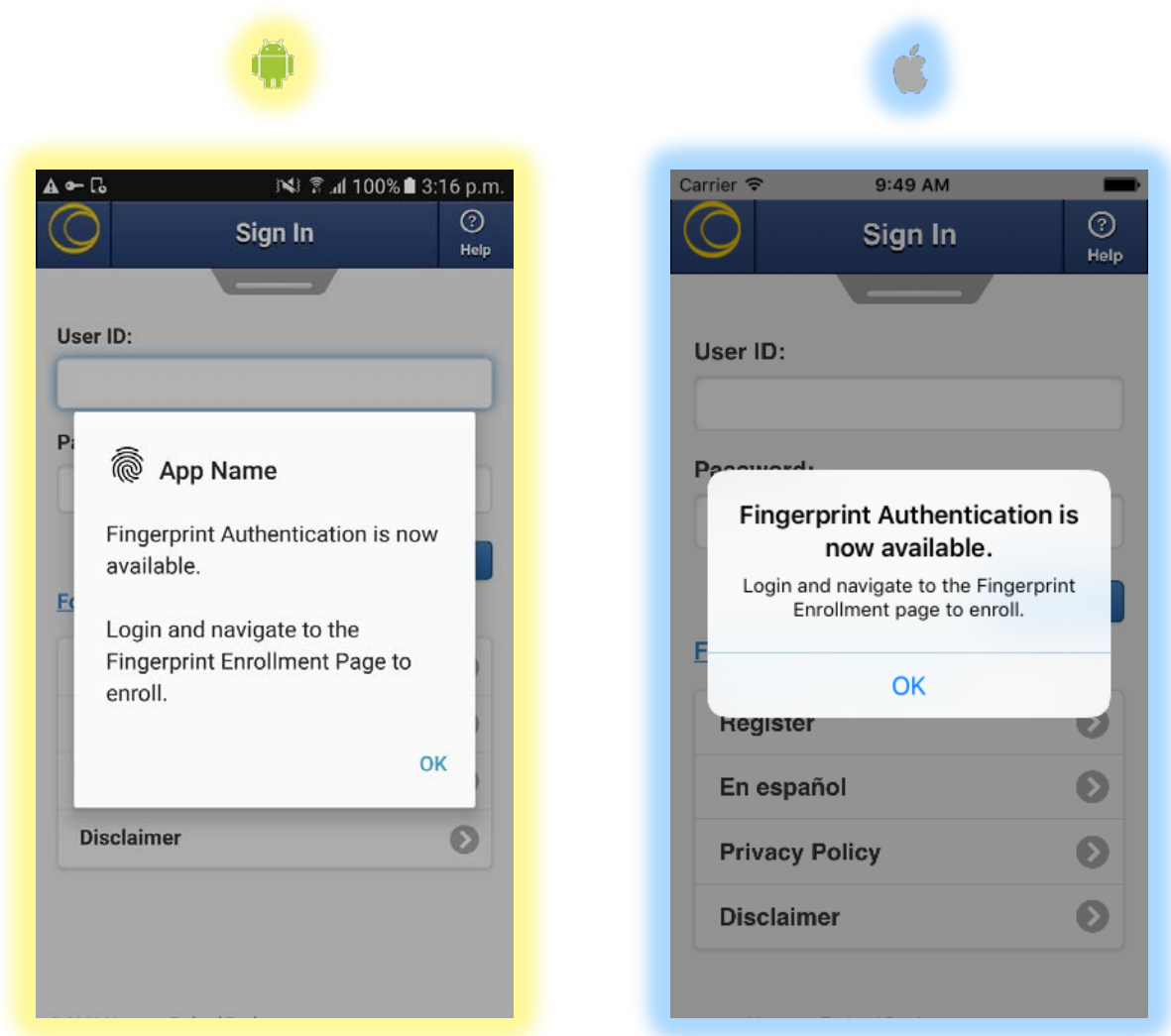


## TO ENABLE FINGERPRINT AUTHENTICATION

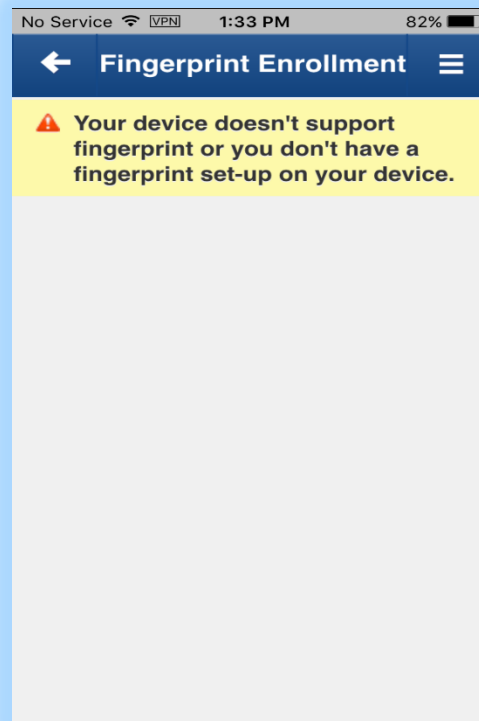
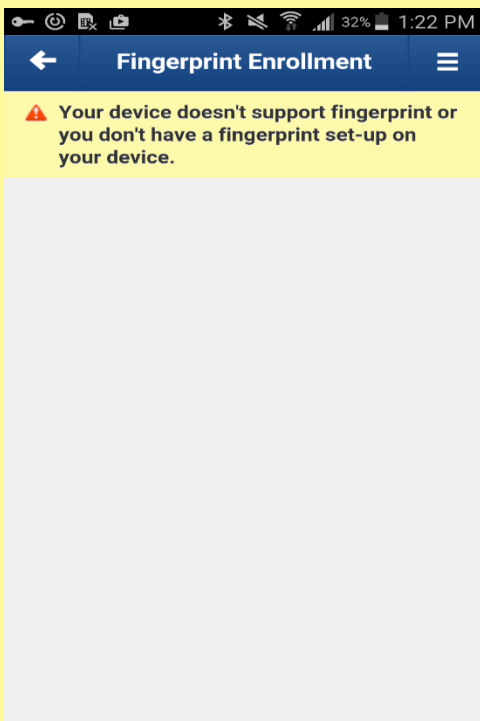
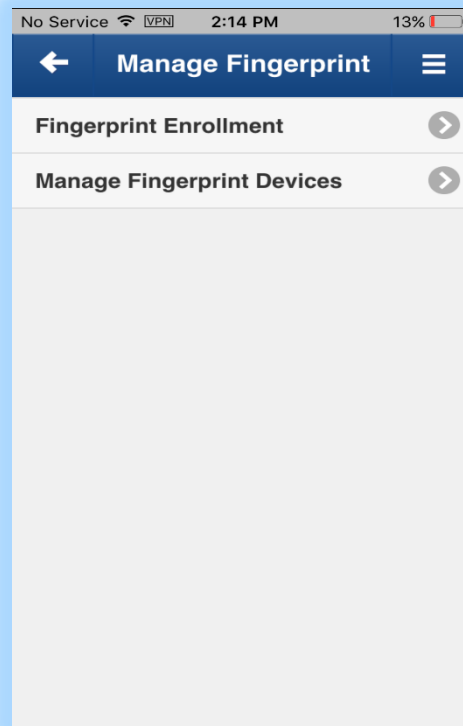
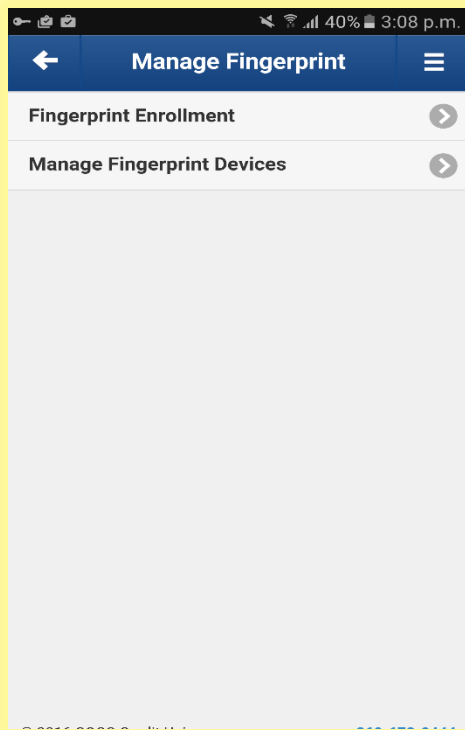
When end user first launches the iMobile app, the app will determine whether the device has Fingerprint support. If so, the First time fingerprint authentication availability prompt is displayed **“Fingerprint Authentication is now available to access your Milford Federal app”**.

On iOS the app checks to see if the device is fingerprint enabled **and** if it has fingerprints registered with Touch ID. If so then the Fingerprint Authentication availability prompt is displayed.



