Consumer Banking User Guide

Getting Started

# Contents

11.13.2017

About the platform

The new platform in online and mobile banking provides an improved account management experience. The interface and features are consistent and intuitive, making managing your information simpler and faster.

You can perform the same tasks with the same basic user interface across each device. These tasks, however, are relative to the device that makes the most sense. For example, you can take a picture of a check for mobile deposits on your phone, but not on a desktop. The graphic below shows the interface on a desktop, a tablet, and a smartphone.

Interface adapts to your device
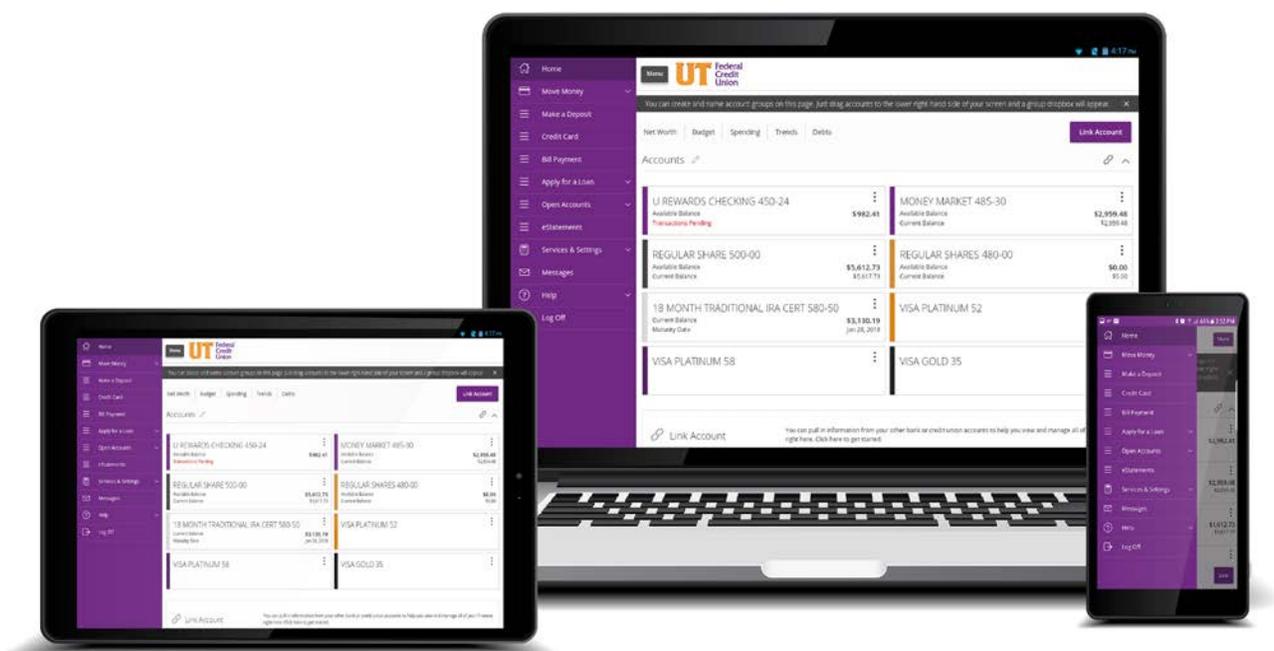
The interface in online and mobile banking adjusts to the unique needs of each device, including screen size and other hardware differences. For example, on tablets and smartphones, the navigation menu is hidden by default. When you need it, you can tap or swipe to display it. In addition, some navigation tools are simplified for use on tablets and smartphones.

When you make a change while using one device, it is reflected in another. If you update a setting in online banking, the same setting takes effect in mobile banking the next time you log in.

Installing the mobile banking app

Install the mobile banking application to use mobile banking on your iOS or Android device. You can download the mobile banking app from the Apple App Store or the Google Play store.

> Caution: To protect your financial information, you should only download and install mobile banking from the Apple App Store or the Google Play store. In the store, verify that UT Federal Credit Union is listed as the seller of the app, not a third party.

To install mobile banking

1. Do one of the following:
    - On an iOS device, open the Apple App Store.
    - On an Android device, open the Google Play store.
2. Search for UTFCU Mobile Banking or UT Federal Credit Union.
3. Install the app.

