

The Business Mobile login experience varies depending if the user goes directly to the mobile app, or if the user already logged into Business Banking web:

If a new user goes directly to Business Mobile (Figures 1, 2, and 3):

1. Enter the system-generated username and password sent via 2 emails.
2. Confirm identity via MFA with “Call me” (only option).
3. Change the temporary password.

If a user logs into Business Banking web first (Figures 1 and 2):

1. Enter username and password (which were updated upon initial login to Business Banking web).
2. Confirm identity (email is not an option):
 - “Call me” - always an option.
 - “Text Me” - option if enabled in Business Banking web.

Figure 1

Figure 1 shows the Old National Mobile Banking login screen. The header is blue with the Old National logo and 'Mobile Banking' text. Below the header, there is a white box containing the FDIC logo and the text 'FDIC-Insured - Backed by the full faith and credit of the U.S. Government'. The login form has fields for 'User ID' and 'Password', both with 'Save' and 'Show/Hide' icons. A 'Forgot Login?' link is below the password field. A large blue 'Login' button is at the bottom of the form. Below the button is a 'Fingerprint Unlock' option. At the very bottom, there are links for 'Sign Up', 'Locations', and 'More'.

Figure 2

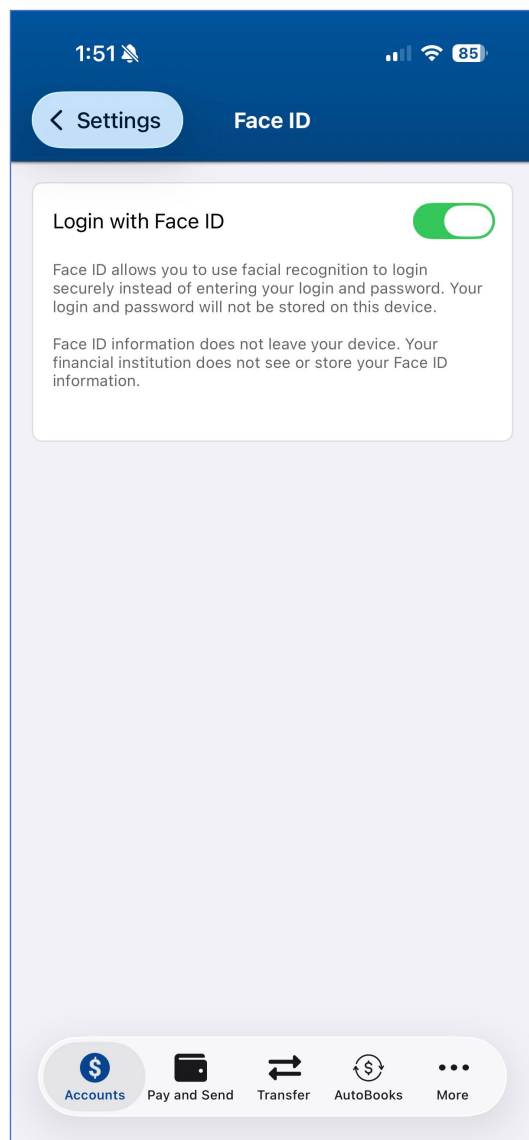
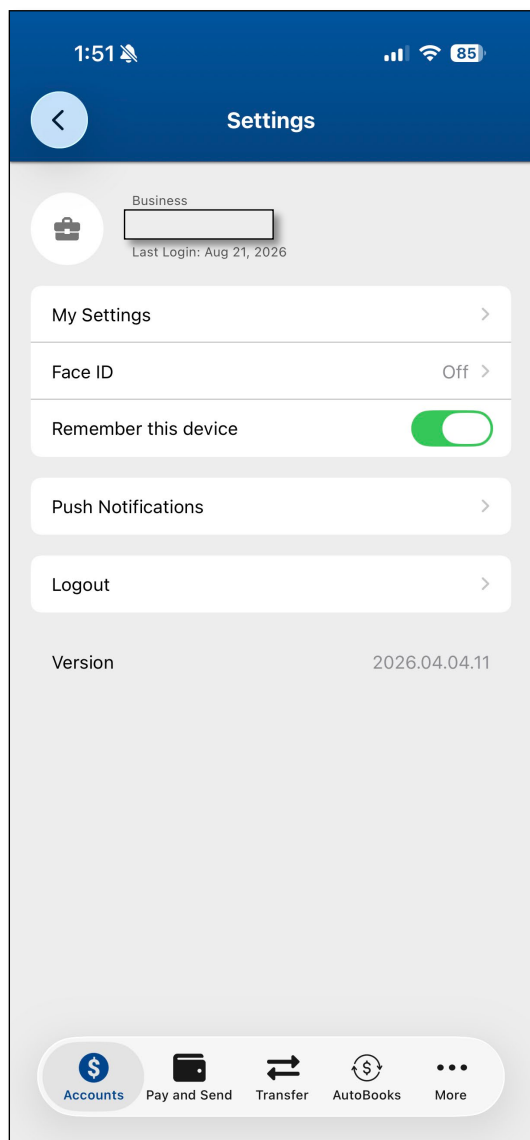
Figure 2 shows the 'Secure Login' screen. The header is blue with the text 'Secure Login'. The main content area is white and contains the following text: 'To access your account, we need to verify your identity. We will call you or send you a text message to your registered number. Respond to the call or text on your phone to verify your identity. Select the number where we can contact you.' Below this text is a phone number field with a placeholder '(xxx) xxx-5019' and two buttons: 'Text me' and 'Call me'. At the bottom, there is a link that says 'I can't access this number now'.