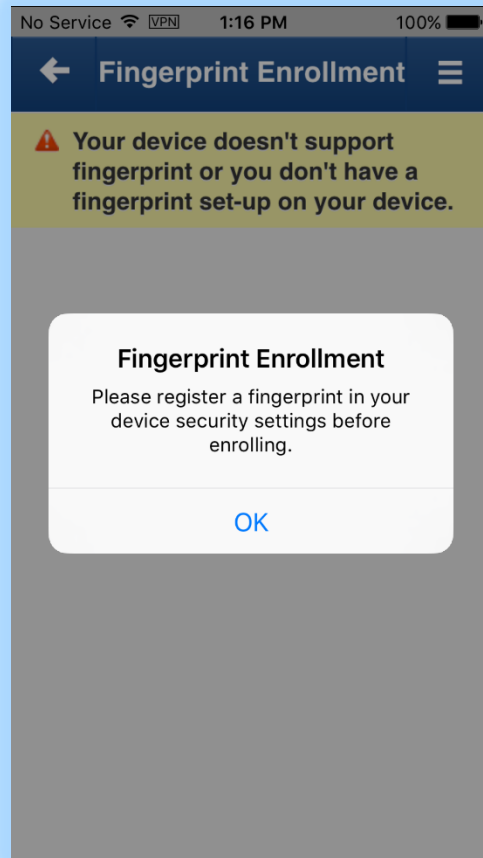
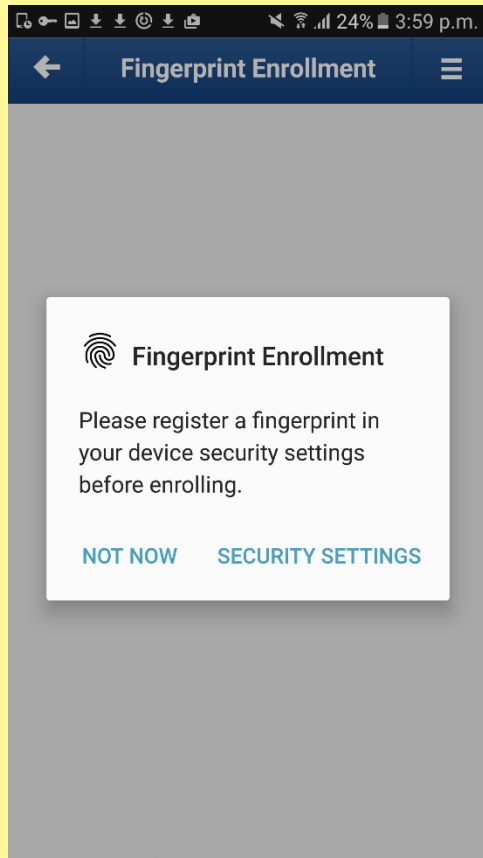
\*Note – These screens are only displayed on the initial install and launch of the app (for Android devices), and on initial launch and validation that a fingerprint is registered on iOS. All other times the user must enable/disable fingerprint authentication from the “Fingerprint Enrollment” menu under Mobile Services → Manage Fingerprint.

After a user selects the “Manage Fingerprint” menu two options are displayed: “Fingerprint Enrollment” and “Manage Fingerprint Devices”. *The Enrollment page will notify the user if the feature is unavailable.*



## Regular Sign in attempts (Device supported, no fingerprint stored on device)

There may be situations in which devices support Fingerprint Authentication, but where no fingerprint is stored on the device yet. If this is the case, when the end user goes to the Fingerprint Enrollment page, they will be prompted to register a fingerprint.

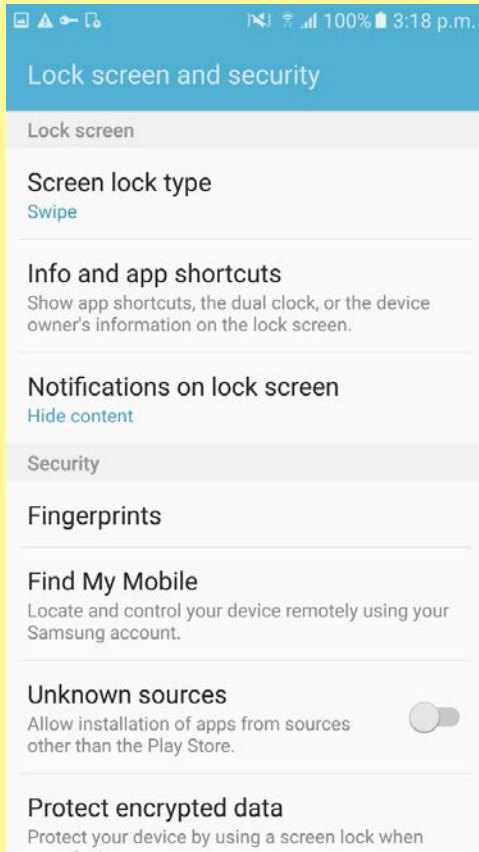


End users will then need to go into their device settings pages to add a fingerprint. After a fingerprint is added, the user would go back to the Fingerprint Enrollment page to enroll in Fingerprint Authentication.

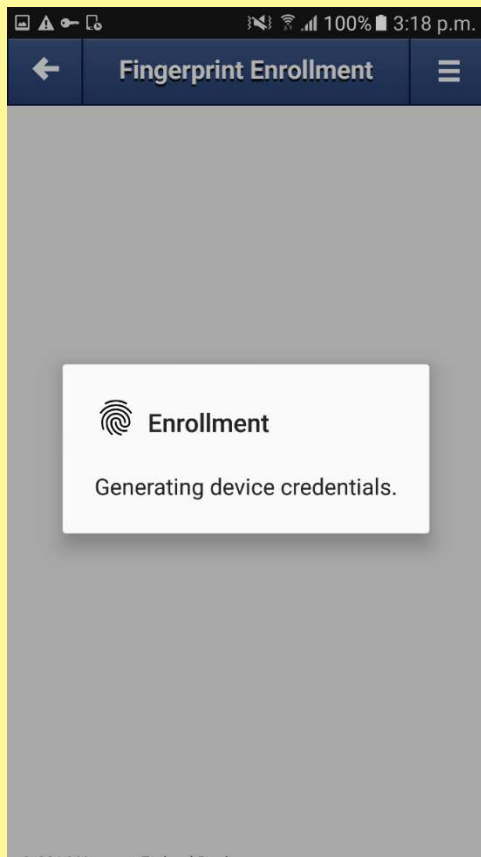
*\*Fingerprints are checked during the enrollment phase because they are required to exist prior to generating the credentials. It is not possible to enroll without a fingerprint even if the device supports fingerprint enrollment.*

