RECOMMENDATIONS ON INFORMATION SECURITY

Since Internet frauds is a common issue with remote banking services, to prevent unauthorized access to the Customer Accounts, the Bank highly recommends that all individual Customers follow these information security measures when accessing the System via the Internet:

- Use antivirus software with the latest database updates at all times.
- Perform an antivirus scan regularly to detect malicious software.
- Update your operating system and the Internet browser you use to access the System regularly.
- Access the System by typing the following link: https://elf.faktura.ru/?site=evrofinance directly in your web browser or by clicking the link on the Bank's website. Make sure the connection uses secure HTTPS protocol – this can be seen by the browser's address bar turning green or showing a closed padlock icon.
- Avoid accessing the System from shared workstations (Internet cafes, etc.).
- Do not install system software or Internet browser updates you received in email or otherwise, pretending to be from the Bank. In fact, do not open any links in such email messages at all. Please notify the Bank immediately about any such emails you receive.
- Check information on the Orders registered and the Account status at least once a day.

The Bank recommends that the Customers mind the risks of accessing the System via the Internet and understand that antivirus software alone does not give a 100% guarantee against attackers gaining unauthorized access to the System.

The following online fraud schemes are most popular in the Internet these days:

- Social Engineering – attackers send out SMS messages pretending to be from the Bank and use different methods to trick the Customer into giving away their login, password, name, account numbers, cards numbers, PIN codes, etc.
- Phishing – the attackers send an email or other message with a fake link that looks similar to the actual Bank's website, requesting login, password and other data. Different reasons can be given, such as "your password has expired", "additional confirmation needed", "unlock your account", etc.
- Malware – malicious software is commonly distributed online, e.g., in social media or by email spam. Once the Customer's computer is infected with a virus or Trojan software, hackers get full control of the System.

When using the System, please keep in mind the Bank never sends SMS messages or emails requesting Customer data or information about the System.

If the Customer detects any suspicious activity in the System, please contact the Customer Support immediately, using phone numbers published on the Bank's official website.