Pickens Savings and Loan Association

Mobile Banking Security Best Practices

According to recent studies, security is the number one fear among potential mobile banking customers. The good news is that technology advancements and established risk protection truly do make mobile banking secure and safe. In addition, mobile banking is a great tool you can use to detect fraudulent activity because it provides an easy way to check your account on a regular basis for suspicious activity. The security measures currently in place include:

- **Username and password** – used to confirm your identity and ensure the confidentiality of your mobile banking session, plus session will be locked out after three incorrect login attempts.
- **New device** – enhanced layers of security used in the event you log in from a new device wherein identity verified through a one-time security code via a phone call or SMS (text) message or answering a series of questions obtained from public records.
- **Device profiling** – mobile banking not used in last 90 days may require stepped up authentication to enhance security.
- **Encryption** – system uses the industry's strongest 128-bit SSL encryption standards to protect the transmission of data.
- **Firewalls and routers** – used to protect programs from any unauthorized malicious intrusion.
- **Time-out** – function is enabled when mobile device is not being utilized or you forget to log out.
- **Account data** – no confidential customer or account data such as account numbers (that are masked) is ever stored on your mobile device, and sensitive information is not sent via text messages.
- **Lost or stolen phone**– service can be immediately disabled by either going to the Mobile Banking Center in online banking and disabling or removing your device, contacting our bank, or calling your mobile service provider to stop the service.
- **Transfer of money** – can only transfer funds between Pickens Savings and Loan accounts and pay existing bill payees within mobile banking (new payees are set up only within online banking bill pay).
- **Unauthorized transactions** – in the rare event of an unauthorized transaction, certain protections are in place for consumers as long as reported to the bank within 60 days of receiving your statement showing unauthorized activity.

The likelihood of fraud is no greater than using your online banking, but keeping in mind that you should use the same best practices that you follow when browsing the Internet or accessing email from your PC. There are many security tips and precautions that you can exercise to practice safe mobile banking:

- **Password** – PIN or password protect your phone or tablet and lock it when not in use; don't reveal password information to anyone or keep it stored on the device; and don't let your device automatically log you in or save any of your login information.

- **Texting or email – do not text message or email any confidential information about your account to the bank or elsewhere since text messages and email are not transmitted on a secure channel.**
- **Identity protection –** never respond to a "phishing" text or email that requests your PIN, account number, or any card, and please remember that Pickens Savings and Loan *will never request this information in this manner*.
- **Anti-virus software –** if available, install mobile anti-virus and anti-spyware software on your device and keep it updated.
- **Opening files –** be cautious of opening unsolicited files, text messages, or applications, especially if they are received from unknown sources.
- **Application downloads –** only download and install a bank application from reliable sources such as Apple iTunes store or Google Android market; and report any banking application that appears to be malicious to Pickens Savings and Loan right away.
- **Connection –** only connect to the bank via a secure connection or a non-public Wi-Fi network and remember to log out of mobile banking when you are finished with your session.
- **Bluetooth –** disable Bluetooth, or set the Bluetooth status to hidden, until you want to share something.
- **Monitor –** monitor your accounts on a regular basis to more readily detect unauthorized activity.
- **Lost or stolen device –** immediately disable within the Mobile Banking Center in online banking, contact the bank, or call your mobile service provider to disconnect the service.
- **Phone lock –** lock your device to your SIM card and enable a PIN to prevent access to the device in the event that it is lost or stolen.