

MyCII mobile application

User guide

Concorde Investments Ireland Ltd.

Contents

1. User guide.....	3
1.1. Launch the MyCII mobile application.....	3
1.1.1. Installation.....	3
1.1.2. Launch	3
1.2. The menu items.....	4
1.2.1. Portfolio.....	4
1.2.2. Transactions	5
1.3. Settings	5
1.3.1. Change password	6
1.3.2. Biometric identification.....	6
2. Technical and safety information.....	7
2.1. Concepts.....	7
2.2. Technical requirements.....	7
2.3. General security information	7
2.4. Important Security related to password management.....	8
2.5. Security related to portable devices (smartphone)	8
2.6. Protection of electronic contacts.....	9
2.7. Actions to be taken in the event of technical, security problems and incidents.....	9

1. User guide

The purpose of this user guide is to present the structure and usage of the MyCII mobile application, which is available on smartphones.

1.1. Launch the MyCII mobile application

1.1.1. Installation

Download and install the MyCII mobile application on your device via the App Store or Google Play.

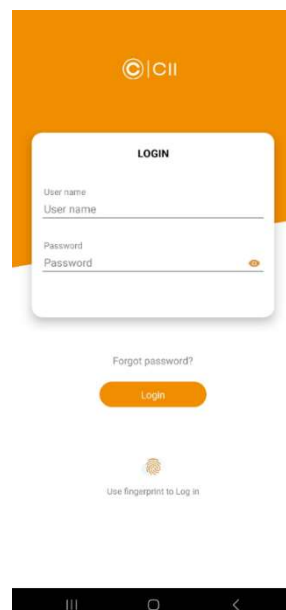
Concorde Investments Ireland Ltd. (CII) publishes the MyCII mobile app exclusively on the App Store and Google Play. Please use only the application published there. Do not download or install the MyCII application from unknown sources, CII does not assume responsibility for these.

1.1.2. Launch

Click on the MyCII mobile application icon



For the first time log-in need to use the CII client code (CWxxx) and answer three identification questions, and then the device is assigned to the MyCII service via a confirmation SMS code which is sent to the registered default mobile phone number of the Account Holder.

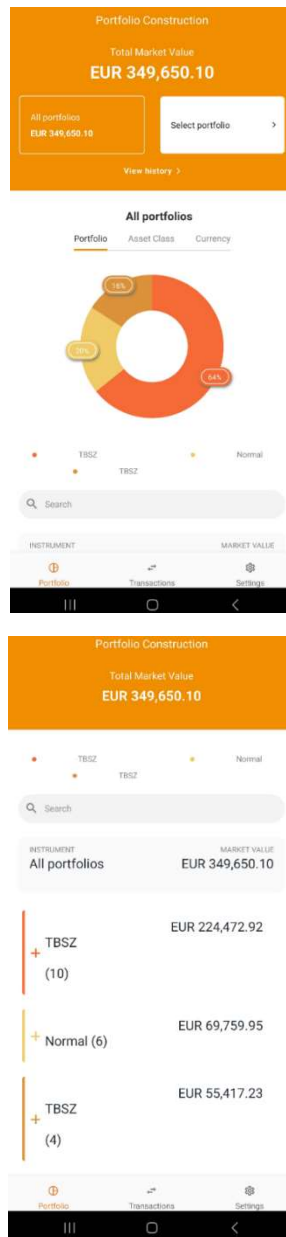


1.2. The menu items

1.2.1. Portfolio

In the Portfolio menu, you can find the detailed data of your portfolio, and there is an option for the account holder to view all sub-accounts at the same time. On the Portfolio Construction the account holder can find the Total Market Value of all accounts.

It is also possible, with the help of the account selector tool, to view the accounts separately by asset class and by currency.



1.2.2. Transactions

In the Transactions menu, you can find under process, pending transactions , as well as the history of the closed transactions.

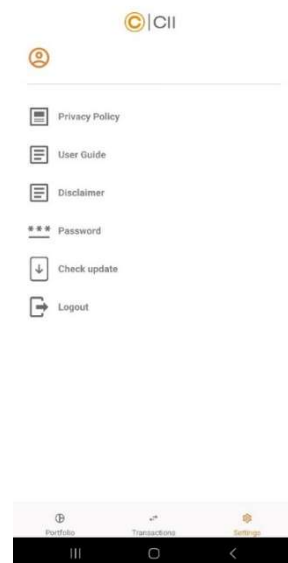
By default, this shows the transactions of the last 2 months, which can be changed by clicking the filter button.

In the filter, we can choose from client accounts, different transaction types, and time intervals.



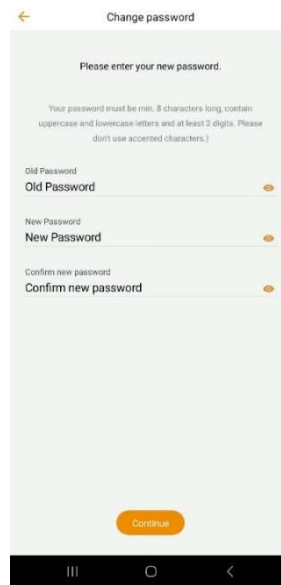
1.3. Settings

In the Settings menu you can find this user guide along with the GDPR – Data Protection Manual. Under this menu, you can also change your current password or turn on the biometric identification.



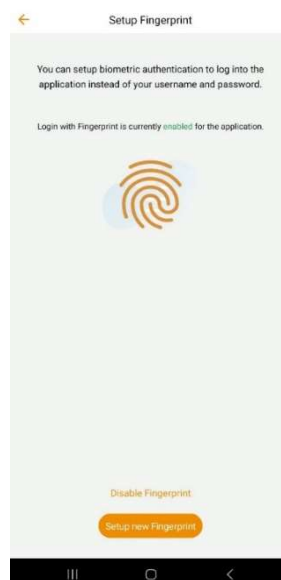
1.3.1. Change password

In the Settings menu, you can change your password by clicking to Change Password. To change our password, you must enter your current password, then enter and confirm the new password. The password must be at least 8 characters long and contain at least one lowercase letter, one capital letter, and one special character.



1.3.2. Biometric identification

If you want to login to the application with biometric identification instead of a password, you can do this by turning on Biometric identification in the Settings menu. To enable biometric identification, we must enter our current password for confirmation. After that step, the biometric identification becomes active.



2. Technical and safety information

The purpose of this section is to define the system requirements of the MyCII mobile application and to provide information on the safe use of the service.

We would like to draw the attention of the users of the services that the users responsibility to provide the appropriate level of security protection of the devices and user accesses (username, password).

2.1. Concepts

MyCII mobile application: a financial service provided by CII that can be used by clients on smartphones.

Username: a 6-digit, numerical identification code that is used to uniquely identify the user.

Password: an alphanumeric identification code used to uniquely identify the user.

Biometric identification: the fingerprint (TouchID), facial recognition (FaceID), or iris scanning set as default on the mobile device, which the user can use to enter the MyCII mobile application.

Two-factor authentication (2FA): is an identity and access management security method that requires two types of authentication to access resources and data. Two-factor authentication makes it possible to ensure the protection of the most sensitive information.

2.2. Technical requirements

You can use the application on the following devices:

- iPhone 6S and newer iPhones running at least the iOS 13 operating system.
- Android smartphones running at least the Android 5.0 operating system.
- The application is currently not available on Huawei phones released since autumn 2019 (e.g. Huawei Mate 30, P40) that do not support the Google Play Services (GPS) ecosystem.
- The application cannot be used on smartphones with modified (rooted or jailbroken) operating systems.

2.3. General security information

- Use up-to-date virus protection and firewall programs to protect your devices (computer, mobile phone, tablet) against viruses, spyware, and malicious software.
- Keep the operating systems used by your devices (Windows, Linux, MacOS, iOS, and Android) and the applications installed on the devices up to date by regularly installing the official updates and repair versions issued by the manufacturers.
- Use only legal software on your devices, and do not install dubious applications from unknown sources.
- Disable the automatic connection to unknown wireless networks (Wi-Fi, Bluetooth) for your devices.
- Please contact CII immediately by email (mobilapp@ciireland.com) if you receive a message asking you to provide personal or confidential data (name, phone number, password) from CII. CII never asks for this type of data from its clients in an email or SMS.

- Always deal with messages, attachments, and links from unknown senders with special care, and avoid answering or opening them.

2.4. Important Security related to password management

- Do not use personal information (date of birth, phone number, address, favourite pet, spouse's name, PIN or TPIN number, etc.) and dictionary-based words in your passwords.
- The system requires the use of complex passwords. The length of the password is at least 8 characters, which must include capital and lowercase letters and at least 2 numbers.
- Try to provide a password that cannot be linked to CII.
- Do not give your ID or password to anyone.
- Passwords must only be stored in a secure form, for example, using password management applications. User passwords can only be stored in an encrypted form.
- CII never asks users to share passwords through any channel. Please do not share your password with anyone!
- Please change the user password regularly, at least every three months. If you become aware that your user access has been compromised, you should immediately change your user password and report it to CII's by email (mobilapp@ciireland.com).
- We recommend using a unique, generated password for each system. Try not to use the same password for different systems, because that increases the possibility of misuse.
- If you forget your password, you can request a new one by mobilapp@ciireland.com. For security reasons, our colleague will self-identify you and send you a new, temporary authentication password to the phone number you provided earlier.
- After three unsuccessful login attempts, the system temporarily disables access for an hour.

2.5. Security related to portable devices (smartphone)

- If possible, do not use the portable device on which you also receive SMS messages from CII to use the service.
- It is recommended not to change the device's factory authorization settings, do not root or jailbreak the device.
- Use protection against unlocking the screen lock (PIN code, unique pattern).
- Do not store personal data (bank card number, PIN, or TPIN number) on the device.
- Do not install any apps or software directly downloaded from the internet on your devices, instead use the official sources or distribution channels (e.g. Google Play, App Store, Windows Market).
- Check the authorization requests and services that can be used by the application you want to install in every case, and if an application wants to use functions that does not fit its profile (e.g. a wallpaper application wants to send SMS) then, stop the installation process. Always perform this check when updating applications, as new application versions often request additional permissions.
- It is recommended to turn off unused services (e.g. Bluetooth, GPS, and NFC) and enable them only if you are actually using them.
- It is recommended to encrypt the data stored on the device's external storage if it is supported by the device's operating system or the device's manufacturer.

2.6. Protection of electronic contacts

In order to prevent fraud and abuse, CII checks your participation using an SMS authentication code sent to a mobile phone number to perform special functions (e.g. data changes).

For security reasons, CII will notify you by email in cases of changes in contact details. If you did not initiate the change, please report this to mobilapp@ciireland.com immediately. Please check that your e-mail system does not treat emails sent by CII as spam.

Please note that it is your responsibility to protect your personal information and personal devices.

In order to protect your devices and personal contacts, please ensure that they are properly protected by doing the following steps:

- Do not use public computers and networks.
- Always protect your devices with a password and turn them off or lock them after use.
- Install virus and malware protection on your devices.
- Install security updates for the software on your devices regularly.
- Use a firewall to protect your devices.

2.7. Actions to be taken in the event of technical, security problems and incidents

If you experience a problem, please notify us immediately in order to prevent possible fraud and abuse at mobilapp@ciireland.com.