

Redstone Federal Credit Union

Answers to Frequently Asked Questions

Mobile App

Getting Started

What is the Redstone Federal Credit Union Mobile Banking App?

The Redstone Federal Credit Union Mobile Banking App is a service that enables you to access your account information and transfer funds from an Android, iPhone, iPad or Kindle device with Internet access from either a WIFI source or the 3G/EDGE networks.

How does the Redstone Federal Credit Union Mobile App work?

First, you must download our Mobile App from the iTunes App Store, Android Marketplace or Amazon Appstore. You can do this either from your mobile phone, iPad, Kindle or computer. If you access our App from your computer, the App will install on the mobile phone, iPad or Kindle the next time the device is plugged in/synced to the computer.

Once you download the App, you will log in with the same member number/user ID and password that you use for online banking. No separate or different registration is required. Once logged in, you can:

- Access Your Accounts – view account balances and account history
- Make Transfers – you must have more than one account on online banking for this functionality to be available in mobile banking
- Make Deposits – deposit checks to your account (smart phone or iPad, version 2 or later, only)
- Pay Bills - schedule bill payments to already established payees
- Find an ATM/Branch – use the App to locate the ATM or branch nearest your location (smart phone only)
- Contact Us – contact us quickly from the App
- View Checks – see check images within Account Transactions
- View Redstone Rewards – see active Redstone Reward cash back offers (Redstone Rewards is not available on the iPad App at this time.)

Is the Redstone Federal Credit Union Mobile App currently available to all users?

The Mobile App is currently available to all online banking users who own an iPhone, Android, iPad or Kindle device with access to 3G/EDGE or WIFI.

Is it safe to bank using the Redstone Federal Credit Union Mobile App service?

Yes. To protect your privacy, you are required to authenticate yourself on each individual mobile device using the same information from online banking. All communication between your mobile device and the mobile banking server is encrypted. In addition, your password and account information are never stored on the mobile device.

Is a password needed for the Mobile App?

Yes. From your mobile device, you will need to log in to the Redstone Federal Credit Union Mobile App using the same login information you do for online banking. No separate Mobile App sign-up is required.

Verification Code

Will mobile banking require a verification code to access online banking?

Yes, you will go through the security authentication process once on each mobile device. You will be challenged on the device with the phone number that is associated with your account.

Will I be able to change the phone number(s) used to receive my verification code?

You will be able to change your registered phone number(s) within online banking, but there are currently no settings that allow this to be done within the mobile versions. However, during first-time use, you will be able to change the phone number(s) used to receive your verification code. This will allow mobile-only users to add a new number or change an old number so you can log in from the registered phone.

If I don't have any registered phone numbers will I still be able to log in with a mobile device?

Yes, you will be prompted to enter a phone number if there is no existing phone number on file. You will use this phone number for future login attempts on other devices.

Are phone numbers masked?

Yes, the phone numbers are masked throughout all points of the process.

Will I have to authenticate each device I use?

Yes, you will have to individually authenticate each device that uses the mobile app or mobile web banking. This allows us to provide additional security at each access point that is used.

Will I have to authenticate my device(s) every time I log in or only the first time?

You will only have to authenticate your device(s) the first time. Then, we will create a secure cookie that will be used to ensure the same user on the same device makes each future login attempt. If you erase the cookie from a device from within the app, you will have to authenticate the device again.

I don't want my mobile device "remembered." Can I authenticate during every login?

Yes, even though this is not the default behavior of the app, if you choose, you can go into the "More" section and turn the "Remember device" toggle OFF to be challenged when you log in again.

What happens if my mobile device is stolen or lost?

Multi-factor authentication is built to protect against remote attacks, which are the majority of fraudulent attacks. If a mobile device is lost or stolen, you should do exactly what you would do today: call the carrier to report it and cancel service to the device or do a remote lock or data wipe via another device. There is more information (contacts, email, other apps, etc.) on a mobile phone or tablet that should be protected than one particular banking app. Keep in mind, that even if a device is stolen or lost, the thief still needs to get past the username and password, hence multi-factor authentication. Similar to when someone loses their ATM card, the fraudster must know the ATM PIN to move funds out.

How can security be provided if the verification code is sent to the same device?

Multi-factor authentication (MFA) gets its name because there are multiple methods of authentication, to further reduce the risk of fraudulent attacks, both remote hacking attempts and local phone theft. The second factor of authentication that we are adding to mobile further reduces the risk of remote fraudulent attacks, because the phone is "something the user has" and the login has to be verified with the specific phone that is tied to the user's account with the phone in the user's hand at time of login. If a phone is stolen and the thief attempts to log in, then the attack is no longer remote. At this point the thief still must initially get past the username and password. The "something the user knows" factor (username and password through the app) is one channel of communication & authentication, while the "something the user has" factor (verification code through SMS or Voice) is another channel of

communication & authentication. Thus, multiple channels mitigate the risk of malicious remote and local attacks.

