Safety memo when working in the Bank's Mobile Application

The Bank Service is the Bank's Mobile Application, which allows Users to interact with the Bank within the framework of concluded banking services agreements and/or an electronic money agreement, as well as without concluding such, including the exchange of information and the execution of individual transactions via the Internet or a special application of a mobile device (smartphone, tablet, etc.), as well as an electronic payment system that allows Users of mobile devices to pay for services, make money transfers between individuals through the Bank's services and make purchases on the Internet.

Please familiarize yourself with the basic safety rules:

- ✓ Do not give or communicate to anyone the one-time password from the SMS message used when conducting transactions on the Internet and using the Bank's services;
- ✓ Do not use third-party mobile phone numbers when connecting to the Bank's services;
- ✓ Do not transfer the right to use your bank account/payment card/remote banking system to third parties who do not have legal grounds for doing so (representative, authorized person);
- ✓ Do not disclose or transfer the payment card details, as well as the CVC/CVC2 code/3D Secure password data to anyone;
- ✓ Do not under any circumstances disclose your login, password, or code from an SMS message to anyone, including Bank employees, except in cases of independent contact with the Bank's Contact Center to receive advice or a service that requires the provision of a code from an SMS message. Responsibility for the storage of personal confidential data and passwords rests with the User;
- ✓ Do not authorize in the Bank's mobile applications by setting a PIN code or logging in using a fingerprint on someone else's mobile device;
- ✓ daily analyze all notifications about transactions performed and rejected by the Bank, and immediately inform the Bank of cases of unauthorized crediting (transferring) of funds, in order to minimize potential losses;
- ✓ in case of loss/theft of a mobile phone to which the Bank sends SMS messages with a one-time password, or unexpected termination of the SIM Card, you should immediately contact your mobile operator and block the SIM Card, and immediately inform the Bank about this;
- ✓ activate the "SMS-informing" service, set limits on card transactions on the Internet;
- ✓ promptly install updates of the operating system of your mobile device;
- ✓ use licensed anti-virus software and monitor its regular updates;
- ✓ regularly perform anti-virus scans for timely detection of malware;
- ✓ do not install third-party applications at the request of third or unfamiliar parties;
- ✓ The Bank has all the necessary information and never, under any circumstances, sends out emails, SMS messages, phone calls with a request to transfer payment card details, authorization data, PIN code to the payment card, and does not distribute programs and their updates by email;
- ✓ in case of data compromise or detection of facts of unauthorized access and conducting unauthorized transactions from bank accounts through the Mobile Application, you must immediately contact the Contact Center at 595 (free call in the Republic of Kazakhstan) or by email at security@freedombank.kz.