Opening mobile banking

After installing the app, you can use it to manage your financial information.

To open mobile banking

- Locate the app on your tablet or smartphone and tap the icon to open the app.

Accessing the online banking site

You can use a web browser to connect to the online banking site on a desktop computer or other supported device. It is recommended that you enable pop-up windows in the browser for your online banking site. If they aren't enabled, certain features may appear in separate windows in your browser or may not appear at all.

> Tip: For the best experience with online banking on a tablet or smartphone, use the mobile banking app instead of an Internet browser.

Browser Requirements

Internet browsers—the software application that lets you surf the Web—play a role in protecting your online data. The most common browsers are Microsoft Internet Explorer®, Microsoft Edge®, Mozilla Firefox®, Google Chrome™ and Safari®.

As online fraud and theft evolves, browsers become more secure with each new version. That's why companies that provide Web browsers continually release patches to stay one step ahead of fraudsters. So it's vital that individual users, like you, routinely apply the upgrades to stay protected on your smartphone, tablet and computer.

Always using a current Web browser is vital to keeping the information you share and the sites you visit secure. This includes the financial information you view and exchange while using Online Banking. Knowing you're using the most current version is one of the best ways to give yourself peace of mind.

View the online banking page on the UTFCU website for current browser requirements. (www.utfcu.org/online-banking)
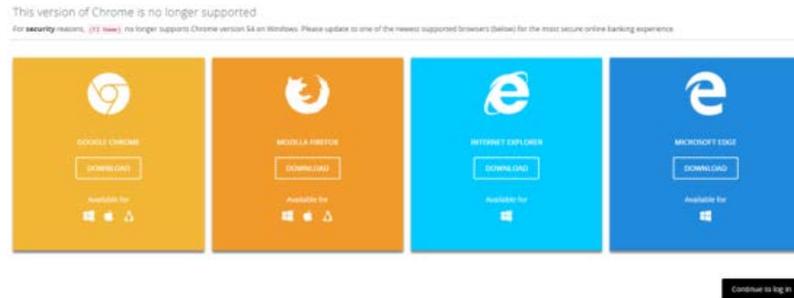
Unsupported browser notification

Continued use of unsupported browsers represents a security risk for users. Unsupported browser notification presents targeted advance notice to users accessing online banking via a browser for which support has been scheduled to end. It facilitates an easy process for installing an up-to-date, secure, and supported browser as a replacement. These three methods will be applied to all future browsers for which support is discontinued:

- **Notification text within online banking** — A notification bar appears at the top of the online banking screen letting you know that for security reasons, we will stop supporting the browser version you are using in the near future. When you see this notification, we recommend that you update your browser.

- **Soft block** — Prior to accessing online banking, a screen appears with notification text, as well as links to supported browsers. You can continue past the soft block to online banking by clicking or tapping **Continue to log in.**

This version of Chrome is no longer supported

For **security** reasons, [??] no longer supports Chrome version 54 on Windows. Please update to one of the newest supported browsers (below) for the most secure online banking experience.

GOOGLE CHROME	MOZILLA FIREFOX	INTERNET EXPLORER	MICROSOFT EDGE
DOWNLOAD	DOWNLOAD	DOWNLOAD	DOWNLOAD

Continue to log in

- **Hard block** — Similar to soft block, however, hard block does not include the option to continue to online banking. You must upgrade your browser to a current version or select another supported browser.

Moving forward, browsers will continue to be evaluated. The appropriate date to end support for a particular browser will be based on several factors:

- The vendor's official end-of-support date for security patches
- The quality of the user's experience on that browser in online banking
- The percentage of users still leveraging that browser version

Logging in overview

When you login to online and mobile banking, enter the following when prompted:

- Login ID
- Password

If you enter an incorrect password too many times, your account will be temporarily suspended and you will not be able to log in. If your login ID is blocked, contact UTFCU to unblock your login ID.

Note: If you try to log in without a recommended Web browser, you will be directed to a website where you can download a supported browser. View the online banking page on the UTFCU website (www.utfcu.org/online-banking) to learn more about the latest browser requirements.

If you have never used a particular browser or device to log in, you may need to request a Secure Access Code (SAC) to use it. If the Web browser or device is one that you plan to use again, you can register it. By registering a browser or a device, you confirm that it is under your control and that you intend to use it to access online banking or mobile banking.

