Mobile Passcode and Touch ID

Through TB&T Mobile Banking, users have the ability to access multiple features via their mobile devices. Mobile Passcode and Touch ID increase the speed of access to key features since a user will be able to enter a short set of digits instead of a full username and password to authenticate. This increases convenience while still maintaining the security of financial information.

Mobile Passcode and Touch ID allow quick access to these features of Mobile Banking:

- ✓ **Account Balances**
- ✓ **Account Activity**
- ✓ **Transfers**
- ✓ **Mobile Deposit**

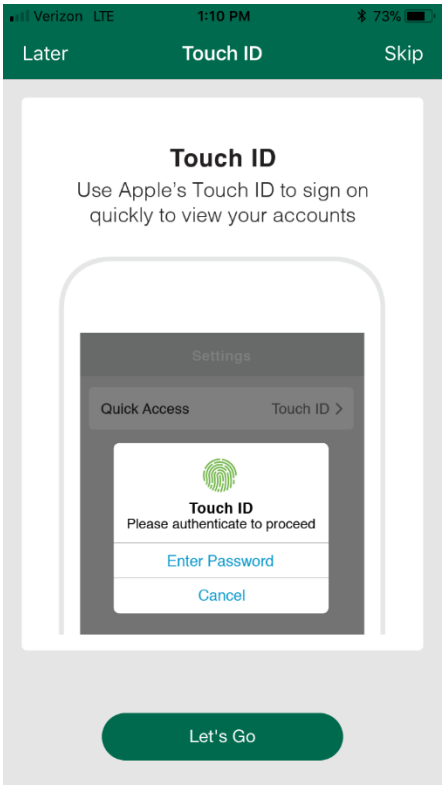
Username and Password must be entered to access these features of Mobile Banking:

- ✓ **Bill Pay***
- ✓ **Manage Payees**

Users must enter their Username and Password credentials via a link on the Passcode and Touch ID sign in screen when prompted to access these features.
**Bill Pay for customers who have enrolled for this service*

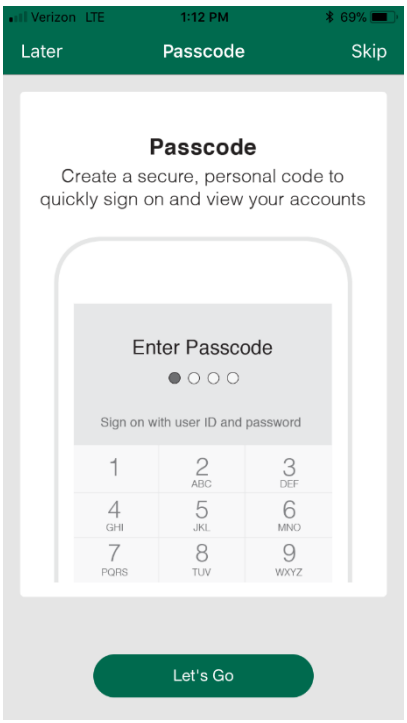
Touch ID

- Users can leverage the fingerprint scanner on iPhone 5S and newer devices (running iOS 8 or newer) to access Account Balances and Transactions
- The user must first have enabled the Touch ID feature within their iPhone settings. Unless there are registered fingerprints on the device, Mobile Banking Touch ID will not be able to function within their application.
- Touch ID will allow any fingerprint stored within the device to access mobile features regardless of whether or not it is the fingerprint of the account holder.
- Registered Touch ID fingerprints cannot be changed via the Mobile Banking application. The user would need to make any changes, such as adding or removing fingerprints from within the settings, on the device itself.



Member FDIC

Passcode



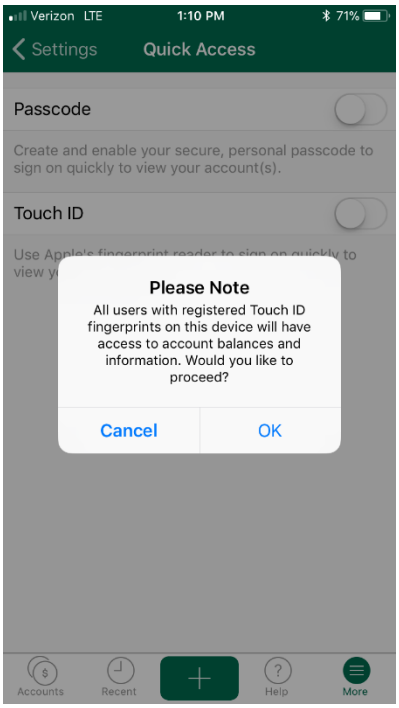
In order to maintain crucial security measures, users' passcodes must meet a set of requirements which are as follows:

- No repeating digits
- No ascending sequential digits
- No descending sequential digits
- Must match the chosen number of required digits
- Must be numeric characters

Restrictions – Only one quick access method can be selected at a time:

- *Even though users will have options to enable both Touch ID and Passcode within the settings of the Mobile Banking application, only one quick access method can be selected at a time.*
- *Enabling Touch ID will disable Passcode authentication and vice versa.*

The user will have up to three attempts to access their account information using either Passcode or Touch ID. After three attempts an error message appears for the user indicating that their unsuccessful attempts have disabled the feature on their application and prompts them to log in using their Username and Password. Once the user successfully authenticates with standard credentials they can re-enable Passcode or Touch ID.



Passcodes are managed per user token within the mobile database, meaning that a user with multiple mobile devices will conveniently have one passcode across all devices. Since Touch ID is specific to only the fingerprints that have been enabled through the operating system on the device, only the fingerprints stored on the individual device can use the feature. Users are not required to enable the passcode or Touch ID functionality and may leave Passcode and Touch ID disabled using standard authentication methods instead.