Converse Bank CJSC FO 72-03-07-1 Rules of Card Issuance and Use Edition 7

Rules of Card Issuance and Use

1/7

1. Definitions

- 1.1. Bank Converse Bank CJSC.
- 1.2. Payment system the set of general rules, procedures and the supporting software tools defined and developed by the payment organization, based whereon the Bank issues cards, provides services and/or accepts cards as a means of payment. The Bank issues and services the cards of the following payment systems: Visa, Mastercard, UnionPay and ArCa.
- 1.3. Card(s) Payment cards issued under the payment systems with the participation of the Bank, by means of which the Cardholder may credit and debit cash to the Card Account based on the terms and conditions set for the particular service/card type, make transfers and payments within the Credit Limit at the cash-out or trade and service points of the particular Payment System.
- **1.4.** Rules Rules for issuance and use of cards.
- 1.5. PIN code Personal Identification Number (PIN) applied to identify the Cardholder in certain transactions.
- **1.6. Agreement** the agreement and/or an offer accepted by the Cardholder to enter into an agreement on issuance, service and use of payment cards.
- **1.7. Cardholder** any person eligible to use the Card under the Agreement with the Bank.
- 1.8. Accountholder Cardholder any party to the Agreement eligible to use the Card.
- **1.9. Card Account** an account opened with the Bank on behalf of the Cardholder, and the cash available on the latter may be disposed by using the Card.
- **1.10. Credit Limit** Credit line/overdraft (based on specific agreement) provided by the Bank to the Cardholder, which can be used for transactions with the Card/through the Card Account.
- 1.11. Payment Limit the total sum of the card account balance and the Credit Limit, which can be used by the Cardholder.
- **1.12. Card Transaction** a transaction, where the Card is used to make payments for goods and services, to withdraw cash or to make transfers.
- **1.13. Transaction Day** the actual day of making the Transaction.
- 1.14. Transaction Record Day the day of recording the Transaction on the Cardholder's account with the Bank based on the submission of the Transaction to the Bank for registration by the Payment System servicing the Card.
- **1.15. Point of Sale/Service** (POS) a point of sale of goods/provision of services, including in the internet environment, where the payment for the sold goods/provided services can be made with Cards.
- 1.16. Automated Teller Machine (ATM) an automated self-servicing machine for financial transactions in or out of the office.
- **1.17. Authentication** the Bank's permission or approval for the card transaction.
- **1.18. Expiration Date** 24:00 of the final day of the period stated on the Card.
- **1.19. Overlimit** in specific cases, depending on the place of use of the Card and the nature of the Transaction, exceeding the Payment Limit of the Card due to one or several Transactions. A penalty is charged against the overlimit based on the tariffs and rates of the Bank.
- **1.20. Linked Card** an additional Card issued under the same Card Account.
- **1.21. PRIORITY PASS Card** a pass issued to the Cardholder together with the Bank's Visa Platinum/Visa Signature/Visa Infinite Card, which provides the Cardholder access to the VIP zones of the airports.
- **1.22. Offline Transactions** transactions that do not need online Authentication.
- **1.23. Debit Card** a card to be used to withdraw cash and to make cashless transactions within the cash limit available on the Cardholder's Card Account.
- **1.24.** Credit card a card to be used to withdraw cash and to make cashless transactions within the cash limit available on the Cardholder's Card Account and/or the credit line/overdraft provided by the Bank.
- 1.25. Loan Card a card to be used to withdraw cash and to make cashless transactions within the credit limit provided to the Cardholder. Furthermore, the same rules are applied to the sums credited in excess of the used amount of the Credit Limit and the sums used from the Credit Limit.
- **1.26. Card Blocking** suspension/banning of online Authentication of the Card.
- 1.27. Freezing of Card Account full or partial restriction of debit/credit transactions on the Card Account.
- 1.28. 3D Secure "Verified by Visa", "MasterCard SecureCode", "UnionPay 3-D secure" and other security systems providing two-factor authentication when authenticating card transactions in online/electronic domain. The cards issued by the Bank are 3D Secure.