If the secure access code contact methods (that is, the email address and phone numbers where the secure access code can be sent) that are available to choose from are not correct or accessible from your location, please contact UTFCU for assistance.

See the "Registering a browser or device" section of this document for more information.

Logging in for the first time

The login process for online and mobile banking requires a Secure Access Code.

When you use a Secure Access Code, we send a one-time code to an email address, text message number, or phone number that is on file for you.

Note: If you're an existing online banking user and do not know your login ID, contact UTFCU to determine what your login ID is. If you're new to online and mobile banking with UTFCU and need to enroll, click on the **New User Registration** link on the login page.

To log in for the first time with a Secure Access Code

1. On the Login page, do the following:
   a) Enter your **Login ID**.
   b) Click or tap **Submit**. The Select Secure Access Code Target page appears.
2. On the Select Secure Access Code Target page, click or tap one of the contact methods to send a secure access code. The Enter Secure Access Code page appears.
3. On the Enter Secure Access Code page, do the following:
   a) When the code arrives, enter the code.
   b) Click or tap **Submit**.
   c) If prompted to register the device, click or tap **Register Device** if you want to register the device and browser for future use without a Secure Access Code.
4. Enter a password, then re-enter it in the **Confirm Password** field.
5. Click or tap **Submit**.
6. Your current contact information will appear as view only. If any of the information needs updated, visit the Manage Contact Info menu item.
7. Read the agreement on the Disclaimers page and click or tap **I Accept**. When you accept the agreement, the Home page appears.

Logging in after the first time

When you log in, enter your login ID and password. If you use a browser or a device that is not registered, you must also enter a Secure Access Code.

To log in after the first time

1. On the Login page, enter your **Login ID**.
2. Enter your **Password**.
3. Click or tap **Sign In**. When the connection is complete, the Home page appears.

Registering a browser or device

A conventional authentication system relies on two forms of identification to prove your identity: your login ID and your password. Multi-factor authentication uses multiple forms of identification to make it harder for attackers to access your account. The multiple forms of identification can include something that you know, such as a password, and something that only you have.

In online and mobile banking, we can send a secure access code to a contact address that you configure. The code is only valid for a single use and it expires after a short time. You choose one of the following ways to deliver the code:

Secure access code delivery methods

Method	Details
Phone	The system calls the telephone number on file. You answer the phone normally and make a selection to hear the code. If necessary, you can repeat the code. The system does not leave the code on voice mail. If you miss the call, you can request a new code.
Text (SMS)	The system sends a text message with the code. Standard text messaging fees apply.
Email	The system sends a short email with the code. Depending on the configuration of the filters on your mail server, the message may be in your junk or spam mailbox.

Whenever possible, you should configure phone and text delivery methods, and leave email unconfigured. Attackers can use viruses or other malicious activity to compromise your email and view the secure access code. If you do not configure an email address as a Secure Delivery Contact, you can help prevent this type of attack.

If you have never used a particular browser or device to log in, you may need to enter a Secure Access Code to use it. If the browser or device is one that you plan to use again,

you can register it. By registering a browser or a device, you confirm that it is under your control and that you intend to use it to access in online banking or mobile banking.

Tip: Multiple users can register the same browser or device.

You will need to register your browser or device again in the following circumstances:

- You use a different browser on your desktop.
- You delete and reinstall the mobile banking app.
- Your browser does not save browser cookies.
- You clear existing browser cookies.
- We reset registration for all users for security reasons.

Caution: Only register a browser or device if it is under your control. Do not register a browser on a public computer.

Passcode

You can set up a Passcode that can be used on a mobile device in lieu of a login ID and password.