On Android, we can navigate to the device's settings from the pop-up message. This isn't available on iOS. Below are sample images from the device's Security Settings page. Please note that each Android Manufacturer, may have a different Security Settings page. So the image below is just a sample. In general the device fingerprint management

screens would be located in the settings app and either under device “Security” or “Lock Screen and Security”. For iOS it will be located in the settings app under “Touch ID & Passcode”.



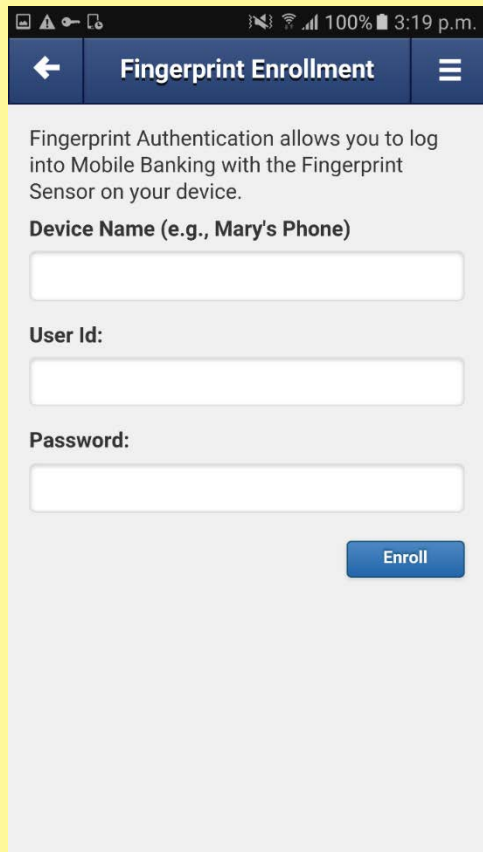
Navigating back from Security Settings refreshes the page and generates the credentials.



**Note: Corresponding image not visible in iOS.**

## Fingerprint Enrollment:

After navigating to the Fingerprint Enrollment page, the end user is presented with the following screen in which they would enter a device name and confirm their existing iBanking User ID and Password.



The screenshot shows a mobile app interface for Fingerprint Enrollment. The status bar at the top indicates 100% battery and 3:19 p.m. The app bar has a back arrow, the title "Fingerprint Enrollment", and a menu icon. The main content area contains the following text and form elements:

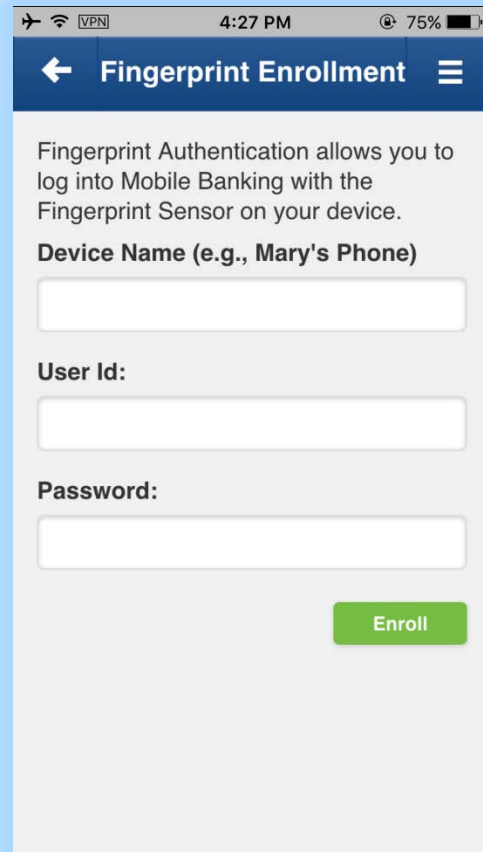
Fingerprint Authentication allows you to log into Mobile Banking with the Fingerprint Sensor on your device.

**Device Name (e.g., Mary's Phone)**

**User Id:**

**Password:**

**Enroll**



The screenshot shows a mobile app interface for Fingerprint Enrollment. The status bar at the top indicates 75% battery and 4:27 PM. The app bar has a back arrow, the title "Fingerprint Enrollment", and a menu icon. The main content area contains the following text and form elements:

Fingerprint Authentication allows you to log into Mobile Banking with the Fingerprint Sensor on your device.

