CARD USAGE AND SECURITY RULES*

1. In order to prevent unlawful use of the Card by third parties, the Cardholder undertakes to strictly observe the following rules:
1.1. ensure the confidentiality of the Card data and the PIN code (for Visa Digital/Mastercard Digital First cards, if such a code exists), for which purpose it is recommended to destroy the receipt containing the PIN code (if any), take all possible measures to keep the Card data and/or the PIN code inaccessible to other persons or recording devices, not write down the PIN code on the Card or in a phone or computer and not keep it together with the Card or in any other place accessible to third parties, and not provide the Card or the PIN code to other persons, including Bank employees,
1.2. ensure the confidentiality of the password registered with the Bank,
1.3. ensure the confidentiality of the password for the email address registered with the Bank,
1.4. ensure the confidentiality of the Card verification code,
1.5. ensure the confidentiality of the 3D Secure security code sent to the Cardholder,
1.6. when making a transaction with the Card, carefully check the accuracy of the amount stated on the receipt and only then sign it,
1.7. when making payments on the Internet, use only websites whose addresses begin with the "https" prefix or that use the "Secure Sockets Layer (SSL)" cryptographic protocol.

2. In the event of loss or theft of the Card or the Card data, or of an attempted fraud or a fraudulent transaction involving the Card, the Cardholder undertakes to:
2.1. block the Card through the acba digital internet banking system or, to have the Card blocked, immediately visit the nearest branch of the Bank and submit a Card blocking application or call (+374 10) 31 88 99, (+374 10) 31 88 88 or (+374 10) 59 22 22,
2.2. after blocking the Card, contact the Bank to have the Card replaced or closed,
2.3. return the Card to the Bank, if available.

3. The Bank has the right to block the Cardholder's Card without notifying the Cardholder in cases of a risk of fraudulent transactions or suspected fraud. The Card may be unblocked only after the suspicion of fraud has been cleared and if

the Cardholder confirms, orally or in writing, having made the transactions in question, except in cases where there is a suspicion and/or risk of fraudulent transactions being made by the Cardholder personally and/or with the Cardholder's knowledge or participation.

4. Upon the Cardholder's written or oral request, the Bank may notify the Cardholder of transactions made with the Card (including cases where a transaction dispute, a refund or any other transaction has resulted in the transaction amount being returned to the Account) by sending SMS messages to the primary mobile phone number registered with the Bank, for which the Bank charges the Cardholder's Account the fee established by the Bank's Tariffs. If the necessary funds in the Account are unavailable or insufficient, the fee is charged to the unused credit line (if any). If there is no unused credit line or it is insufficient, the fee amount is recorded as overspending.

5. SMS messages are sent to the Cardholder for transactions above the amount threshold selected by the Cardholder. However, when the Bank charges fees or makes other charges established by the Tariffs, the uniform minimum threshold set by the Bank applies, which is AMD 200 for AMD cards, USD 1 for USD cards and EUR 1 for EUR cards.

6. When the Cardholder is notified that the amount of a completed transaction has been returned (released) to the Account, or when SMS messages are sent for transactions declined with decline codes predefined by the Bank, the minimum threshold selected by the Cardholder does not apply.

7. The Cardholder undertakes not to modify or damage the Card. (This clause does not apply to Visa Digital/Mastercard Digital First cards.)

***When concluding a contract with a consumer, the Bank is obliged to make these terms available to the consumer. They are included in the "Terms and Conditions for the Issuance and Servicing of Cards" document available on the Bank's official website.**