© CONVERSE BANK	Converse Bank CJSC	FO 72-03-07-1	
	Rules of Card Issuance and Use	Edition 7	2/7

- **1.29. 3D Secure password** a one-time password sent by the Bank to the Cardholder with SMS on the mobile number or by email to authenticate the Transactions in online/electronic domain.
- **1.30. One-time Password (OTP)** a one-time password sent with SMS on the Cardholder's mobile number registered with the Bank, which is used to create the PIN code through ATM and to activate the Card, to activate the Token created by the Cardholder and in other cases as a means to identify the Cardholder.
- **1.31.** CVV/CVC Code a three-digit code on the reverse side of the card to be used when executing Transactions in online/electronic domain.
- **1.32. Password** the Cardholder identification code used by the Cardholder to receive information about the Card and the Card Account, and in cases determined by the Bank (do not confuse with the PIN code of the card).
- **1.33. Tokenization** adding the Card to e-wallets that allow Token payments.
- 1.34. Token the digital equivalent of the card created as a result of Tokenization of the card. The Payment Systems ensure the security of the Cardholder's card data in the process of Tokenization. It is a combination of symbols to which the Card data are encrypted. The last 4 digits of the Token number are printed on the receipt when making transactions with a Token.
- 1.35. Tariffs the tariffs and rates published on the Bank's website and/or fixed in the Agreement.

2. Card Issuance / Reissuance Terms

- 2.1. The Card Account is opened to make transactions with the Card and the Card Account. The Card is issued under the Card Account.
- **2.2.** The Bank may return the Card and close the Card/Card Account unless the Cardholder receives the Card in 1 month after the issuance of the Card.
- **2.3.** The Card is the ownership of the Bank,
- **2.4.** When the Card is handed over to the Cardholder, the latter has to sign in the signature field on the reverse side of the Card. The absence of signature or its variance from the Cardholder's ID card disclosed by the Cardholder and containing the latter's sample signature shall be deemed a legal ground for refusal to service the Card and for seizure of the Card without compensation.
- **2.5.** The Pin code is needed to make the following Transactions with the Card:
 - cash withdrawal from ATM,
 - non-contactless transactions on POS terminals,
 - contactless transactions on POS terminals in excess of the limit set by the Payment Systems.
- **2.6.** The PIN code of the newly issued/re-issued cards is provided in any manner listed below:
 - by the Customer through Converse Mobile app (the App) from the respective Card settings by following the instructions in the set order, after which the Card is activated and can be used for Transactions;
 - by the Customer through the ATM of any ARCA member bank by applying the OTP. The Customer should follow the instructions on the ATM screen by entering the assigned OPT in the respective field and thereafter setting the PIN code, after which the Card is activated and can be used for Transactions. The Cardholder should apply to the Bank unless they receive the OTP in the set time;
 - at the Cardholder's discretion, by issuing the pre-set PIN code, in which case the PIN code envelope is provided to the Cardholder together with the Card. The PIN code is printed in one copy and is handed over to the Cardholder in a sealed envelope, and the Card is activated by the Bank once the delivery of the Card is approved.
 - **2.6.1.** The Bank recommends rather than using subsequent or repeated numbers, apply a complex numerical combination when setting a new PIN code of the Card.
 - **2.6.2.** The Cardholder is responsible for safekeeping the PIN code of the Card.
 - **2.6.3.** The Cardholder may prefer to change the PIN code from the respective Card settings in the App or through the ATM with the relevant option by following the sequence of actions.
 - **2.6.4.** If the Card PIN code is forgotten/lost, the Cardholder may set a new PIN code through the App or by requesting the Bank to reset the PIN code, after which the PIN code may be set in one of the manners listed in paragraph 2.6 above. At the Cardholder's request, the Bank can as well reissue the Card with a new PIN code by charging the fee if required under the Tariffs.
 - **2.6.5.** If the PIN code is set through the App, the non-contactless transactions with the Card on POS terminals can be executed after the Card is used at the ATM of any ARCA member bank.
 - **2.6.6.** Upon mistype of the PIN code for three subsequent times, the Card is automatically blocked and/or can be seized.
- 2.7. Before the expiry of the Debit Card, within the final 15 days prior to the Expiration Date the Bank can reissue the Card for an effective period established by the Bank at the particular date, without seeking the additional

© CONVERSE BANK	Converse Bank CJSC	FO 72-03-07-1	
	Rules of Card Issuance and Use	Edition 7	3/7

approval of the Cardholder, provided that the Cardholder meets the requirements set under the internal regulations of the Bank.

