Frequently Asked Questions – Mobile Banking

How Do I Log Into Mobile Banking?

- In order to use any of Connex Mobile Banking service, you must register for Online Banking via a computer and browser. This is necessary to set-up all security settings and information that will be used to access both Online Banking & Mobile Banking during all future account logins. * For those members who do not have a computer our branches have kiosks available.

FAQs on Mobile Authentication

How is it really multifactor authentication if the passcode is sent to the same device?

- Multi-factor authentication gets its name because there are multiple methods of authentication, to further reduce the risk of fraudulent attacks, both remote hacking attempts and tablet theft. The second factor of authentication that we are adding to mobile further reduces the risk of remote fraudulent attacks, because the tablet is "something the user has" and the login has to be verified with the specific tablet that is tied to the user's account with the tablet in the user's hand at time of login. If a tablet is stolen and the thief attempts to log in, then the attack is no longer remote. At this point the thief still must initially get past the username and password. The "something the user knows" factor (username and password through the app) is one channel of communication & authentication, while the "something the user has" factor (passcode through SMS or Voice) is another channel of communication & authentication. Thus, multiple channels mitigate the risk of malicious remote and local attacks.
- Additionally, remember, a user can use a different phone number than their mobile phone number if they choose. Hence, they could enter their landline or office number to authenticate their mobile device to further reduce risk.

Will the customer experience change when mobile authentication is rolled out?

- When out-of-band (OOB) authentication is added to Mobile and Tablet Apps, the mobile authentication experience will change. On Mobile and Tablet Apps, the user will go through the OOB authentication process once on each mobile/tablet device, instead of being taken directly to the Home page as was the case with the single factor authentication. The user will be challenged on the mobile/tablet device with whatever phone number was used for USP. The security is connected and builds off of itself.

Will end users be able to change the phone number(s) that they registered to use for authentication?

- They will be able to change their registered phone number(s) within Online Banking, but there are currently no settings that allow this to be done within Mobile/Tablet

Apps. However, during first-time use of multi-factor authentication, users will be able to change the phone number(s) they use for authentication. This will allow a Mobile or Tablet Apps-only user to add a new number or change an old number that was set up in USP, so the user can log in from the registered phone.

If the user doesn't have any registered phone numbers, will the user be able to log in?

- Yes, the user can use the same approach as the authentication setup in Online Banking. On Step 1, the user will be prompted to enter a phone number if he or she is a Mobile or Tablet Apps-only user and hasn't registered a phone number for use with Online Banking. The user will use this phone number for future login attempts on other devices.

What happens if a user's mobile device is stolen or lost?

- Multi-factor authentication is built to protect against remote attacks, which are the majority of fraudulent attacks. If a cellphone/tablet is lost or stolen, the end user should do exactly what they do today: call the carrier to report it and cancel service to the phone/tablet or do a remote lock or data wipe via another device. There is more information (contacts, email, other apps, etc.) on an end user's phone/tablet that should be protected than one particular banking app. Keep in mind, that even if a phone/tablet is stolen or lost, the thief still needs to get past the username and password, hence multi-factor authentication. Similar to when a user loses their ATM card, then the fraudster must know their ATM PIN to move funds out.

Do you mask the phone numbers in this feature?

- Yes, the phone numbers are masked throughout all points of the authentication process.

Will end users have to authenticate each device that they use?

- Yes, end users will have to individually authenticate each device that uses the banking app. This allows us to provide additional security at each access point that is used to engage with the financial institution.

Will end users have to authenticate their devices every time they log in or only the first time?

- End users will only have to authenticate their devices the first time. Then, we will create a secure cookie that will be used to ensure that the same user on the same

device makes each future login attempt. If a user erases the cookie from a device from within the app, the user will have to authenticate the device again.

What if a financial institution has several members who are located in other countries and have non-U.S. phone numbers?

- These financial institutions will not be able to receive mobile authentication until international support is available later this year, as we currently only support U.S. phone numbers. However, if Mobile MFA is needed sooner, Google Voice is a viable alternative for international end users to still be able to access their accounts.

Will a user be able to be challenged by MFA every log in if they want to?

- Yes, even though this is not the default behavior of the app, if the user wants, they can go into the "More" section and turn the 'Remember device' toggle OFF to be challenged with MFA when they log in again.

FAQs about Text Message Banking

How secure is Text Message Banking?

- Our Text Message Banking service is secure. You can activate the service only after logging into our internet banking site. Text messages will never contain confidential information about you or your accounts. Messages will never contain full account numbers.

Will I be charged for Text Message Banking?

- We won't charge you, but standard carrier fees for text messaging may apply. Please check with your mobile phone carrier if you aren't sure what fees apply when you send and receive text messages.

Will Text Message Banking work on my phone?

