RECOMMENDATIONS ON INFORMATION SECURITY, IN PARTICULAR ON REDUCING THE RISKS OF RE-TRANSFER OF FUNDS WITHOUT THE CLIENT'S VOLUNTARY CONSENT

With a view to the increasing number of fraud transactions of funds by means of remote banking systems via Internet and for the purposes of prevention of unauthorized access of hackers to the Accounts of the Clients, the Bank strongly recommends to physical entities – EuroLink System users (hereinafter – "the System") to meet the following measures of information security:

- To use on permanent basis anti-virus software with the last updated version of databases (on all devices used to access the System and/or that receive SMS/push notifications).

- To perform anti-virus screening on regular basis for timely disclosure of hazardous programs (on all devices used to access the System and/or that receive SMS/push notifications).

- To install regularly the updates of the operational system and the Internet Browser (which is used for accessing the System) (on all devices used to access the System and/or that receive SMS/push notifications).

- Do not install in devices used for access to the System any software for remote manipulation (Team Viewer, Ammyy Admin, AnyDesk, VNC, etc.)

- To block access to the devices used to access the System. Not to leave unlocked devices unattended.

- To access the System via direct link https://dbo.efbank.ru or the link on the corporate web-site of the Bank. One should always make sure that connection with *.efbank.ru (e.g., dbo.efbank.ru) is established via the secure protocol (https). A closed lock icon will appear in the address bar.

- Do not access the System using the untrusted computers (Internet cafés and other public computers) amd public wi-fi networks when accessing the System, as attackers may intercept all your traffic, including password information.

- Install updates of system software only from official sources.

- Do not save Login and Password for the System in the browser's memory.

- Do not store Login and Password for the System openly in devices used for access to the System.

- Use only those smartphone apps that are downloaded from official app stores. The mobile version of the System is posted on the Bank's official website – https://evrofinance.ru/eng/individuals//system-eurolink/.

- Receive information about the registered Orders and the status of the Accounts and verify it at least once a day.

The Bank recommends the Client to consider the risks upon working in the System via Internet and understand that only use of anti-virus software provides with 100% protection guarantee from fraud transactions by hackers in the System of the Client.

In case if your sim card appears inactive, please contact your mobile service provider and clarify the reasons. May be intruders received a clone (copy) of your sim card.

It is necessary to consider the most widely spread schemes of fraudulent activities in the Internet for today:

- "Social engineering" hackers send SMS /email or call you on behalf of the Bank and under various pretexts try to get the Client's Login, Password, Print Name, numbers of accounts, cards, pin codes, etc.

- "Phishing" – The Client receives by mail or otherwise a link to fake web-site, which can be visually identical to the official one, with a request to enter the Login and Password for any reasons (Password is out-of-date, additional authorization is required, unlocking of the blocked access, etc.).

- Infection by a malicious code by means of spreading malicious programs via Internet resources, for example, social networks web-sites, or by spamming via electronic mail. After infecting the Client's System with a virus or a "Troyan" program the hacker gets full control over the System.

When using the System it is required to remember that:

In case the Client discloses suspicious transactions in the System, it is required to refer to the Bank's Client Support Service immediately via telephone number published on the corporate website of the Bank.