- 2.8. Unless the Cardholder meets the requirements set under the Bank's internal regulations, and where the Cardholder gives a written notice on refusal form the Card at least 15 days prior to the Expiration Date of the Debit Card, the Card is recognized invalid from the Expiration Date and is to be returned to the Bank within 5 days from the Expiration Date or to be destroyed by the Cardholder (the Card needs to be cut into small pieces so that the data become unreadable), and the Cardholder shall bear the consequences of default.
- **2.9.** The Pension Card issued under the social security accounts is reissued based on the reissuance application of the Cardholder.
- 2.10. The payment cards are reissued subject to meeting the requirements of the internal regulations of the Bank.
- **2.11.** The Cardholder should take measures to prevent the access of the Card data to third parties and the unauthorized use of the Card.

3. Linked Card

- 3.1. Based on the Cardholder's application, the Bank may issue one or several Linked Cards on behalf of individuals determined by the Cardholder. In such case, the Accountholder Cardholder should disclose reliable information about the Linked Cardholders to the Bank.
- 3.2. Only the individual on behalf whereof the Linked Card is issued may use the latter.
- **3.3.** The Accountholder Cardholder should introduce the Rules and the basic terms of the Agreement to the Linked Cardholder.
- 3.4. The Rules, as well as the provisions of all bylaws and internal regulations of the Bank are applied to the Linked Cards.
- **3.5.** The Transactions with Linked Cards are executed within the scope of the Credit Limit and are reflected in the Card Account statement based on the Rules; furthermore, the Accountholder Cardholder may set a monthly limit or any other restriction for the transactions with Linked Cards.
- 3.6. The Linked Cards are closed when the Card is closed.
- **3.7.** The Accountholder Cardholder is responsible for the Transactions, including the Overlimit of the Linked Cardholder.

4. Use of Card

- **4.1.** The Cardholder cannot transfer the Card and the PIN code to third parties.
- **4.2.** It is prohibited to write the PIN code on the card.
- **4.3.** The PIN code is not needed for Transactions in the internet environment, nor is required by any Payment System, therefore it is prohibited to enter the PIN code in the particular domains. If entered/disclosed, the Cardholder should immediately stop the Transaction and inform the Bank to have the Card blocked.
- **4.4.** When using the card the Cardholder should enter the PIN code so that it is not seen by a third party and is not videotaped through any device.
- **4.5.** The Cardholder might need to sign the receipt by checking the Transaction amount, when making payment at POS or withdrawing cash.
- 4.6. The PIN code is not needed for contactless Transactions below the limit set by the Payment Systems.
- **4.7.** The Bank sets daily limits for the number and amount of cash withdrawals and/or cashless Transactions per card in its Tariffs. The limits can be changed by the Cardholder in accordance with the internal regulations of the Bank through the App or by filing a request with the Bank.
- **4.8.** The Transaction amount is deemed withdrawn from the Card Account on the Transaction Record Day. Depending on the POS and the type of Transaction, the Transaction may be recorded within 30 calendar days. The Transaction amount is withdrawn from the Card immediately, and is usually recorded in the Card Account and reflected in the Card Account statement on the following dates:
 - on the next business day for Transactions in ARCA system,
 - in 2-3 business days for Transactions out of ARCA system.
- **4.9.** The Cardholder may credit cash or cashless funds to the Card Account in person or through a third party assigned thereby, as well as elsewise, through other banks, including foreign correspondent banks.
- 4.10. The Bank disclaims the responsibility for the potential loss of the Cardholder due to temporary interruption or delay in the availability of funds on the Cardholder's Card. In particular, the Transaction amounts may be made available on the card on a later date due to technical or software problems through no fault of the Bank, as well as in the first 3 business days of every month.
- **4.11.** The funds may be credited to the Card Account in the manner set by the Payment Systems (c2c transfer, ewallet-to-card transfer, cash-in through ATM, etc.), in which case the amount transferred to the Card may be

© CONVERSE BANK	Converse Bank CJSC	FO 72-03-07-1	
	Rules of Card Issuance and Use	Edition 7	4/7

made available immediately or in the period set by the Payment Systems for the particular cash-in manner. The amount is deemed credited to the Card Account on the Transaction Record Day.

