Mobile Banking and Texting Best Practices

- Configure your mobile device to require a PIN for access and set screen locks when not in use. Always protect your online banking credentials and do not save them on your mobile device. We encourage you to use a remote wipe application. Contact your provider for available options.

- To ensure that your Device is protected from and free of viruses, worms, Trojan horses, etc., install an anti-virus program on your mobile device.

- County First Bank will never request sensitive personal or financial information via a Text Banking message. If you ever receive such a request for sensitive personal or financial information - such as your Social Security Number, account number, password, PIN number, or any other personal data - do not respond to the message and call us at (301) 934-2265 to report the incident.

- County First Bank uses an SMS short code (39257) for its Text Banking messages. Only trust text messages from 39257 as being from County First Bank.

- You should only download apps from trusted and approved app stores endorsed by your service carrier.

- Jailbreaking is a method of 'self-hacking' your cell phone in order to gain full access to all features of the technologies of smartphones. You should avoid Jailbreaking because it makes the smartphone extremely susceptible to malware, viruses and other malicious programs.

- Information from a wireless device may be stolen through a Bluetooth connection. Bluetooth is a short range high speed wireless technology used for sharing information between devices. Devices with Bluetooth enabled by default and "always on" may present a target for exploitation and interception of data which can be done undetected. Accordingly, you should keep Bluetooth connections turned off by default and use them only when necessary.