- Yes it will, as long as you have text messaging enabled with your mobile carrier and use a carrier that the service supports. Please check with your mobile carrier if you are unsure.

Which carriers do you support?

- Our Text Message Banking service works on all major mobile providers in the U.S., including:
    - Alltel
    - AT&T
    - Nextel
    - Sprint
    - T-Mobile
    - US Cellular
    - Verizon Wireless

Frequently Asked Questions – Mobile Banking

- Virgin Mobile

How do I deactivate the Text Message Banking service?

- You can text back "stop" to 454545 on your activated cell phone, or you can return to the mobile banking page and click the deactivate link next to your mobile device number. Your phone will no longer receive any text messages from Mobile Banking. You can add a new phone at any time if you change your mind later.

Why do I need to verify my phone?

- Verifying your phone is a one-time step and is one way we ensure the security of mobile text messaging.

Where do I find my activation code?

- During setup we will send you a text message with your activation code. If you have already submitted your mobile number during setup, check your mobile device now. You should receive a text message with your activation code within a few minutes.

Can I come back later to enter my activation code?

- Yes you can. If you experience difficulties we recommend that you go through the setup process again and get a new code.

I still have not received my code, what do I do?

- It might take several minutes to receive your code. If you feel you have waited long enough you can click the "resend code" link. Please check your mobile device shortly for a new text message. If you are still experiencing problems be sure you entered in the correct mobile number during setup.

What is a primary text banking account?

- Your primary account is the default account that we will use when you text BAL to 454545. You should select the one you will likely want to check the most often. You can get all account balances by texting BAL ALL to 454545.

Can I get the balances of all my other accounts?

- Yes – when you text "BAL ALL" to 454545, we will reply with a message containing the balances of all your checking, savings and credit card accounts.

Can I change the primary text banking account later?

- Yes you can. Simply return here to the mobile banking page and select the edit link next to your primary bank information.

Are there any shortcuts for the keywords?

- Yes. The keywords are:
  - STOP =Deactivate service
  - HELP = Help on keywords
  - BAL = Primary account balance
  - BAL CHK = Checking account balances
  - BAL SAV = Saving account balances
  - BAL ALL = All account balances
  - LAST = Last 5 transactions

Are keywords case sensitive?

Frequently Asked Questions – Mobile Banking

- No, keywords are not case sensitive. You can type help or HELP.

What is the number I should send keywords to?

- The short code is 454545. This short code will only work if you have activated the Mobile Text Banking Service.

How long does it take to get a text message?

- You'll receive a text message response within a minute. Exact timing will depend on your mobile service carrier.

Is there any password needed for Mobile Text Banking?

- You don't need a password to access your account information via text message.

I have a new mobile phone number. Can I change or add my number online?

- Yes, you first need to deactivate your cell phone and add your new cell phone number. You can do this within alerts and mobile set up.

FAQs about Mobile Transactions (Apps & Tablets)

How many transactions can I see on my tablet/phone at a time?

- When you select an account name on the accounts tab/button, the last 30 days of transactions will be displayed. Scroll down to see all of your transactions. Select the View More Transactions button to view additional transactions going back 180 days

Why can't I access the Pay Bills Tab?

- The Pay Bills tab is only enabled for users who have signed up for Bill Payment within Online Banking on a personal computer and have set up one or more payees (people or companies you want to pay). When you are ready to make payments on your tablet or phone, select the Pay Bills tab/button to view scheduled payments and make a new payment.

Can I register for Bill Payment on my tablet/phone?

- Sorry, not at this time. Simply access Online Banking using a personal computer, click the Bill Pay button and enroll there. Once enrolled, all you need to do is set up one or more payees (people or companies you want to pay) to get started.

Can I see pending payments?

- Yes, just select the Pay Bills tab/button to see a list or pending payments

Can I remove a pending payment?

- Yes, you can remove a pending payment, but you cannot change it. To remove a pending payment, go to the Pay bills tab/button, select the payment you want to remove and the Cancel Payment button. Then confirm that you want to cancel the payment.

Can I see completed payments on my phone?

- Yes. From the payee list, you can see the last payment associated with each payee.

How do I log out?

- When you're ready to log out, select the Log Out button at the top right of the page. This will return you to the Login Screen.

I have disconnected my Tablet phone. Will my service continue to work?

Frequently Asked Questions – Mobile Banking

- For the Tablet app to work, you must have a device with access to the 3G/Edge (or greater) or WIFI network.

Is help available through my device (Tablet or phone)?

- Click the Contact Us or More Tab, depending on your tablet or phone, to find the Connex support number and email address. For help regarding your Tablet or phone and or wireless internet connectivity, please contact your wireless provider.

What does the "Remember Me" checkbox do?

- Selecting the "Remember Me" checkbox gives the application permission to save your Username so that you do not have to enter it each time you attempt to log in. This information is masked and stored securely to keep your information safe.