- 4.12. The exchange rates may vary at the point of Authentication and the actual recording if the Transaction is executed in a currency other than the currency of the Card Account. The exchange rate set by the respective Payment System is applied at the point of Authentication of the Transaction, and the exchange rate set by the Bank at the end of the banking day preceding the record of the Transaction is applied when recording the Transaction. For international Transactions (outside Armenia and/or at POS serviced by a foreign bank) executed with VISA cards in foreign currencies other than USD and EUR, the Transaction currency is converted into USD at the exchange rate set by the Payment System, and USD is exchanged with the Card Account currency in the amount of the Transaction at the exchange rate set by the Bank at the end of the banking day preceding the Transaction Record Day. The Bank may set and apply the relevant fee for these Transactions under its Tariffs that are published in the Bank's website. The Bank disclaims the responsibility for the currency and other risks related to the difference in exchange rates.
- **4.13.** The charges or double charges from the customer's Card Account due to software or communication failures of the Bank, as well as through the fault of the Bank employee are refunded to the customer's Card Account in 1 business day after the problem is made known to the Bank.
- **4.14.** The Rules and Tariffs contain provisions regulating the Card issuance and service relationship with the Bank. Nonetheless, the Payment Systems may have specific limits and other rules for specific types of Card Transactions, and the Bank and the Cardholder should follow the latter as well. The Bank disclaims the responsibility for the Cardholder's loss incurred due to the failure thereof.
- **4.15.** The Card cannot be used for any illegal action or the related Transactions. In the presence of any doubt about the lawfulness of the Card Transaction, the Bank may ban the Transaction and/or block the Card and/or freeze the account without notifying the Cardholder. Furthermore, the Bank may request additional information and documents from the Cardholder prior to permission of the respective Transaction.
- **4.16.** Prior to executing any Transaction with the Card in online/electronic environment, the Cardholder should review the details of subscription, purchase, shipping, cancellation of Transaction, return of goods and availability of contacts in the particular site.
- 4.17. When executing a Transaction in online/electronic environment, the Cardholder should use renowned and reliable websites, e-wallets and applications that are furnished with up-to-date security tools, such as Secure Sockets Layer (SSL) certificate, "Verified by Visa", "MasterCard SecureCode", "UnionPay 3-D secure" and the like. The Bank disclaims the responsibility for the failure to receive the 3D Secure code and the consequent disruption of the transaction for any technical reason or any reason unrelated to the Bank's activities.
- **4.18.** We recommend refrain from using the ATMs, cash-out and POS terminals and devices that in the Cardholder's judgment are unreliable or suspicious, as well as when additional devices, cables, adhesive tapes and other suspicious items are connected to the latter's card reader, keyboard or cash dispensing window.
- **4.19.** The Cardholder may appeal the transactions reflected in the Account Statement data within 3 (three) months from the date of generation of the Statement (unless a shorter period is established under the rules of the respective Payment System) by completing the form designed by the Bank and attaching thereto all document supporting the appeal. We recommend promptly inform the Bank upon detecting any non-compliance or any unauthorized transaction.
- **4.20.** The Bank will support the refunding of the sum of the appealed transaction on the Cardholder's Card Account based on the rules of the Payment System, however the Cardholder is not relieved of the obligations towards the Bank when refunding is impossible.
- **4.21.** The conditions, procedures and terms of appealing Card Transaction are established by the Payment Systems.
- 4.22. In response to the appeal, in 90-day period the Bank either recovers the sum of the appealed transaction on the card account or provides a written response to the Cardholder substantiating the impossibility of refund. In specific cases after the Cardholder is duly notified, the written response may be provided or the sum may be recovered beyond 90 days, depending on the rules of the Payment System or other unforeseen circumstances.
- 4.23. The Cardholder has to keep all payment documents relating to the Card Transactions until the receipt of the Card Account Statement, to check the transactions stated in the Statement against the actually made expenses and upon inconsistency inform the Bank thereon in the period set in paragraph 4.19 above. The Bank may decline the appeals filed later than the specified date.
- **4.24.** An Overlimit can generate on the Card depending on the specifics of certain types of Transactions (hotel booking, car rent, services used at tourism and recreation centers, etc.), the timing of disclosure of Transaction by the servicing bank, software problems, cashbacks/chargebacks made by the service point, offline Transactions (in

© CONVERSE BANK	Converse Bank CJSC	FO 72-03-07-1	
	Rules of Card Issuance and Use	Edition 7	5/7

which case the Overlimit may generate in the absence of cash on the Card), the fees set by the Bank, the FX Transactions and the like.