Before enabling this feature on a mobile device, you must first log in to your mobile banking app and follow the Secure Access Code process. After successfully logging in and registering the device, you can enable the four-digit passcode feature on the Login or Security Preferences pages.
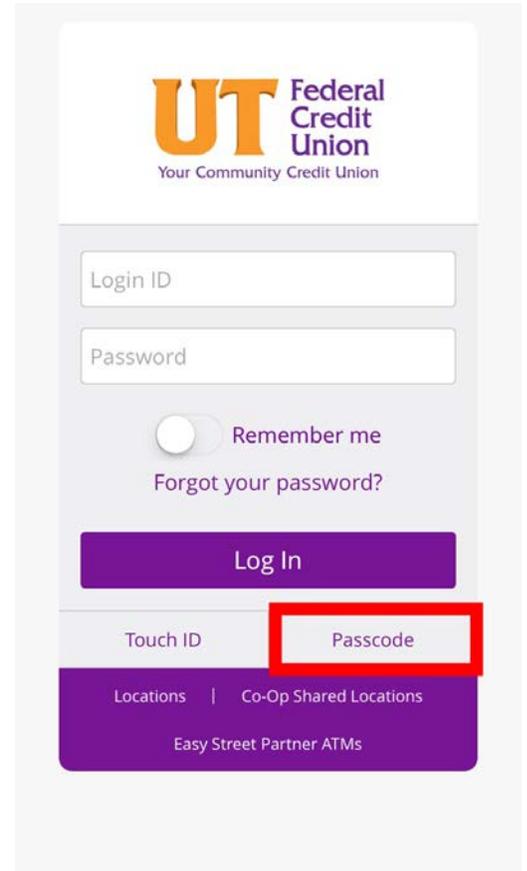
Note: Only one registered user per mobile device can enable this feature. If another user already enabled the feature, the related option on the Security Preferences page will appear dimmed.

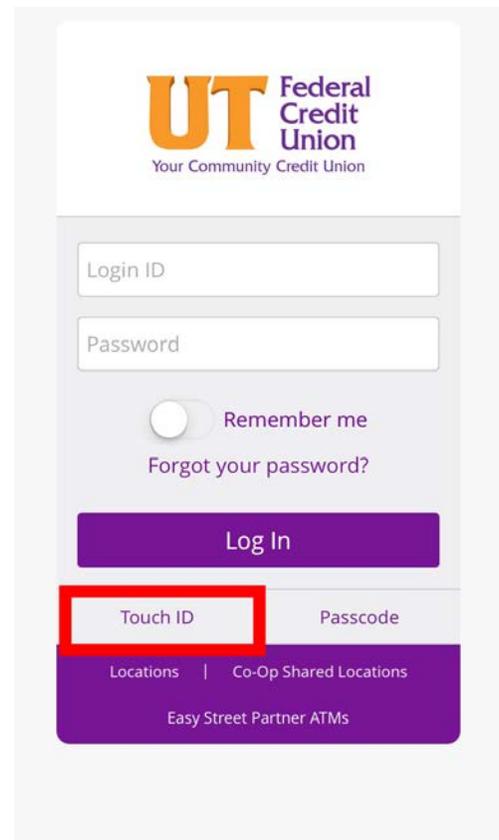# Logging in with Touch Authentication

You can use the Touch Authentication feature to log in using your mobile device's fingerprint sensor rather than a login ID and password.

If your Apple or Android mobile device has a fingerprint sensor and is operating on a supported OS version, you can log in by using your fingerprint. Only one fingerprint can be registered to an account. The fingerprint is encrypted and stored on the mobile device only and is not made available to any other service providers, including UTFCU.

Caution: You must set up fingerprint authentication on your device before logging in. For iOS, refer to https://support.apple.com for more information on setting up Touch ID on your device and scanning a fingerprint for the first time. For Android, refer to http://developer.android.com for more information on fingerprint authentication.

To enable Touch Authentication settings

1. On the Login page, tap **Touch ID**.

2. On the page explaining the fingerprint authorization feature, tap **Enroll Now**.
3. On the Touch Authentication page, do the following:
   a) Enter the **Login ID**.
   b) Enter the **Password**.
   c) Tap **Authorize** to finalize changes.

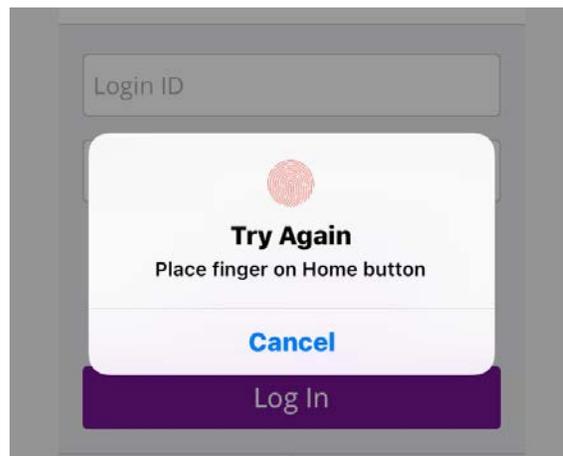4. Place your finger on the Home button to capture your fingerprint.