Additionally, remember, a user can use a different phone number than their mobile phone number if they choose. Hence, they could enter their landline or office number to authenticate their mobile device to further reduce risk.

Finally, if a user does have their phone stolen, the best defense will always be to call the carrier and have it deactivated and its data remotely wiped, just as users do today, as there is more data on a phone that a user will want to protect than one particular banking app (such as contacts and email, for example). Additionally, the user can also utilize other iPhone & Android native app capabilities of remotely locking or wiping the phone.

Navigation

Are different kinds of funds transfers available?

To do a funds transfer, you must have more than one account in online banking. On the Transfers button, you can enter an immediate transfer between your accounts. However, you are not able to see scheduled transfers nor can you change or remove a scheduled transfer this way.

Can I pay bills using the Mobile App?

Yes, you can schedule bill payments to already established payees. New payees must be set up through the full online banking service.

Can I make a deposit through the mobile app?

Yes. Deposits can now be made using the camera on your smart phone. The deposit feature is not available for Kindle devices.

Can I view checks in the mobile app?

Yes. Check images are displayed within Account Transactions. Check icons are displayed next to transactions associated with cleared checks.

What does the 'Remember Me' checkbox do?

Selecting the Remember Me checkbox gives the application permission to save your member number/ user ID so you will not have to enter it each time you attempt to log in. This information is masked and stored securely to keep your information safe. However, you will need to enter your password each time you log in.

My session timed out pretty quickly, can I change the timeout value?

No. For your security and protection, when there has been no account activity for ten minutes, the session times out and the Redstone Federal Credit Union Mobile App login page displays with a Session Expired message.

How do I log out?

When you're ready to log out, select the Log Out button at the top right of the page and you will exit the Redstone Federal Credit Union Mobile App. This will return you to the Login screen.

I have disconnected my mobile phone. Will my service continue to work?

For the Redstone Federal Credit Union Mobile App to work, you must have a mobile device with access to the 3G/EDGE or WIFI networks.

Is help available through my mobile device?

For assistance with your Redstone accounts, click the More tab to find our support phone number, 256-837-6110 (smart phone only), and email address, general-info@redfcu.org. For help regarding your specific mobile device and/or wireless Internet connectivity, contact your wireless provider.

Redstone Rewards

Redstone Rewards are available for view in the Mobile App.* Please read below on how to access Redstone Rewards.

(*Redstone Rewards is not available on iPad App at this time.)

Redstone Rewards Main Navigation

If you have at least one Redstone Reward enabled account, you will see an option to access your offers. If there are no enabled Redstone Reward accounts, there will be no visible content related to Redstone Rewards. Redstone Rewards accounts that have either been opted out or disabled will not display in the mobile application.

If you have at least one offer, the button will also display the total number of non-expired offers currently available for activation or redemption. In instances where there are multiple enabled checking accounts, the button will display the sum total number of offers for all enabled accounts. For example, you, as a primary owner and joint owner with two enabled Redstone Reward accounts, have 5 offers on your primary checking account and 3 offers on your joint checking account, the button would read "8 offers." For accounts with no non-expired offers, the "# offers" text will not display.

Redstone Rewards Offer List

Upon tap of the main navigation button or icon, you are taken to a screen where you can view all non-expired offers currently available for activation or redemption. The headers of the Redstone Reward screens are entitled "Offers" on the iPhone application and "Cash Back Offers" on the Android and Kindle applications. In addition to the offer list, you can (1) see the account that offers are attached to, (2) re-sort available offers [Android and Kindle only] or (3) navigate to the redemption screen to see details about which offers have been

recently redeemed. This screen will display the total \$ of redemptions earned during the current month and last two months. Each offer will display the merchant logo, offer expiration date, short description of offer details and the current offer activation status. Offers that display "Add to debit card before using" beneath the offer summary description need to be activated; this can be done by simply tapping the offer. Offers that display "added" beneath the offer summary description have already been activated and are ready to be redeemed. The default sort for the offer list is "Newest first." This means that the offers that were presented most recently will always be at the top of the list, each time you log in.

Redstone Rewards for Multiple Enabled Accounts

Offers are displayed one account at a time. If you have multiple enabled accounts, the top bar displaying the associated account will be selectable. The account bar will also display the total number of offers attached to the selected account. Upon tapping this bar, you are presented with an account selector allowing you to view offers for another account. By default, upon login the first account displayed is the account last viewed during the most recent login. For the first login, the first account in the account list will be displayed.