Amendments shall be effective as of February 04, 2025

The following amendments has been introduced to the "Banking Services Conditions" published on the web page www.procreditbank.ge:

The following subparagraphs 16 and 17 shall be added to the Article 19:

16. The Customer has the right to change their card profile as often as they wish and can select from the following types of card profiles:

16.1. **Blocking payments to high-fraud-risk merchants or service facilities and disabling the CVV2/CVC2 code feature -** This option helps protect customers from potential risks associated with payments made at high-risk merchants or services. Additionally, the CVV2/CVC2 code serves as an extra layer of security for verifying online transactions.

16.2. **Blocking payments to high-fraud-risk merchants or service facilities and enabling the CVV2/CVC2 code feature** - This option helps protect customers from potential risks associated with payments made at high-risk merchants or services. Additionally, since the mandatory CVV2/CVC2 code feature was disabled on the card, enabling it does not prevent unauthorised transactions from occurring.

16.3. **Allowing payments to high-fraud-risk merchants or service facilities and disabling the CVV2/CVC2 code feature** - The Customer understands that enabling this feature increases fraud risks. Additionally, the CVV2/CVC2 code serves as an extra layer of security for verifying online transactions.

16.4. **Allowing payments to high-fraud-risk merchants or service facilities and enabling the CVV2/CVC2 code feature** - The Customer understands that enabling this feature increases fraud risks. Additionally, since the mandatory CVV2/CVC2 code feature was disabled on the card, enabling it does not prevent unauthorized transactions from occurring.

16.5. **Blocking payments to high-fraud-risk merchants or service facilities -** Enabling this feature will block payments at high-risk merchants or service facilities. All other types of transactions will still be permitted on the card.

16.6. **Removing all card restrictions or allowing all transactions -** The Customer understands that activating this feature will permit all types of transactions and operations on the card.

16.7. **Enabling the Fallback feature** - The Customer understands that activating the Fallback feature on the card permits transactions to be completed by entering the card number at the POS terminal. This process may involve deactivating the mandatory CVV2/CVC2 code requirement, which serves as an extra layer of security for verifying online transactions. By enabling the Fallback feature, the card will be functional for a duration of 24 hours.

16.8. **Disabling the Fallback feature -** Although the mandatory CVV2/CVC2 code features were deactivated on the card during the period in which the Fallback feature

was enabled, the Customer understands that the deactivation of the Fallback feature does not preclude the potential for unauthorized transactions on the card.

16.9. Disabling online purchases - The Customer understands that by deactivating the online purchase option on the card, online purchases will be unavailable. However, all other forms of transactions will remain permissible.

17. The Customer acknowledges the following: a) The Bank shall not be held liable for the reimbursement of funds in cases of unauthorized transactions, nor for disputes arising from transactions with merchants or service facilities. b) The Customer assumes full responsibility for all transactions conducted using the card, both over the Internet and at the merchants' or service facilities, as well as for the associated consequences and risks. c) The practice of blocking payments at merchants or service facilities deemed to have a high risk of fraud is implemented for the Customer's protection and is compliant with Georgian legislation. d) The Bank retains authority, without the necessity of obtaining the Customer's consent, to independently modify the list of high-risk merchants or service facilities specified in this document, either by adding to or reducing it. e) The Customer may, at their discretion and at their own risk, reactivate payments with previously blocked merchants or service facilities and/or place further blocks on payments that have been reactivated.