

Digital Banking FAQs

Smartphone Device Minimum Requirements

- iOS – 10.3+ or higher
- Android
 - Lollipop (5.0-5.1.1)
 - Marshmallow (6.0-6.0.1)
 - Nougat (7.0-7.1)
 - Oreo (8.0-8.1)

Supported Web Browsers

- Chrome – 60 and 61
- Firefox – 54 and 55
- Safari – 10 and 11
- IE – 11
- Edge – 39 and 40

The minimum requirements for the Apple version of the app is listed in iTunes when searching for the application. iTunes will list the devices that the application is compatible with as well as the iOS (operating system version). If your device does not have the most current iOS or operating system available, connect the device to any PC or Mac running iTunes and install the latest version.

Who is allowed to use the Greater Texas Credit Union iPhone or Android Applications?

Any member with GTFCU or Aggieland CU with a savings account, checking account, term share certificate, loan, or deposit account. You must also be in good standing with the financial institution.

Can a Small Business members use the Greater Texas Credit Union's Mobile Banking Application?

Yes. You will enroll using your business EIN as the Social Security Number and the business start date as the date of birth.

Can multiple members use the GTFCU Mobile Banking Application through the same device?

Yes. If another member wishes to access the application through another registered member's device then the second member may enter their existing credentials at the login screen. If successful, they will be prompted to answer a one-time security validation question.

I have forgotten my username or password. How can I retrieve it?

If the username or password has been lost, locate the "Help" icon at the login screen and follow the necessary steps to retrieve the forgotten credentials. It is highly recommended that all members reset their passwords by using the help feature in the application.

Having problems creating a username?

The username is restricted to between 6-20 characters in length. The guidelines for creating a username are stated specifically within the registration process.

Having problems creating a password?

The password must contain the following:

- Password must be between 6 to 12 characters At least one
- number
- At least one special character (!@#\$%^&* _+==()[]{}|:./?)
- At least one uppercase letter
- At least one lowercase letter

The password must also be entered in twice to confirm and also match during the registration process.

What is the Auto-Login feature, can anyone who uses that mobile device have access to all my account features?

Auto Login is a feature accessible in the settings menu that will allow a member to use the application and bypass the login screen. In order to activate, the member will go to the settings menu after they've logged in and toggle the switch on. A disclaimer is brought up which the member must accept before being able to proceed. When Auto Login is activated only basic features of the application are available to use. For example the following features will require you to login if they are accessed through Auto Login:

- Transfers
- Remote Deposit Capture
- Check Images
- Accessing the Settings Menu

Why does the application ask to select the "primary account" upon completing registration?

Members are asked to select a primary account in order to make sure the application shows the preferred account's list of transaction on the account dashboard. Members can always view another account's transaction history by selecting that account from the dashboard. The primary account can be changed through the settings menu at any time.

Mobile Application Security: Is the member's data stored on the mobile device?

No sensitive member data is stored locally on the mobile device. Data is cached locally during an active mobile banking session, but no data is stored once the session is terminated. No sensitive data is transmitted from the mobile infrastructure to the local device. Data is encrypted in the transmission between the device and servers.

How is the data encrypted on my device?

All data that flows from the mobile device to the mobile infrastructure and credit union again, is encrypted. Very much like Internet encryption, mobile banking deploys 256-bit SSL encryption. Authentication certificates are deployed within all Malauzai SmartApps and the certificated are issued by VeriSign, just like for the Internet. 256-bit encryption is very strong encryption and it is technically identical for mobile and for when it is deployed on an Internet browser for a desktop computer.

How does the app verify who is logging in?

To comply with Multi-Factor Authentication Guidelines, three (3) factors need to be used when an end-user logs in to a mobile banking application. The first factor, who you are, is the user ID. Each end-user has a primary mobile banking identifier or user ID. The second factor, what you know, is the password. Each end-user establishes a single password. Each time an end-user logs in, they must provide the user ID and password. These fields cannot currently be "remembered" and they must be typed in by the end-user each time they log in to the service. The third factor, what you have, is the device and the SmartApp itself. The mobile banking SmartApp generates an additional application ID. The ID is generated when the SmartApp has been installed and a successful customer validation has taken place on a specific mobile device.

Can I be registered on multiple devices?

Yes. A member can be registered on multiple devices on different platforms. Once an end-users identity is verified, another important event takes place; device registration. The device can be associated with that end-user upon registration. That is important because the device will be used as a way of verifying the user in the future.

Can I use the mobile app to deposit a check if I don't have a checking account?

No, mobile deposit capture is only available to members with a checking account.

If I don't have a checking account will I see the Deposit icon in the mobile app?

Yes. If you try to use this feature you will receive the following error message: "Sorry, a checking account is required to use mobile deposit. Please contact a Member Service Representative to open a checking account."

How long will the listing of previous checks stay in check deposited screen

The check will show in the listing until it is submitted successfully.

Can I get a copy of scanned check?

Yes. You can contact the credit union to receive a copy of your check. All standard check copy fees would apply. See our Fee Schedule.

Will there be a hold placed on my check?

Please refer to our Funds Availability Policy

What do I do if I come across an error in my deposit?

Please contact Member Services, Monday through Friday, 9a.m. to 4p.m. (C.S.T.) at (800) 749-9732.

What items cannot be deposited via the mobile app?

1. Any item that is stamped with a "non-negotiable" watermark.
2. Any item that contains evidence of alteration to the information originally contained on the check.
3. Any item issued by a financial institution in a foreign country or not payable in U.S. Dollars.
4. Any item that is "stale dated" or "post dated".
5. Any third party check, i.e. any item that is made payable to another party and then endorsed to you by such party.

What accounts can I deposit to?

You can deposit only to the checking account you used to log into the mobile app.

Do I endorse the back of the check?

Yes. Endorse and put the account number on the back of your check.

Can I deposit more than 1 check at a time?

No, only one check, per deposit.

What is the minimum amount I can deposit?

There is no minimum amount to use the feature.

Is there a maximum check amount I can deposit?

Yes, \$2,500.

Is there a fee to use Mobile Deposit?

There is NO fee to use Mobile Deposit.

When is the money I deposit available for my use?

Deposits submitted no later than 3:00pm C.S.T M-F will be available by 5:00 pm C.S.T. on the same day.
Deposits submitted after 3:00p.m C.S.T M-F will be available the following business day by 9:00 am C.S.T.
All checks are subject to review.

Will I get an email once the deposit is cleared?

No. If you have a valid email address in GTNet, you will only receive an email if the deposit was rejected. You can also check the app or GTNet and review your checking account history to verify the deposit was cleared.

What happens if a check I deposit and receive credit for is returned for insufficient funds?

The amount will be reversed from your account and you will be charged a regular return check fee. See our Fee Schedule.

What should I do with my paper check?

After depositing your check using Mobile Deposit, please follow these best practice guidelines:

1. Write "Mobile deposit on Date" on the front of your check. The date should be the month, day, and year of your deposit.
2. Securely store your check for 30-days after your deposit, and then destroy it. This allows sufficient time in case the original check is required for any reason.