**Device Name (e.g., Mary's Phone)**

**User Id:**

**Password:**

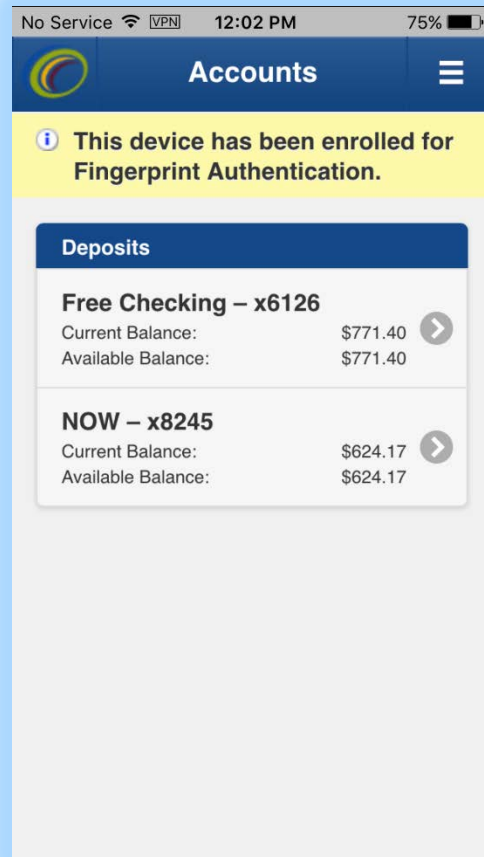
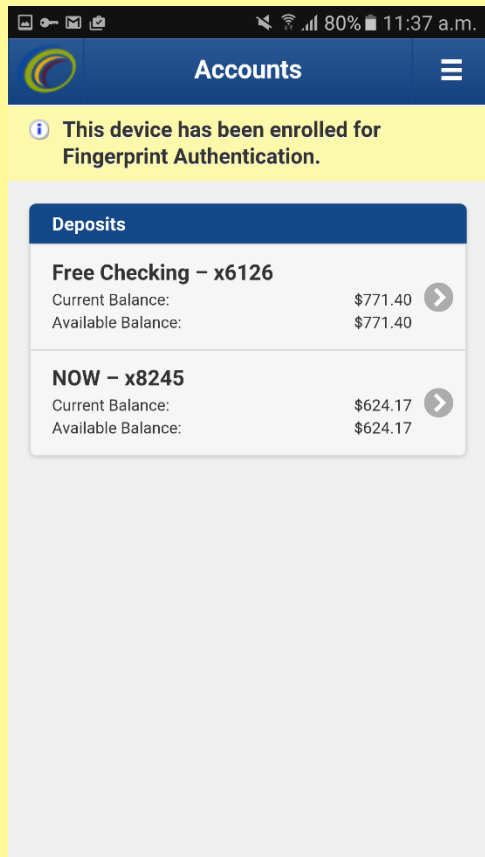
**Enroll**

### *\*Please Note:*

- *It is suggested for users to enter a unique descriptive device name, since iBanking will allow duplicate entries. For Ex: If an end user and their spouse both have an iPhone 6 and both enroll in Fingerprint Authentication access to the same account, then there will be 2 iPhones listed in device management with the same name.*
- *The user would enter their iBanking credentials here.*
- *Currently the end user can register up to 5 devices.*

## Post Device Enrollment

After the user has filled out the required fields to enroll their device in fingerprint authentication, the page will refresh and load with the 'Accounts' page where they will see a message at the top indicating their successful enrollment for the feature.



If a user navigates to the enrollment page after already having enrolled their device, they will see the device name and a “Manage Devices” button which will bring them to the “Manage Fingerprint Devices” page. If a user has added a new fingerprint to their device (or deleted their device from the device management page, they must unenroll via this page using the Unenroll button.

This screenshot shows the 'Fingerprint Enrollment' screen for a device named 'S7'. The status bar at the top indicates a signal, 35% battery, and the time 2:03 p.m. The header bar is blue with a back arrow, the title 'Fingerprint Enrollment', and a menu icon. The main content area has a light gray background and contains the text 'Unenrolling will disable Fingerprint Authentication on this device.' followed by the label 'Device Name' and a text input field containing 'S7'. At the bottom, there are two buttons: 'Manage Devices' and 'Unenroll'.

← Fingerprint Enrollment

Unenrolling will disable Fingerprint Authentication on this device.

Device Name

S7

Manage Devices Unenroll

This screenshot shows the 'Fingerprint Enrollment' screen for a device named '6plus'. The status bar at the top indicates 'No Service', VPN, 12:20 PM, and 22% battery. The header bar is blue with a back arrow, the title 'Fingerprint Enrollment', and a menu icon. The main content area has a light gray background and contains the text 'Unenrolling will disable Fingerprint Authentication on this device.' followed by the label 'Device Name' and a text input field containing '6plus'. At the bottom, there are two buttons: 'Manage Devices' and 'Unenroll'.

← Fingerprint Enrollment

Unenrolling will disable Fingerprint Authentication on this device.