- **4.25.** The Card Transactions should be executed within the scope of the Credit Limit. A penalty is charged for the overlimit against the sum exceeding the limit based on the Tariffs and/or the Agreement. In similar cases, the Card may be blocked until the repayment of the total debt.
- **4.26.** Within 5 (five) days from the date of the Cardholder's written request for termination of the Agreement, the Bank stops servicing the Card subject to repayment of the Cardholder's liabilities to the Bank and the liabilities generated within 45 days from termination of the Card servicing, from the amounts available on the Cardholder's accounts with the Bank. The negative balance on the Card Account is to be paid by the Cardholder within 5 (five) banking days from the date of generation of the negative balance.
- **4.27.** Where the servicing of the Card is stopped, the Cardholder continues to bear liability and responsibility for payment of Transactions that have been executed before the termination of the Card service and/or the handover of the Card to the Bank (destruction).
- **4.28.** The Bank disclaims responsibility for the direct or indirect loss caused to the Cardholder due to the failure to service the Card/the expired Card at any ATM or POS terminal (including those registered in the internet environment) or due to their malfunction.
- **4.29.** The Cardholder has to immediately inform the Bank about any unauthorized use or a threat of such use of the Card in the manner specified in paragraph 6 below and request restricting the use of the Card. The Bank shall bear no responsibility for the Card Transactions executed before notification of the Bank and at the date of the Bank's confirmation of the notice based on paragraph 6 below.
- **4.30**. The Bank disclaims all responsibility for the loss incurred by the Cardholder due to the Card Transactions:
 - **4.30.1.** executed with chip card by entering the Card's PIN-code;
 - **4.30.2.** executed by reading/entering the Card's magnetic tape and/or the Card's chip and/or the CVV2/CVC2 code on the reverse side of the Card, and receiving online Authentication from the issuing bank (even if the signature on the transaction receipt varies from the actual signature of the Cardholder);
 - **4.30.3.** executed offline, if they were executed before the Customer returns the Card to the Bank and/or during the period when the Card was not placed in the international blocking system;
 - **4.30.4.** having 3D Secure Authentication, as well as online transactions executed in 3D Secure sites but not having 3D Secure Authentication.
- **4.31.** The Bank's responsibility for contactless Transactions is established based on the CBA Board Resolution #300-N at 04.11.2014.
- **4.32.** The Bank places the Card in the international card blocking system in the presence of a real threat of an unauthorized use of the Card in a foreign country, in which case the Cardholder has to pay the international blocking fee based on the Tariffs irrespective of the fact whether the card is blocked or closed.
- **4.33.** The Cardholder shall not be responsible for the Transactions executed offline while the Card was placed in the international card blocking system.
- **4.34.** The Bank may ban or restrict the Transactions in high-risk countries for security reasons.
- **4.35.** For the sake of protection of the Cardholder's interests, in the absence of turnover on the Card Account for 6 (six) months and longer, the Bank can unilaterally freeze the Card Account and block the Card without additionally notifying the Cardholder thereon, which by no means shall restrict the Bank's right to charge the respective amounts from the Cardholder's account to repay the Cardholder's liabilities to the Bank.
- **4.36.** The Bank may on its own initiative block the Card and freeze the Card Account, where:
 - **4.36.1.** the Card details (expiry, CVV2/CVC2 code) have been entered incorrectly multiple times while attempting a Transaction;
 - **4.36.2.** the Cardholder has overdue liabilities to the Bank,
 - **4.36.3.** the Cardholder has failed to pay the fees based on the Tariffs in due time,
 - **4.36.4.** the Bank has received a blocking notice from the government authorities,
 - **4.36.5.** the Bank has detected fraudulent transactions due to monitoring,
 - **4.36.6.** in specific cases the Bank may also place the Card in the international blocking system on its own initiative.
- 4.37. The Bank can unblock the Card and unfreeze the Card Account, where:
 - **4.37.1.** the Cardholder has repaid the overdue liabilities,
 - 4.37.2. the Cardholder has paid the fees based on the Tariffs,
 - 4.37.3. the Bank has received an unblocking notice from the government authorities,

© CONVERSE BANK	Converse Bank CJSC	FO 72-03-07-1	
	Rules of Card Issuance and Use	Edition 7	6/7

- **4.37.4.** the Bank has received verbal or written confirmation from the Cardholder denying the fact of fraudulent transactions in response to the findings of the Bank's monitoring related to alleged fraudulent transactions.
- 4.38. The Cardholder has an option to receive SMS from the Bank on credits and debits to their Card, thus preventing the unauthorized use of the Card to the best extent possible. The Bank may set the relevant fee for this service under its Tariffs.
- **4.39.** Once the SMS is received, the Cardholder should make sure that the Transaction has been concluded with their or their authorized representative's knowledge, instruction or involvement.
- **4.40.** The fees for access to VIP zones in the airports with PRIORITY PASS are charged unconditionally from the Cardholder's Card Account, without seeking the Cardholder's additional approval. In the absence of cash on the Cardholder's Card Account, the fee is charged from other accounts of the Cardholder.
- 4.41. The Bank can demand the Cardholder to return the sums paid by the Bank to the Payment Systems for the Card Transactions executed through the Cardholder's fault, as well as upon the loss/theft of the Card before the notification of the Bank.
- **4.42.** The Bank may terminate the Cardholder's subscription to e-commerce and/or virtual service platforms in case of any doubt and/or failure to receive transaction authentication 3 times in a row.

