FCCB Mobile Banking FAQs
4/26/17

1) Is Mobile Banking secure?

   We are committed to protecting your personal information. All data is encrypted as it travels to and from your mobile device. Your ID and password are required every time you login. Our mobile banking solutions never save your account numbers, transaction information, or balances on your device. Your password will only be saved if you activate Touch ID, Fingerprint, or similar biometric authentication within the Mobile Banking app, and in such case, will be saved in accordance with Apple or Android security standards. Mobile Banking is merely an extension of NetTeller, and NetTeller's security measures remain intact.

   Please review our recommendations below (#11) on how you can help keep your mobile device and mobile banking session secure.

2) What are the prerequisites to use the FCCB Mobile Banking app?
   - You must be a current NetTeller user, and must have previously logged into NetTeller to establish your watermark and personal security questions. If you are not enrolled in NetTeller, please visit your nearest community office. The NetTeller application is also available at www.firstcitizensbank.com
   - You must have a supported mobile device with a data plan or Wi-Fi capabilities. A supported mobile device generally means an Apple or Android device with a recent operating system.
   - You must download the FCCB Mobile Banking app from the iTunes App Store or Google Play.

3) Will I get a separate userid and password for FCCB Mobile Banking?

   Mobile Banking is an extension of NetTeller and uses the same userid and password as NetTeller.

4) How do I get the FCCB Mobile Banking app, and is it free?

   The app is free and can be downloaded from the iTunes App Store or Google Play. Please refer to your mobile service provider for any applicable data or web access fees.

5) What functions are available in the FCCB Mobile Banking app?
   - View account balances, transactions, check images, and statements
   - Transfer funds
   - Bill Payment:
     - Add/delete payees and payments
     - Edit one-time payments
     - View payment history
   - Change your NetTeller password
   - View login alerts
   - Find our nearest Branch or ATM
   - Link to the FCCB website
   - Deposit checks (enrollment and approval required; transaction fees may apply)

6) What functions are available in NetTeller, but are ***not*** available in Mobile Banking?
    - Establish watermark and security questions
    - Bill Payment:
        - Enroll in bill pay
        - Edit payees
        - Full editing of payments
    - Various user options, such as:
        - Establish password reset information
        - Edit alerts
        - Edit display options (e.g., amount of transaction history and bill pay history to display)
        - Set user and account pseudo names
    - Cash Management
    - Printing

7) Can I control the amount of transaction and bill pay history displayed in Mobile Banking?

    These settings are controlled under the Options / Display tab in NetTeller, and affect both NetTeller and Mobile Banking.

8) Why are the distances on the Location screens different from the distances on the maps?

    By default, mobile operating systems show the Location distances "as the crow flies" whereas the maps generally show driving distances.

9) Can I deposit checks via my mobile device?

    Mobile Deposit is now available! To activate this service, you must complete the Mobile Deposit enrollment process within the Mobile Banking app; meet the specified eligibility requirements; and agree to the terms, conditions, and associated fee schedule.

10) What can I do to protect my mobile device and mobile banking sessions?

    We recommend the following precautions to protect your mobile device and your mobile banking sessions:
    - Avoid disclosure of your login information and mobile banking sessions:
        - Password-protect your mobile device, and set your device to automatically lock after a brief period of inactivity.
        - Logoff and close your Mobile Banking session after every use.
        - Don't provide your username, password or other access information to any unauthorized person.
        - Don't store your password on or with your mobile device, other than as required for optional biometric/fingerprint authentication.
        - Don't leave your device unattended while logged into Mobile Banking.
        - Remember that we will never contact you (e.g., by calling, texting, or e-mailing) to ask for your personal or account information.

- Avoid malware infections and being spied upon:
  - Only use trusted networks. Ensure that any Wi-Fi network you use is properly secured / encrypted.
  - Don't circumvent your operating system's internal controls by "jailbreaking" or "rooting" your mobile device.
  - Only download apps from a trusted source and known provider. Make sure you understand the app's permission requirements and privacy policy.
  - Don't respond to unsolicited text messages, emails, or voice messages, and don't follow links contained within the messages.
  - Exercise caution when visiting websites you are not familiar with.
  - If possible, run security software on your mobile device.
- Keep your operating system (e.g., iOS, Android), Mobile Banking App, and all other Apps up to date.