Security

Effective date: 14.01.2021

Finci UAB is a licensed e-money institution with the right to execute the activity related to issuance of e-money and provision of payment services all around the European Union. The e-money institution license No. 60 was issued by the Bank of Lithuania on 5 December 2019.

Finci UAB constantly makes every effort to keep its system secure, but the security of your account and your data also depends on actions performed by you on the internet. In order to help you to ensure the security, this documents sets out the recommendations on how can you protect your account, how can you protect yourself from phishing and how you can keep your data safe online.

Please note that the recommendations mentioned below are indicative, non-exhaustive and do not constitute any guarantees, warranties or promises regarding the security of your account and your data.

Finci UAB reserve the right to update, change or replace any part of this document by posting updates and/or amendments and/or alterations to its official website, updating the “Last Updated” date at the top of this document.

Protection of the account

Finci UAB applies the following security measures to safeguard your account:

- Your login details which consist of your mobile phone number verified by Finci UAB and password created by you. Please always use a secure password and do not disclose to anyone your login details.
- Strong customer authentication - an authentication process based on the use of two or more secure elements. When you log into your account, make a transfer, SMS code will be sent to your number verified by Finci UAB to confirm your login attempt or your initiated transaction.

How can you protect your account?

- Always make sure that you use a reliable account password that would not be related to your personal data and that would include letters (uppercase and lowercase), numbers and special characters. Password should not be easily guessed (e.g. you should not use your or your family member’s date of birth, name, surname, etc.)
- Regularly change your password details used to access your account or any other website where your account details are stored, also your mobile phone code or other security means.
- Never transfer or disclose your login details used to access your account or any other website where your account details are stored (Security details), mobile phone code, authorization codes,

transaction confirmation codes or other security means and do not to write them down on paper or on other items.

- Always log out from your account when you're not using it.
- As the account holder, you and only you should create and have access to your login details. Therefore don't allow others to use your Security details, authorization codes, transaction confirmation codes, mobile phone code or other security means.
- Don't allow your Security details to be stored on any device such as a computer or mobile phone.
- If you suspect that other persons know your password details used to access your account, change password immediately and check if there have been any unauthorized logins to the account and if there have been any actual or attempted payment transactions. If you are not able to change password, immediately inform about this Finci UAB to the email indicated on the official website address of Finci UAB.
- Please note that Finci UAB will never ask for password details used to access your account, your account number, card number, eWallet number, security code, password, or your card PIN, SMS codes or other security means.

What is phishing and how can you protect yourself from it?

- Phishing - attempts of scammers to obtain your personal data (name, surname, etc.), account login details, card details and other sensitive information by pretending to be, for example, the employees of Finci UAB, representatives of a known company, an entity you trust or other. Phishing could be done via emails, fake websites, text massages.
- Please note that Finci UAB system is accessible only at an official **website address of Finci UAB**.
- Always make sure that you have accessed an official website address of Finci UAB , because scammers might use the names similar to official website address of Finci UAB and/or its content in order to direct you to other fake websites. If you have some suspicion that you have accessed a fake website, please immediately notify Finci UAB by email indicated on the official website address of Finci UAB .
- Do not send your personal identification documents, your personal information to unknown or unverified recipients.
- Never provide your username, password, or PIN codes in an external website or app, even if it similar to Finci UAB.
- Always make sure that you have received email from official email address of Finci UAB which is indicated on the official website address of Finci UAB , because scammers might use the email addresses similar to official email address of Finci UAB . If you've received a suspicious email that claims to come from Finci UAB , please forward it to us to email address indicated on the official website address of Finci UAB .

How you can keep your data safe online?

- Before shopping online, always check the reputation and reliability of merchants (online stores) in internet search engines (e.g. Google), on rating websites, forums or other sources. The low credibility of the online store can indicate, for example, that real name, registration number or/and contact information of the legal entity is/are not indicated on the website.
- Check the addresses of websites and content of the websites you accesses to, because scammers might use the names and/or content similar to website addresses of actually existing legal entities in order to direct you to fake website.
- Always keep a record of your online purchases and check the balance on your account regularly.
- Never open emails, messages, web links, attached documents/files, do not install any software send from unknown senders, if you are not sure that they are reliable, safe and trusted, regardless of whether send by e-mail, SMS or other means.
- Do not provide your personal information on the websites and/or to unknown recipients if you are not sure that they are reliable, safe and trusted.
- Do not access unsafe/non-reliable websites and do not install software from unknown sources.
- When accessing internet (e.g. online stores), always use only safe devices (mobile phones and/or computers), safe internet connection and licensed software, also install software updates, ensure control over devices access rights.