To log in with Touch Authentication

> Note: Touch Authentication is tied to your online banking password. Therefore, if you change your password for online banking, you must disable fingerprint authentication, then enable it again to be able to log into online banking with Touch Authentication.

- On the Login page, do the following:
    - Touch the Home button with your enrolled finger. If fingerprint authentication doesn't recognize your finger, a message will prompt you to touch the button again.
    - (Optional) Select the **Remember me** check box to save your login ID for the next time that you log in. When the connection is complete, the Home page appears.

> Note: After five failed attempts, you'll be given the option to enter your account password. You will also have to enter your password after you restart your device, or enroll or delete fingerprints.

Disabling Touch Authentication

If you want to stop using Touch Authentication to log in, you may change the Touch Authentication settings. After changing the settings, you can use a login ID and password to access the site.

The mobile login screen offers all login methods supported by UTFCU. The last method you used is the one you will be prompted to use again the next time you log in. However, other

options are always available on the login page, so you can switch between login methods at any time.

To disable Touch Authentication

1. On the Login page, touch the Home button with your enrolled finger. If the Touch ID sensor does not recognize your finger, a message will prompt you to touch the button again. The Home page appears.
2. Click or tap **Services & Settings** > **Security Preferences**. The Security Preferences page appears.
3. In the Touch ID (iOS)/Fingerprint Authentication (Android) row, click or tap **Off** to turn off touch authentication. A message appears asking for confirmation. Click or tap **Yes** to confirm the setting. The Security Preferences page appears.

Logging off overview

Logging off online and mobile banking is an important part of keeping your financial information secure. You can log off voluntarily when you finish using online and mobile banking. In addition, online and mobile banking can log you off involuntarily after a certain amount of time elapses.

If you navigate from online banking to another site and do not close the browser, you may remain logged in until the session ends. This can make it possible for someone else to access data from your previous online banking session. The session ends when you log off, close your browser, or close the mobile banking app.

Caution: To maximize the security of your online information, you should always log off to end your online banking session.

Logging off voluntarily

In online banking, you should always log off before you close the browser window. In mobile banking, you should always log off before you open another app on your tablet or smartphone.

To log off

- In the navigation menu, click or tap **Log Off**.

Involuntary log off after session timeout

To help ensure your security, we automatically log you off when you have been logged in for an extended period. This session timeout is designed to protect the security of your financial information. There are two types of session timeouts.

Session timeout types

Timeout type	Notes
Logged in but inactive	Protects you if you are logged in and inadvertently leave your device. A warning message appears to give you a chance to stay logged in. If you miss the warning message, you can immediately log back in on the same browser or device by re-entering your login credentials, restoring your session and any tasks that you were working on. This window is only available for a short period of time. If you enter an incorrect password, any pending work is discarded.
Logged in but exceed session time limit	Limits the maximum time of any session. When the maximum session time ends, you are prompted to log off manually. If you do not log off manually, the system will automatically log you off.

Resetting a forgotten password

If you forget your password and your account is not locked, you can use the Forgot Your Password option on the Login page to reset your password. Depending on the configuration, you may not be able to reset your password from an unregistered browser.

To reset a forgotten password

1. On the Login page, do the following:
   a) Click or tap **Forgot your password?**
   b) Enter your login ID.
   c) Click or tap **Submit**.
2. Click or tap the destination you would like to receive your **Secure Access Code**. If the destination options do not contain accurate contact information, contact UTFCU for assistance.
3. On the Secure Access Code page, enter the code and click or tap **Submit**. The New Password page appears.

Note: If you close out of a session after receiving a secure access code, but before you enter it in the application, and then open it within a very short time frame, click or tap **I already have a Secure Access Code**.

4. Enter your new password.
5. Re-enter the password in the **Confirm Password** field.
6. Click or tap **Submit**. The Home page appears.

Note: If the **Remember Me** check box is selected, it will block you from entering a different login ID.