5. Creation and Use of Token

- **5.1.** Visa and MasterCard cards of the Bank can be Tokenized.
- **5.2.** The Token may be created through Converse Mobile app, as well as through specific e-wallets by entering the relevant card data, activating the created Token through OTP or contacting the Bank in the manner specified in paragraph 6.1 below.
- **5.3.** Token payments may be made at all points of sale/service and ATMs having the devices for contactless Transactions with international Visa and MasterCard cards, as well as on online platforms where you can pay with the Token created in the particular e-wallet.
- 5.4. The Token Transactions are equivalent to the Card Transactions that are covered by the Rules.
- **5.5.** You may execute Token Transactions with a mobile phone or the respective device (the Device) where the particular e-wallet is accessible. You may execute Token Transaction subject to identification/approval (password, fingerprint, other bio data, etc.).
- **5.6.** To chargeback the Token Transaction, you should use the Token of the e-wallet with which the initial Transaction was executed.
- **5.7.** The Cardholder may at any time remove the Token from the e-wallet or contact the Bank to have it terminated. The removal of the Token does not change the status of the Card.
- **5.8.** No Token can be created for the blocked/inactive Card.
- **5.9.** Visa and MasterCard payment systems or e-wallets may set upper limits for Token Transactions. In the similar case, the Cardholder can execute the transactions in excess of the upper limit with the Card.
- **5.10.** The Cardholder should ensure the safety of registration and protection of the Device identification tools and prevent their transfer to a third party.
- 5.11. The Cardholder should not disclose the OTP for activation of the Token to a third party.
- **5.12.** Upon the loss/theft of the Device, third-party access to the Token passwords or otherwise making the Token accessible to a third party, you should promptly contact the Bank to have the Token blocked. The Bank disclaims the responsibility for the loss caused to the Cardholder due to the failure to inform the Bank in due time.
- **5.13.** When replacing the Device, the Cardholder should make sure that the Tokens are detached from the replaced Devices or call the Bank to be advised about detaching the Tokens.
- **5.14.** The Token is also blocked if the Card is closed or blocked based on paragraph 4.36 above. In all other cases the Token is blocked only if the Cardholder calls the Bank or removes the Token from the e-wallet.

6. Unauthorized use, loss or theft of Card/Token

- 6.1. The Cardholder should immediately take actions to block the lost, stolen or unauthorized use of the Card/Device, in particular in any manner listed below:
 - 6.1.1. Block the Card from the respective Card settings in the App;
 - 6.1.2. Call Converse Bank CJSC (+37410) 511211, (+37412) 444444 24/7 and make a verbal request, whereafter the Card is blocked after the Cardholder is identified;
 - 6.1.3. Call the phone number printed on the Card and make a verbal request, whereafter the Card is blocked after the Cardholder is identified;
 - 6.1.4. Send an appropriate written message at <u>card@conversebank.am</u>, through the App chat, or file a written request through Internet-Bank or with any branch of the Bank.

© CONVERSE BANK	Converse Bank CJSC	FO 72-03-07-1	
	Rules of Card Issuance and Use	Edition 7	7/7

Furthermore, the Bank shall be deemed duly notified by the Cardholder by means listed herein from the date of receiving by the Cardholder of the Bank's confirmation of the Cardholder's message.

- 6.2. Once the Bank receives the notification about the unauthorized use of the Card, the Card is immediately blocked and the Bank reviews the details of the Transaction based on the Cardholder's request and starts the Transaction appeal process as appropriate.
- 6.3. The Bank disclaims the responsibility for the Cardholder's loss due to the failure to inform the Bank or the delayed notification.
- 6.4. To unblock the Card if the lost Card is found after blocking, the Cardholder should submit a request with the Bank through the App, send an appropriate written message in the manner described herein or visit any branch of the Bank; the Card is unblocked subject to the due identification of the Cardholder.
- 6.5. The validity of the Card can be restored subject to payment of fees (if any) set under the Tariffs for unblocking the Card.