Fraud Preventions

Mobile Apps

- Only download mobile apps from a reputable source to ensure safety for you personal information.
- Sign off when you are finished using RCU's mobile app rather than just closing it.
- Don't set an app, web or client-text service to automatically log you into your account. If your phone is lost or stolen, someone will have free access to your money/information.

Online Security

- If it sounds to good to be true, it probably is.
- When banking and shopping online, check that the site is securely enabled. Look for web addresses with https:// meaning the website takes extras measures to help secure your information.

Passwords

- Update your passwords every 90 days. Use alpha, numbers and symbols for a strong password.
- Don't use the same password for multiple sites. This can help minimize the chance of a hacker gaining access to other accounts.

Personal Information

- Don't give personal information over the phone, mail, or on the internet unless you know the person and you've initiated the contact.
- Never give out your Social Security Number, driver license number, or date of birth. If you must share personal information, confirm that you are dealing with a legitimate organization
- If you receive an email asking for personal information, do not hit the reply button or click on any links in the email. Instead, go directly to the sender's website by typing in its web address

Personal and Public Computers

- Be cautious when using public hotspots and check your wi-fi auto connect settings. If you have a wireless network at home, be sure it is encrypted and password- protected.
- Don't walk away from your computer if you are in the middle of an online banking session, always make sure to log off when completed with your session.
- Install, run and keep anti-virus and all other software updated.

Smartphones & Tablets

- Use the keypad lock or phone lock function on your mobile device when it is not in use.
- If you lose your mobile device, or change your phone number, remove the old number from your mobile banking profile.
- Immediately tell your mobile service provider and your bank if you lose your phone.
- Never provide personal identification, or banking information over your mobile device unless you initiate the contact and you know that you're dealing directly with your financial.
- Never share your password, account number, PIN and security questions answers. Don't save this information anywhere on your phone.