GFAMobile Security

GFAMobile includes the following security standards:

- A unique user ID and Password that you have chosen
- A security image and phrase known only to you
- Security Questions that you have chosen and answered
- We only display your first name upon login
- The last time you logged in is presented to you at each new session
- Only the last four digits of your account number are displayed
- No account information is stored on your mobile device

How do I securely leave my Mobile Banking browser session?

- Select the *log out* link to sign out of Mobile Banking, and then close your browser through your mobile device browsing options. If you are using a downloadable app, click on *log out* to stop your Mobile Banking session.

Can someone intercept my Mobile Banking transactions?

- The 128-bit SSL encryption protects your information as it travels from your mobile device to GFA. The 128-bit SSL encryption technology is the same encryption that safeguards Internet traffic for secure web applications.

Is it secure?

- Yes, the Mobile Banking service utilizes best practices from Online Banking, such as HTTPS, 128-bit SSL encryption, registration authentication questions, access with a User ID and Password, security authentication questions, and application time-out when your mobile device is not in use.

What are some tips to keep my Mobile Banking experience safe?

Here are some tips and general good practices for banking on your mobile device:

- Always create strong passwords using alpha/numeric characters, upper and lower case and symbols
- Avoid using any automatic login or remember my login information features
- Change your password periodically or anytime you have a concern that someone may know it
- Download and apply security updates and patches to your mobile browser when they are made available by your wireless provider. These are designed to provide you with protection from known possible security problems
- To prevent viruses or other unwanted problems, do not open attachments from unknown or untrustworthy sources
- Do not install pirated software or software from unknown sources
- Limit unauthorized access to your mobile device by protecting access to it with a passcode.

- Do not leave your mobile device unattended during an open Mobile Banking session
- Never save your User ID and Password in the mobile device, in memos, or anywhere on your device
- Always remember to log off properly using the *log off* button when you have completed your Mobile Banking activities
- Never share your user ID and password
- Be aware of the potential for fraudulent Mobile Banking apps
- Review your account activity regularly and notify GFA of any unusual activity.

Is Mobile Banking as secure as other GFA online services?

Mobile Banking offers the same security features and protection as our other online services, including encryption and security questions. Mobile Banking users are protected by:

- Firewall systems and intrusion detection software
- Encryption of sensitive information that protects information sent over the Internet
- Internationally recognized security standards and industry best practices
- Profile and Password security