Device Name

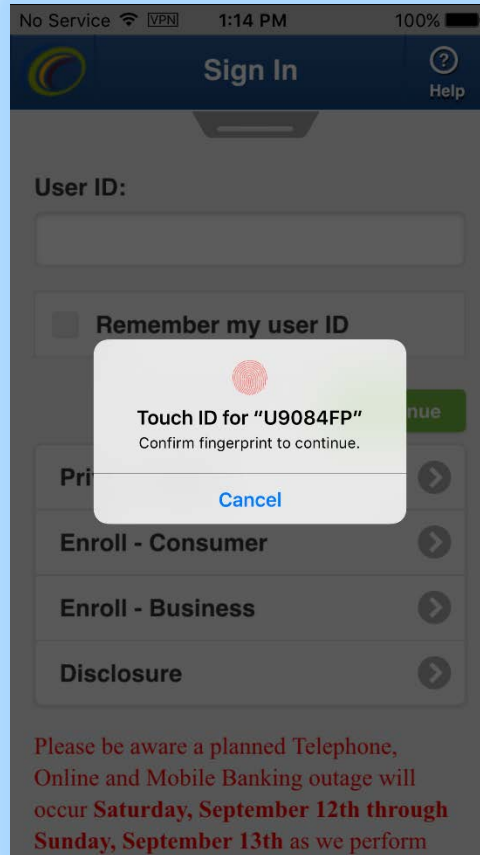
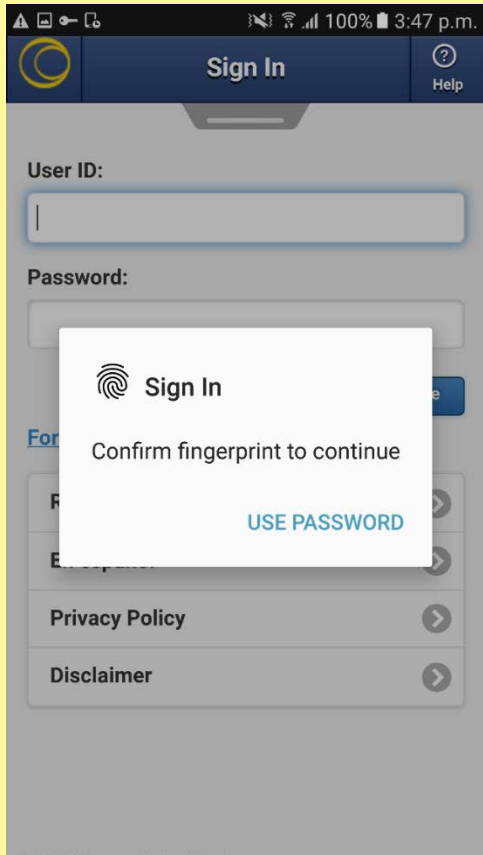
6plus

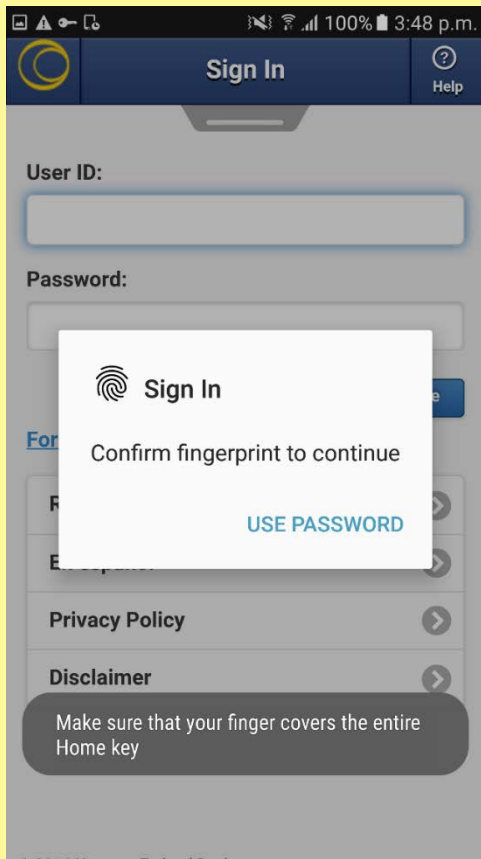
Manage Devices Unenroll



## Failed Sign In with Registered Fingerprint

If an end user has difficulty with their fingerprint, the device's existing process for fingerprint access will apply. Whether that be a device being locked out for a certain timeframe or needing to use a password or pattern to enter the device. The iMobile app will also prompt the end user to Sign In with their iBanking password and will be able to use their fingerprint once again at next Sign In.



