

**Amendments shall be effective as of February 3, 2022.**

**The following amendments have been introduced to the Banking Services Conditions published on the web page [www.procreditbank.ge](http://www.procreditbank.ge):**

**1. Subparagraph "n" has been added to Article 20 (2) of the Banking Services Conditions in the following wording:**

**"n) A trusted device** is a possession category authentication element, which can be a device (mobile device, computer, etc.) that has been granted the status of a trusted device by the client and used for strong user authentication in exchange for a code."

**2. In paragraphs 13 and 13<sup>1</sup> of Article 20 of the Banking Services Conditions, the address of the website has been changed to be <https://online.procreditbank.ge> instead of <https://online.procreditbank.ge/New>:**

**3. The following paragraph 25<sup>1</sup> has been added to Article 20 of the Banking Services Conditions:**

„25<sup>1</sup>. Without registration of the service required for obtaining the authentication code and strong authentication, the client is restricted from the possibility of initial activation of a trusted device. Initial activation time is 24 hours after strong authentication. The activation period of a trusted device is 6 months. Besides, in case of wishing to use a trusted device, after the expiration of the above period, the client shall re-activate it by confirming the TAN code. "

**4. Paragraph 26 of Article 20 of the Banking Services Conditions has been amended to read as follows:**

“26. If the Customer suspects that his/her user name or password has become known to a third party and/or if his/her electronic device/means for generating TAN and/or authentication code and/or cell phone are lost or stolen and/or the access to/reliability of its trusted device is compromised, the Customer shall contact the Bank and request blocking of Internet Banking, or may block himself/herself the access to Internet Banking for his/her user or deactivate/change the trusted device through the website: <https://online.procreditbank.ge>. If the Customer does not inform the Bank about the loss of the password and/or electronic device/means for generating TAN and/or authentication code/cell phone or compromising the reliability of a trusted device, or does not block access to Internet Banking or does not deactivate/change the trusted device through the website: <https://online.procreditbank.ge>, then the Customer is fully responsible for the loss that may occur as a result of Internet Banking operations.”

**5. Paragraph 26<sup>7</sup> of Article 20 of the Banking Services Conditions has been amended to read as follows:**

“26<sup>7</sup>. Blocking of Internet Banking service - if the Customer suspects that his/her username and password has become known to a third party and/or if his/her DIGIPASS, cell phone and/or other electronic device/equipment for generating TAN/authentication code are lost or the reliability of a trusted device is compromised, or the username and password are disclosed, the Customer shall block access to Internet Banking immediately by:

- Contacting the Bank Contact Center to the contact data specified in paragraph 26<sup>6</sup> of this article from 09:00 to 21:00; or receiving information about the blocking through the automatic responding machine from 21:00 to 09:00; or visiting any branch of the Bank during the working hours of the branch;
- Blocking the Internet Banking service by visiting the Bank web page <https://online.procreditbank.ge> during 24 hours, using one-time code. The one-time code, as the Customer selects, shall be sent to the e-mail address specified in the Internet Banking Agreement or at the agreed cell phone number, or the Customer generates himself/herself the code valid for blocking the Internet Banking through TAN generation device – DIGIPASS/Mobile Token according to the instructions provided at the official web page of the Bank: <http://www.procreditbank.ge>.”

**6. Paragraph 31 of Article 20 of the Banking Services Conditions has been amended to read as follows:**

“31. The Bank is authorized to reject a Customer’s electronic document for execution in the following cases:

- The electronic document does not include all necessary information;
- Information in any field of the electronic document is incorrect;
- The Client has not sent via Internet Banking a document evidencing the grounds for transfer in the foreign currency;
- The Customer has violated any of the rules established by this document or by the Bank;
- The Customer fails to present the ID document when the transfer is made instead/in favour of a third party.