Figure 3

Figure 3 shows the 'Change Password' screen. The header is blue with the text 'Change Password'. The main content area is white and contains the following text: 'You must change your Password. Your new Password must meet these requirements:'. Below this text are four requirements, each with a green checkmark: 'Between 8 and 32 characters long', 'Minimum of 1 letter', 'Minimum of 1 number', and 'Minimum of 1 special character'. There are three password input fields: 'Current/Temporary Password', 'Password', and 'Retype Password'. Each field has a 'Show/Hide' icon. Below the fields, there is a green checkmark and the text 'Password must match.' At the bottom, there is a large blue 'Change' button.

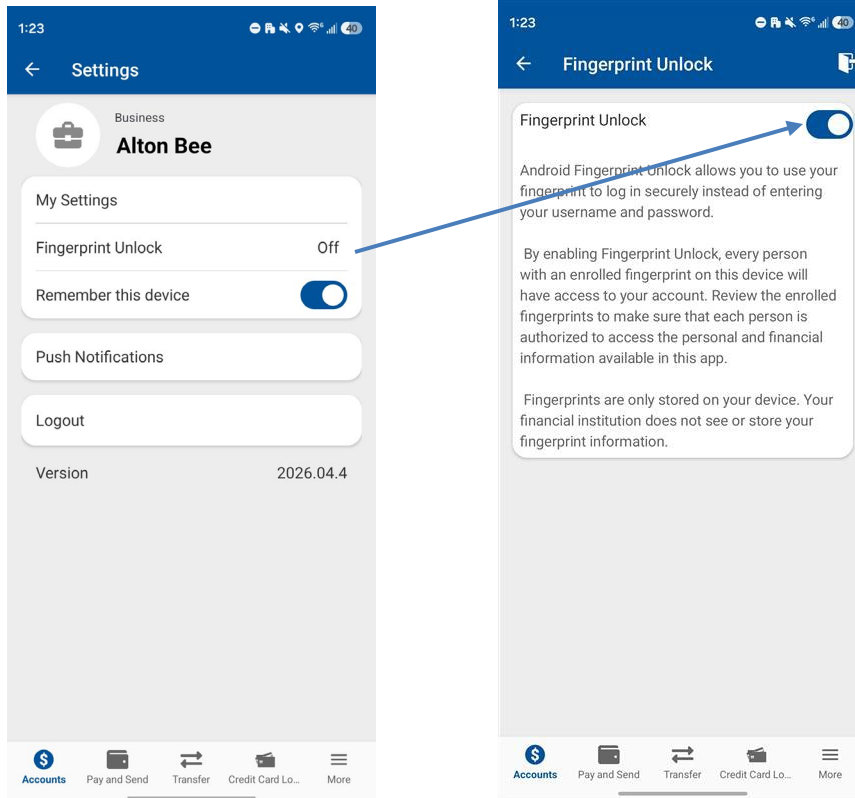
Enable Face ID for future logins:

1. Select Settings icon in the top right corner.
2. Toggle “Remember this device” to ON to bypass login MFA.
3. Toggle Face ID to ON to use Face ID instead of username/password.
4. On the login screen, slide left/right to switch between username/password (see Figure 1) and Face ID.



Enable fingerprint for future logins:

1. Select Settings icon in the top right corner.
2. Toggle “Remember this device” to ON to bypass login MFA.
3. Toggle Fingerprint Unlock (on iPhone, called Touch ID) to ON to use fingerprint instead of username/password.
4. On the login screen, slide left/right to switch between username/password (see Figure 1) and fingerprint.



Note: Biometrics are marked invalid after a user's password is reset (whether the user changes it, or the financial institution resets their password).

The user must log in with their username and the newly updated password. After login, the user can reestablish biometrics for future logins.