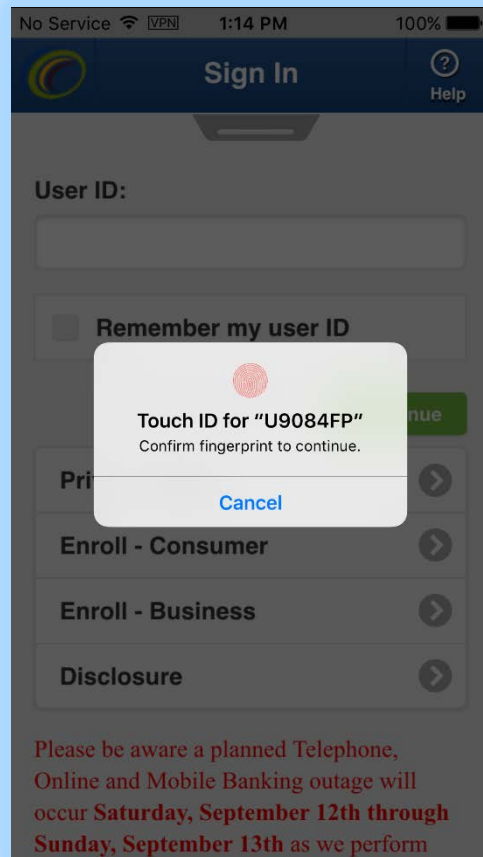
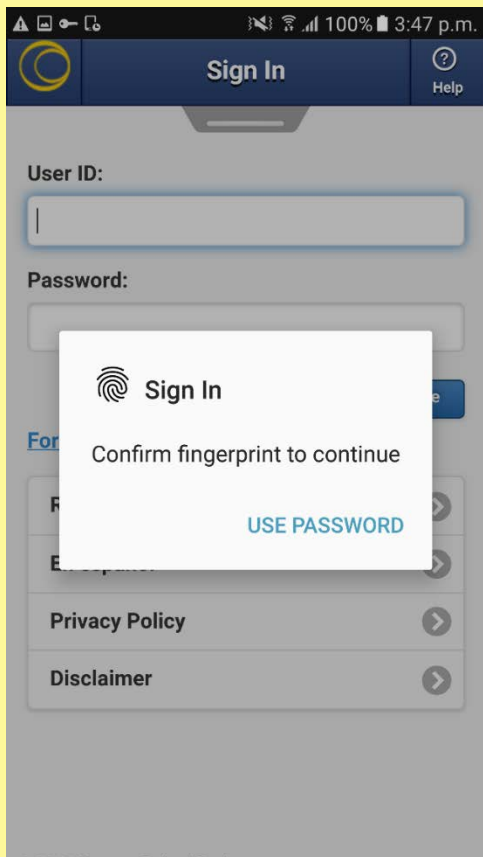


**Note: Corresponding image not visible in iOS.**

*\*Note: Helper messages issued by Android are also displayed (these messages are not available on IOS).*

## Regular Sign In (After Fingerprint is enabled)

Below is what end users will see after their device has been registered and when they attempt to Sign In to the iMobile app using Fingerprint recognition or the regular User ID and Password.

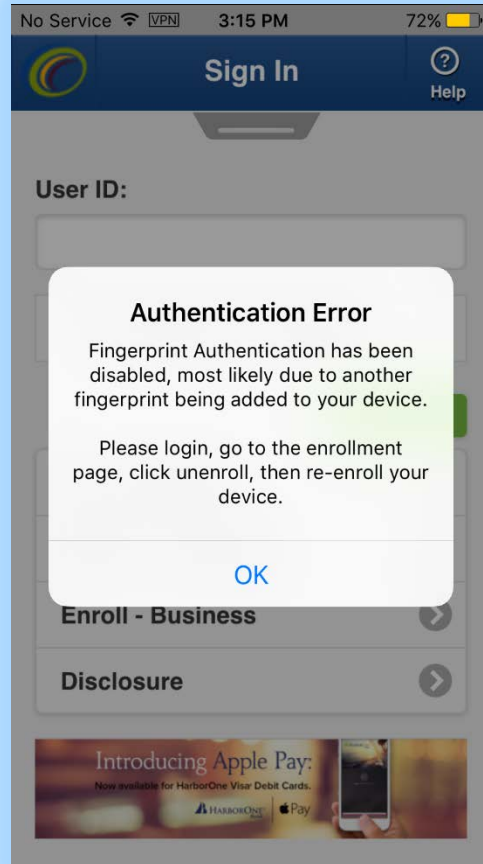
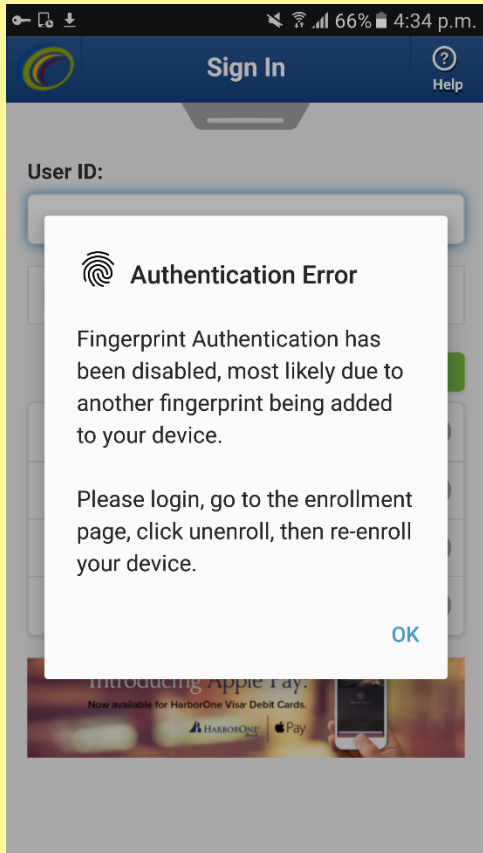