Password tips and recommendations

A strong password helps you protect your account. To create a strong password, keep the following guidelines in mind:

- Create unique, original passwords.
- Use the longest practical password.
- Use a mix of upper and lower case letters.
- Include one or more numbers.
- Do not use repeating or adjacent characters.
- Use at least one of these special characters: `` `~!@#$%^&()_+={}| []:"?,./\. ``
- Avoid using software or toolbars that store your password.
- Change your password regularly.

Remember to avoid the following password pitfalls:

- Do not choose passwords or security codes that others can easily guess.
- Do not reuse passwords for multiple sites.
- Never use your account numbers.
- Do not use personal contact information, such as addresses or phone numbers.
- Do not use personal information, such as your name, birthday, Social Security Number, passport number, or the names or information for family members or friends.
- Do not use sequences of characters such as *1234567* or *abcdefg*.
- Do not rely on look-alike substitutions of numbers or symbols alone. Passwords like *P@ssw0rd* are easy to guess, but can be effective when you also change the case of the letters, the length of the words, and misspellings, or when you use multiple unrelated words in a phrase.
- Do not use dictionary words.

Tip: Go to support.microsoft.com for more information on creating strong passwords. We do not endorse or guarantee the site.

Navigating the Home page

When you log in, the Home page appears. On any device, the Home page includes the navigation menu, the Account Overview, and the Sidebar.

You can view the Home page at any time.

To view the Home page

- In the navigation menu, click or tap **Home**.

The Home page includes some or all of the following:

- Menu
- Account overview with the name and balance of each of your accounts
- Sidebar with Quick Actions and other information
- Your last login date and time
- Account Summary graph that displays the balances in your accounts

> Note: The Account Summary graph is only available on desktop and tablet due to mobile space restrictions and graph dimensions.

- System notifications for online banking or mobile banking
- Personal Financial Management (PFM) links

Using the menu

You can use the options in the navigation menu to perform multiple tasks. The navigation menu is always available to the left of or above the page you are viewing on a desktop. The order of the items in the navigation menu may vary, but the following items should normally appear based on your access to the functions.

Item	Notes
Home	Review account summaries on the Home page.
Move Money	Transfer funds, make a loan payment, transfer to any member, Person 2 Person transfer, withdraw by check, view online activity.
Credit Card	Link to access UTFCU credit cards.
Bill Payment	Link to access BillPay site.
Commercial	Create and manage Business payments.
Apply for a Loan	Apply for a credit card, person loan, vehicle loan, home equity, or mortgage.
Open Accounts	Open a checking account, savings account, or share certificate.
eStatements	View your official UTFCU statements.
Services & Settings	Stop check payments, order checks, manage alerts, view UTFCU locations, edit your profile, and configure alerts.
Messages	Securely message UTFCU.
Help	Access help documentation.
Log Off	Securely log off banking.

On a tablet or a smartphone, the navigation menu does not always appear. Tap the Menu button or swipe from the left edge of the screen to show it. Tap the Menu button again or swipe to the left edge of the screen to hide it.

Viewing accounts

On the Home page, the Accounts area lists every account whose history you can view. For each account, you can see the account name, the last few digits of the account number, and the balance. Accounts that include a label (External) are serviced by a third-party vendor and will open a new window in order to display transaction information.

If you configure nicknames for accounts in **Settings** > **Account Preferences**, the nicknames appear. You can drill down into any account to see account details, where 100 transactions are displayed per page.

Accounts overview

Accounts ✎	🔗 ∧

U REWARDS CHECKING 550-24 ⋮	MONEY MARKET 485-55 ⋮
Available Balance **$982.41** Transactions Pending	Available Balance $2,959.48 Current Balance $2,959.48

REGULAR SHARE 500-00 ⋮	REGULAR SHARES 480-55 ⋮
Available Balance $5,612.73 Current Balance $5,617.73	Available Balance $0.00 Current Balance $5.00

18 MONTH TRADITIONAL IRA CERT 550-55 ⋮
Current Balance $3,130.19 Maturity Date Jan 28, 2018

When you click or tap an account with the External label, a new page linked to a third-party vendor opens in either a new browser tab or a window overlay on the Home page.

Viewing the Sidebar

The Sidebar includes some or all of the following:

- Quick Actions
- Rates
- Required approvals
- Deposit check history
- Other information from UTFCU

On a tablet or a smartphone, the Sidebar does not always appear.

To view the Sidebar in mobile banking

- Do one of the following:
  - Tap **More** on any page.
  - Swipe from the right edge of the screen.

To hide the Sidebar in mobile banking

- Do one of the following:
  - While the Sidebar is visible on any page, tap **More**.
  - Swipe to the right edge of the screen.

Using the grid and list views

Some pages in online and mobile banking include information in either a grid or list view.

You can change between the grid and list views at any time. The grid view and list view include the same information.

To switch between the grid and list view

- Click or tap the grid icon (▦) or the list icon (☰). The view changes.

Account information on the Home page

The following information may appear on the Home page for each account:

Account information on the Home page

Name	Description
Account name	The default name for the account or a custom nickname that you create in Services & Settings> Account Preferences.
Account number	The masked account number. For your security, only the account name, last part of number, and share ID may appear. For example, regular checking account number 123456789 with a Share ID of 20 may appear as Checking 789-20.
Balance	The balance and balance type (Available and Current) for the account.
External	A label (⧉ External) indicating an account serviced by a third-party vendor.

Tip: If the Home page includes the Asset Summary graph, you can click or tap the segment of the graph that represents an account to view account information.

To hide or show the Account Summary graph

1. In the Account Summary area, click or tap the hide/show icon (⌃). The Account Graph disappears.
2. (Optional) Click or tap the hide/show icon again (⌄) to display the graph.

Grouping accounts

You can use the Account Grouping feature to categorize accounts on the Home page—both internal accounts within UTFCU, and external accounts that are aggregated via the Personal Financial Manager (PFM).

To create a new account group, click or tap an account and drag it to the New Group icon (⊙) that will appear in the lower-right corner of the screen while an account is being moved.
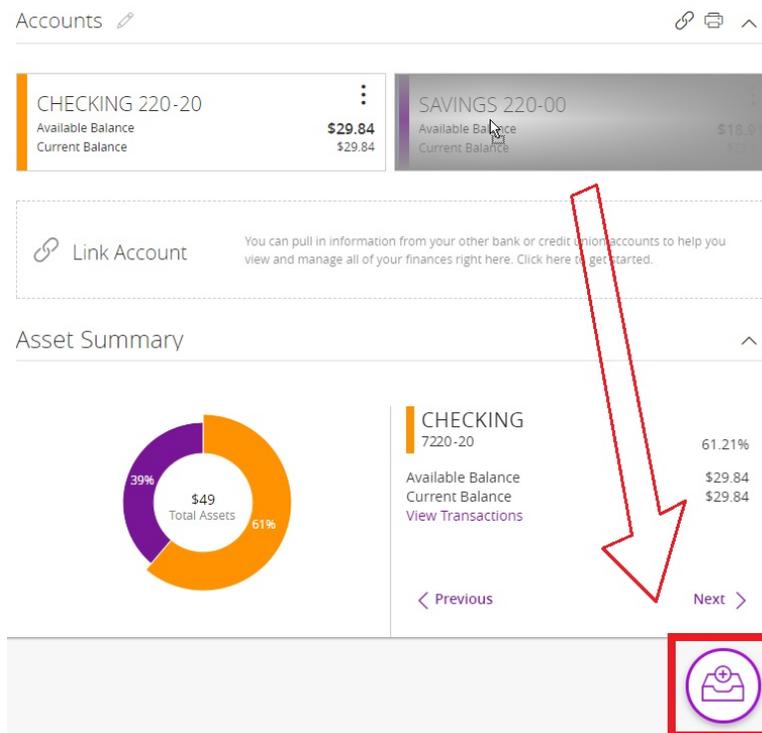
When the card is "dropped" on the New Group icon, the following field appears. Enter a name for the new group and click the check mark button to save the changes.

New Group   ✕   ✓

You can easily rename a group by clicking the pencil icon (✎) to the right of the title, editing the name, and clicking the check mark button to save the changes.

To move accounts to different groups you have created, click on an account, hold the mouse button, drag the card to the desired location, and release the mouse button. On a mobile device, tap an account, drag it, and lift your finger to drop it in that location.

Account grouping – Home page