Mobile Banking Terms & Conditions

People's Choice
Banking for life

By using this Application, you agree to the Terms & Conditions set out below and the terms and conditions set out in the current version of our Accounts & Access Facilities Terms & Conditions (a copy of which can be accessed here) in relation to your use of this Application and any transactions you conduct using this Application. Words and expressions defined in our Accounts & Access Facilities Terms & Conditions have the same meaning in the below Terms & Conditions.

If any provision set out below is inconsistent with the terms in our Accounts & Access Facilities Terms & Conditions, in relation to your use of this Application, the Terms & Conditions set out below prevail to the extent of the inconsistency.

Terms & Conditions
This Application is a Mobile Banking software application referred to in the definition of 'Mobile Banking' in our Accounts & Access Facilities Terms & Conditions.

Access to Mobile Banking
Mobile Banking is only available to People's Choice Credit Union Members that are current registered users of Internet Banking.

Not all Devices may be capable of accessing and using Mobile Banking and all Internet Banking services and features may not be available for Mobile Banking.

The features available to you via Mobile Banking, the way in which you can access and use Mobile Banking, and the transactions and actions you can conduct by Mobile Banking may differ depending on the Device and the version of our Mobile Banking application you are using and may change from time to time without notice to you.

You are responsible for obtaining a compatible Device to use our Mobile Banking service.

Any conditions of use and charges relating to a Device or the use of any telecommunications networks to access Mobile Banking are your responsibility. We are not liable or responsible for any costs you incur in relation to your use of a Device to access Mobile Banking or loss or damage to a Device resulting from your access or use or attempted access or use of Mobile Banking, except to the extent that the loss is caused by our fraud, negligence or wilful misconduct (including that of our officers, employees, contractors or agents).

We may disable or remove your ability to access Mobile Banking at any time for any reason in accordance with clause 5.25.6 in our Accounts & Access Facilities Terms & Conditions.

Logging in and registering your device
You may only access and use Mobile Banking on a Registered Mobile Device.

To register a compatible mobile Device as a Registered Mobile Device you must:

- Download the latest version of our Mobile Banking application for your type of mobile Device;
- Open the Mobile Banking application and log in using your Member Number and Internet Banking password; and
- Authorise the registration of your mobile Device using Second Tier Authentication.

If you delete the installation of our Mobile Banking application from a Registered Mobile Device you will be required to re-register your Device.

After you have registered your Device, we may allow you to set an access code in the Application ('App PIN') which you can use to log in to Mobile Banking on that Registered Mobile Device in the future. We may reset your App PIN, require that you set a new App PIN or cease to allow you to log in using an App PIN at any time.

If you have a compatible Device, we may allow you to log into Mobile Banking and authorise transactions or actions using Biometric Verification functionality provided by your Device. If you want to use Biometric Verification with Mobile Banking you will first need to log in to Mobile Banking using your Member Number and Internet Banking password or App PIN and then enable the functionality within the application settings. You will also need to follow the relevant procedures to register and store your biometric information on your Device for Biometric Verification purposes.

On some Devices, if you enable Biometric Verification for Mobile Banking on the Device you may also be able to log in to Mobile Banking on the Device using the password, passcode or security code you have set on the Device for the purpose of 'unlocking' or otherwise securing use of the Device ('Device Passcode').

You must not enable Biometric Verification for Mobile Banking on a Registered Mobile Device if any biometric information of a person other than you is registered on that Device for Biometric Verification purposes or if you are aware or suspect that another person knows your Device Passcode. You must ensure that no biometric information of any other person is registered or stored on a Registered Mobile Device for Biometric Verification purposes while Biometric Verification is enabled for Mobile Banking. With Biometric Verification enabled for Mobile Banking, subject to the ePayments Code:

- you will be liable for all transactions conducted on the Registered Mobile Device including any Unauthorised Transactions conducted by any person with their biometric information registered on the Registered Mobile Device for Biometric Verification purposes or who knows your Device Passcode;
- we will not be responsible for any loss you suffer as a result of any Unauthorised Transaction conducted by a person who has their biometric information registered on the Registered Mobile Device for Biometric Verification purposes or who knows your Device Passcode, except to the extent that the loss is caused by our fraud, negligence or wilful misconduct (including that of our officers, employees, contractors or agents); and
- any person with their biometric information registered on the Registered Mobile Device for Biometric Verification purposes or who knows your Device Passcode will have access to your personal information that is available by Mobile Banking.

You must keep your App PIN and your Device Passcode secure and not disclose either to any person. You must promptly notify us and change your App PIN and Device Passcode if you become aware or suspect that either your App PIN or Device Passcode has become known to another person.

You must notify us on becoming aware, if you have set an App PIN or have enabled Biometric Verification on a Registered Mobile Device and the Device is lost or stolen.

You must notify us on becoming aware, if your Device with a VIP Access App installation or an Access Token that is registered to your Membership is lost or stolen.

Deregistering your device
You may deregister a Registered Mobile Device:

- In Mobile Banking on the Registered Mobile Device;
- In Internet Banking accessed through an internet browser; or
- By calling us on 13 11 82 and requesting that we deregister your Device.

If you deregister a Registered Mobile Device through Mobile Banking or Internet Banking we may require that you authorise the deregistration using Second Tier Authentication. Deregistering a device can also be completed by calling us on 13 11 82 or visiting your local branch.