*\*Note: Currently 5 devices per user are allowed*

## New Fingerprint Added to Device:

The following screens will be visible to end users in various situations:

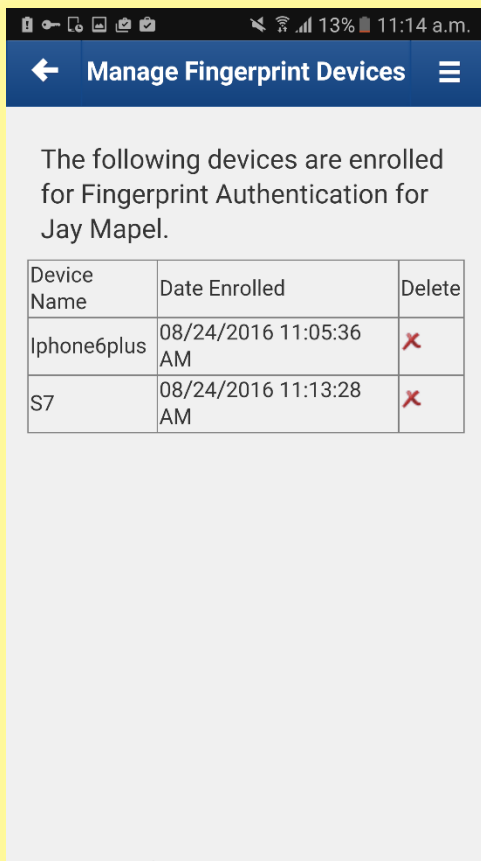
- *If a new fingerprint is added to the device.*
- *All fingerprints are deleted from the device (Android).*
- *The device is deleted from device management.*



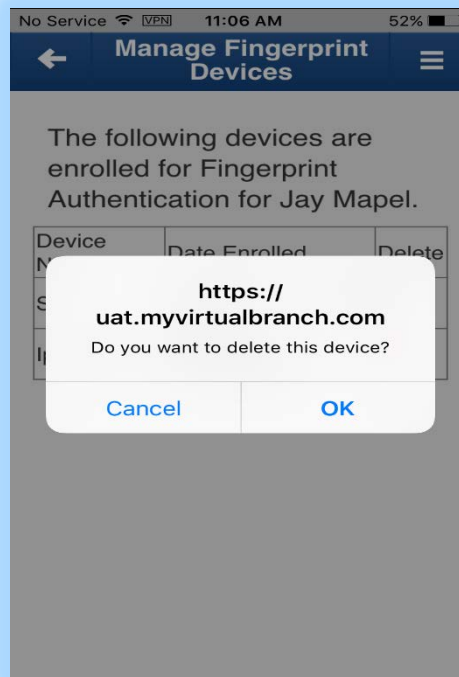
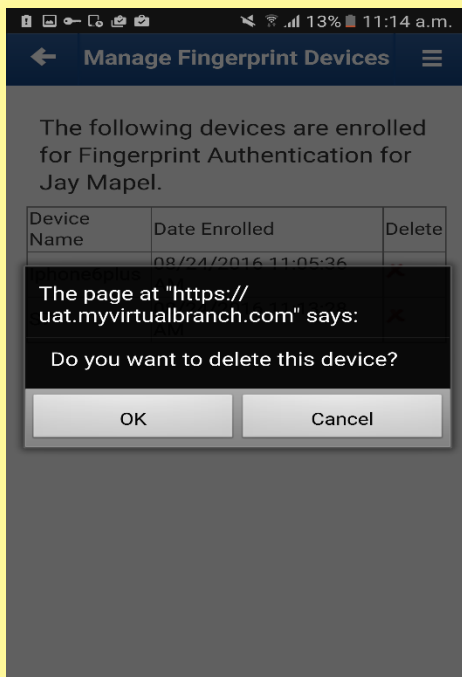
## Unenrolling in Fingerprint Authentication:

Users will be able to unenroll/ delete their devices using the following methods:

1. By using the mobile app and navigating from the: Sign In page → Mobile Services → Manage Fingerprint → Fingerprint Enrollment → Click “Unenroll”.
2. Using the mobile browser to Sign In into their accounts and navigate to the “Manage Fingerprint Devices” screen shown below or the Fingerprint Enrollment page.
3. Using a PC and navigating to the desktop version of “Manage Fingerprint Devices” shown in the next section.
4. If the end user deletes their device from the Mobile app using the Manage Fingerprint devices screen (Mobile Services → Manage Fingerprint → Manage Fingerprint Devices → Click the red ‘x’ in the delete column that corresponds to the device you wish to delete), the next time that device attempts to Sign back in, they will be unable to use the registered device fingerprint and must unenroll their device from the Fingerprint Enrollment screen.



The following confirmation prompt is displayed when deleting a device.



Once the user confirms to delete the device, the page will refresh and display as shown below:

