credit transfer for which it is not possible to withdraw the authorization.

Upon execution of the national payment order, the irrevocability of the payment order shall be deemed to have arisen.

Andas a user, we initiatealog for payment , and we do not have the means to perform it At the same time , the Bankshallstart to implement the J a n a n n g when the Bank is used to Ganje d t a t a t i on o f the r v reme n g e n g o n g o d 30 d a na na n a l g e n o n g p On the other hand, the U.S. Navy and the International Transport Industry Project. The Bank of Applied Sciences is an additional part of the work in the above-mentioned hands, It is believed that the Prophet (peace and blessings of Allah be upon him) said that the Prophet (peace and blessings of Allah be upon him) and the Prophet (peace and blessings of Allah be upon him) And the U.S. Navy is a good fit for the U.S. Senate .

If the User initiates an instant credit transfer and there are no funds available in their account to execute the payment transaction, the Bank will notify the User that there are insufficient funds in the account and will not receive an instant payment order.

If the User initiates an instant credit transfer, and the amount of the order exceeds the maximum amount of the User's limit set for instant credit transfers (daily and/or per transaction), the Bank will refuse to execute the payment order, of which it will notify the User and inform him how to change the maximum amount. Authorized international accounts can also be revoked by the user after the payment order has been executed. For international payments made via SWIFT, the Bank will send a request for reversal of the payment to the correspondent bank.

In the case of international payments to SEPA member states made through SEPA payment schemes, the user may request the revocation of the payment, which must be made within 10 working days or within 13 months in the case of fraud. Also, the beneficiary may request a refund of the payment funds, which must be initiated by the Bank to the bank of the payee, and it must be made within three working days from the date of payment.

Upon acceptance of the revocation by the recipient's bank, the Bank will refund the funds to the payer's transaction account. In the event that the recipient's bank does not approve the request for revocation, the Bank will notify the Client of the rejection of the revocation, stating the reason for the refusal.

If a payment transactionis initiated through the payee, the User may revoke the payment order.

In the eventthat the User does not make additional funds available to the Bank, a reservation will be made on the account for the amount of the previously entered payment order. In order to free the account from the reserved funds, the User must revoke the payment order on their own initiative, through the Bank's application.

14. RESPONSIBILITY OF THE BENEFICIARY AND THE BANK

The user is obliged to keep the devices and data for authentication and authorization in such a way as to prevent their damage, destruction, loss, theft and bears all the risk of its misuse.

The user is responsible for ensuring the confidentiality and security of any user identification and accepts full responsibility for all obligations arising in connection with his user identification.

The user is obliged to immediately notify the Bank of unauthorized use of his user identification, as well as of any other form of security breach.

The user is obliged to have a licensed operating system on the computers or smartphones from which he will use electronic banking services. The Bank is not responsible for non-execution of orders due to an unlicensed and improperly configured operating system and improper use of Electronic Banking.

The User agrees that for services and transactions processed through Electronic Banking, the Bank charges a commission in accordance with the Bank's Tariffs and/or the provisions of the applicable Product Catalog.

Any damage caused by non-compliance with these provisions shall be borne by the User.

If the execution of unauthorized payment transactions is the result of the use of a lost or stolen payment instrument or misuse of a payment instrument, the User may be obliged to bear losses related to these unauthorized payment transactions up to a maximum of 50 euros.

The user is not obliged to bear losses up to the amount referred to in the previous paragraph, if:

1) the loss, theft or misuse of the payment instrument could not have been detected before the unauthorised payment transaction was executed;
2) unauthorised payment transactions are the result of an act or omission of an employee, agent or branch of the payment service provider or a person to whom the activities of the payment service provider have been outsourced;
3) the payment service provider has failed to provide adequate means to notify the loss, theft or misuse of the payment instrument, in accordance with the provisions of the Payment System Act;
4) the payer's payment service provider does not require reliable customer authentication;
5) the payee's payment service provider fails to apply the required customer authentication requirement.

The payee or the payee's payment service provider who fails to apply the required reliable customer authentication shall be obliged to compensate the payer's payment service provider for the damage suffered as a result.

Notwithstanding the previous paragraph, the User shall bear all losses associated with unauthorised payment transactions, if the payer has acted with the intention of fraud or has intentionally or grossly negligently failed to fulfil one or more obligations and to use the payment instrument in accordance with the terms and conditions of issue and use of that payment instrument set out in the contract, which must be objective. non-discriminatory and proportionate and/or immediately upon becoming aware of the loss, theft or misuse of a payment instrument, i.e. its unauthorized use, notify the Bank or a person designated by the payment service provider.

The User shall not be liable for the amount of unauthorized payment transactions made after immediately notifying the Bank or a person designated by the payment service provider upon learning that the loss, theft or misuse of the payment instrument has occurred, i.e. its unauthorized use, unless he acted with the intention of fraud.

The Bank is not responsible for the quality, delivery or legal and material defects of the goods and services purchased by the User. Such a dispute is primarily resolved by the User with the merchant, without affecting the obligation to settle a duly executed card transaction, unless otherwise determined by the regulations or rules of the card organization.

15. FEES AND COSTS

The User pays fees, commissions, membership fees and costs according to the valid Tariff and the contracted product.

Fees may be one-time, periodic, transactional, fixed, or percentage-based and may relate to issuance, personalization, delivery, urgent production, exchange, reissue, use, certificates, tokens, shutdown, or other services.

The User authorizes the Bank to collect the due obligations by debiting the appropriate account, i.e. the User's second account with the Bank, in accordance with the contractual documentation and regulations.

The tariff is available at the Bank's branches, on the website and through other distribution channels.

16. NOTIFICATIONS, PERFORMANCES AND COMMUNICATION

The Bank delivers notifications via a durable medium, branch, website, mail, e-mail, SMS, mobile or web application or other agreed channel.

The user is obliged to regularly monitor the statements, traffic review, push messages and other notifications and to report irregularities without delay.

The user is obliged to provide the Bank with accurate and up-to-date address and contact information. The Bank is not responsible for the consequences of failure to deliver the notification if it was sent on the last reported data or if the delivery is prevented for reasons beyond the control of the Bank.

Promotional messages are delivered by the Bank only in accordance with the given consent and applicable regulations.

17. COMPLAINTS AND COMPLAINTS

17.1. Types of Addresses

The beneficiary may submit:

- objection to the Bank's conduct, product or service;
- a complaint or a request to contest a card transaction;
- reporting an unauthorised or incorrectly executed payment transaction;
- reporting a problem at an ATM or payment device;
- a complaint to a trader about the quality or delivery of a good or service.

A complaint against the Bank and a complaint about a card transaction are not the same procedure and may have different deadlines, forms, evidence and decision-making rules.

17.2. Complaint of a card transaction

The user is obliged to keep the slip, receipt, order confirmation, correspondence with the merchant and other documentation that may be necessary for the complaint.

A complaint shall be filed without delay upon learning of the disputed transaction and within the deadlines prescribed by the law and the rules of card organizations, on the Bank's form and with the available evidence.

The bank checks whether the transaction is authenticated, authorized, properly recorded and booked and whether the execution has been affected by a technical failure.

The process may depend on the Visa/Mastercard policy, the processor, the merchant and the accepting bank. Provisional approval of the account, if made by the Bank during the procedure, does not constitute a final decision. If it is subsequently determined that the complaint is not founded, the Bank may re-debit the account and charge the costs according to the Tariff.

Filing a complaint does not release the User from settling other due obligations under the Card.

17.3. Unauthorized Transaction

If the User claims that he did not approve the transaction, he is obliged to immediately report it to the Bank and take measures to block the Card or service.

The Bank will refund an unauthorized transaction within the deadlines and under the conditions prescribed by law, except when there are reasonable grounds to suspect fraud or other legal exceptions.

17.4. The ATM did not withdraw cash or retained the Card

If the account is debited and the ATM has not withdrawn cash or has withdrawn an incomplete amount, the User shall notify the Bank without delay and provide the date, time, location of the ATM, the amount and other available information. The bank verifies the transaction through the available electronic records and, when necessary, initiates proceedings against another bank or card organization.

If the ATM holds the Card, the User should contact the Bank immediately. The return of the Card depends on the status of the Card, the reason for the retention, the owner of the ATM and security rules. A card retained at an ATM of another bank can be returned only after verification and consent of the issuing bank, and if a refund is not possible, the User submits a request for a new Card.

17.5. Dispute with the trader

Complaints about quality, quantity, delivery, cancellation or return of goods and services are primarily resolved by the User with the Retailer. The Bank may initiate a card complaint procedure only when the conditions of the card organization are met and when the User submits the necessary evidence.

17.6. Complaint against the Bank

The User may file a complaint in person, by mail or electronically, through the channels published on the Bank's website. The objection should include identification data, a brief description, a request and available evidence.

The bank responds within 8 working days. If the User is not satisfied with the answer, the User may use protection before the Central Bank of Montenegro, the Alternative Dispute Resolution Body and the competent court, in accordance with the regulations.

18. DAMAGE, LOSS, THEFT, MISUSE AND BLOCKING

The loss, theft, compromise or unauthorized use of the Card, telephone, token, certificate or credential must be reported by the User without delay through the Contact Center, branch office or other channel designated by the Bank.

Upon receipt of the application, the Bank will block the appropriate instrument or service in accordance with the technical possibilities. The time of registration is considered to be the time when the application is registered with the Bank.

If the User finds the Card after reporting a loss or theft, he/she must not use it, but must act according to the Bank's instructions.

In case of suspicion of theft or fraud, the Bank may require a report to the competent authority and the submission of appropriate documentation.

19. RENEWAL, REISSUE, REPLACEMENT AND TERMINATION OF THE CARD

The card can be used until the last day of the month specified as the validity period. The Bank may automatically reissue the Card when the criteria specified by the type of product, contractual documentation and internal rules are met.

If the User does not wish to reissue, he is obliged to notify the Bank at least 30 days before the expiry of the Card.

The Bank may refuse to reissue or replace the Card, in particular due to the status of the account, outstanding obligations, inactivity, security or regulatory reasons.

In the case of a credit Card, the termination of the basic Card may result in the termination of all additional Cards. All liabilities incurred prior to termination shall remain in force until final settlement.

Unclaimed, reissued and replacement Cards are subject to clause 6.4 of these General Terms and Conditions.

20. RESTRICTIONS, BLOCKADES AND TEMPORARY SUSPENSION OF SERVICES

The Bank may restrict, block or suspend the use of the Card or electronic service due to:

- the security of the payment instrument or service;
- suspected unauthorized use, fraud or compromise;
- increased risk that the User will not settle its obligations;
- Unpaid obligations;
- the expiration of an identification document or non-up-to-date data;
- acting contrary to the contract, these General Terms and Conditions or regulations;
- legal, regulatory, sanction, AML/CFT or other mandatory reasons.

The Bank shall notify the User before or immediately after the blockade, except when the notification would be contrary to the regulations or objectively justified security reasons.

The Bank will unblock the instrument or allow the exchange when the reasons for the blocking cease to exist and when the Bank's conditions are met.

Access to the account of the PIS or AIS service provider may be denied only for proven and objectively justified reasons related to unauthorized access or fraud, in accordance with the law.

21. CANCELLATION OF THE USE OF SERVICES

The User may cancel the Card, electronic banking, Office Banking, SMS/Email info or other service by submitting an appropriate request to the Bank.

Deletion of the application, termination of use, return of tokens or absence of transactions does not constitute a cancellation of the service if the Bank has not received and implemented the request for cancellation.

Cancellation does not release the User from the obligation to settle all transactions, interest, fees, membership fees and other obligations incurred until the termination of the service.

The card whose use has been cancelled must be returned to the Bank or destroyed according to the Bank's instructions. An additional Card may be cancelled at the request of the Basic User or its User.

In the case of legal entities, the Bank must be immediately notified of the termination of the authorization of an individual user, the change of representative or the right to sign.

The Bank may cancel the service in cases prescribed by the contract, these General Terms and Conditions and the law.

22.AMENDMENTS TO THE GENERAL TERMS AND CONDITIONS

The Bank may amend these General Terms and Conditions, notifying the User at least two months before the proposed date of application, through a durable medium or other permitted channel.

If the User does not agree, the User may cancel the service to which the change relates before the start of the application of the changes, with the settlement of all obligations.

If the User does not cancel the service by the day of application, it is considered that he has accepted the changes, when such an assumption is allowed by regulations and contractual documentation.

Changes resulting directly from the law, decisions of the competent authority, rules of the payment or card scheme may be applied from the date specified by that act, with the notification of the User in the prescribed manner.

23. FINAL PROVISIONS

These General Terms and Conditions for the use of payment cards and electronic banking services apply to legal entities and natural persons.

The provisions of these General Terms and Conditions for the Use of Payment Cards and Electronic Banking Services (Version 1.1) relating to the service of instant credit transfers (TIPS Clone) shall apply from the date of publication on the official website of Bank www.adriaticbank.com.

The provisions of the Terms and Conditions for the Use of Payment Cards and Electronic Banking Services (Version 1.0) are contained (integrated) in these General Terms and Conditions (Version 1.1) and will begin to apply within two months from the date of their publication on the official website of Bank www.adriaticbank.com.

Until the beginning of application of the provisions of the General Terms and Conditions from the previous post, the provisions of the GENERAL TERMS AND CONDITIONS FOR THE ISSUANCE AND USE OF PAYMENT CARDS ADRIATIC BANK AD PODGORICA and the GENERAL TERMS AND CONDITIONS FOR THE USE OF ELECTRONIC BANKING SERVICES shall apply, except for the provisions relating to the instant credit transfer service (TIPS Clone), to which the provisions of these General Terms and Conditions referred to in paragraph 1 of this Article shall apply.

With the beginning of the application of these General Terms and Conditions for the Use of Payment Cards and Electronic Banking Services, the provisions of the GENERAL TERMS AND CONDITIONS FOR THE ISSUANCE AND USE OF PAYMENT CARDS ADRIATIC BANK AD PODGORICA and the GENERAL TERMS AND CONDITIONS FOR THE USE OF ELECTRONIC BANKING SERVICES shall cease to be valid