Mobile Banking Security Awareness

First FarmBank's Mobile Banking allows you to bank anytime, anywhere from the convenience of your mobile phone. This service provides secure access to your bank accounts, allowing you to view account balances and recent activity. You will also be able to search account activity, transfer funds, and find our locations. First FarmBank uses multiple forms of identification authentication, log-in procedures and encrypted communications to make sure your mobile banking application is safe and secure.

The continuing growth of mobile phones and mobile banking is providing conveniences for you and offers more ways to access accounts. Of course, fraudsters (*those individuals trying to steal personal information*) are going to follow the same path and turn their attention to mobile banking with malware and social engineering in search of potential targets. Fraudsters know that one of the possible keys to their success lies within an account holder. Security awareness education is a key to minimizing these risks to First FarmBank customers from fraudsters.

Tips for safe and secure Mobile Banking:

• Research any application (app) before downloading it. Just because the name of an app resembles the name of the bank, don't assume it is the official FIRST FARMBANK app. It could be a fraudulent app designed to trick users into believing the service is legitimate. The best place to download the First FarmBank mobile banking app is from the First FarmBank website or from the app store. First FarmBank will have a link on the website that will take you directly to the app store. Be aware that fraudsters will continue to create fraudulent applications. If you have any doubts about any websites or mobile banking applications contact First FarmBank.

• First FarmBank will never ask for your password under any circumstances. Do not tell your password to others under any circumstances (including mobile phone support operators or mobile phone sales representatives, etc.). Fraudsters will try to obtain mobile banking passwords by e-mail, letter, phone calls, asking for your mobile banking account number, username, password, and other important information. If you have any doubts, please contact First FarmBank.

• Please use strong passwords that are not easily guessable. They should be composed of numbers, letters (upper case and lower case) and special characters.

• It is good practice to change your mobile banking password regularly.

• Do not lend others your phone with the mobile banking function opened as this will prevent infringement and deter others from spying on your personal information.

• Be careful about where and how you conduct transactions. Don't use your device in an unsecured Wi-Fi network or in a public place, such as in a coffee shop because fraud artists might be able to access the information you are transmitting or viewing. Also, don't send account numbers or other sensitive information through regular e-mails or text messages because those are not necessarily secure.

• Password protect your mobile device and lock your device when it's not in use. Keep your mobile device in a safe location.

• Delete text messages from your financial institution on your mobile device, especially if they contain sensitive information.

• If you change your mobile number, immediately contact First FarmBank to change the details of your mobile banking profile. You should also take additional precautions in case your device is lost or stolen. Check with your wireless provider in advance to find out about features that enable you to remotely erase content or turn off access to your device or account if lost or stolen.

• Do not modify (jailbreak) your mobile phone. It will make your mobile phone susceptible to an infection from a virus, Trojan, or malware.

• When possible, install mobile security software on your mobile phone, similar to Anti-virus software you have on your laptop or desktop computers.

• Be alert to changes in your mobile phone performance. If you download any new applications and your mobile phone starts performing differently (for example-responding slowly to commands or draining its battery faster), that could be a sign that malicious code is present on your mobile phone.

• Monitor your financial records and accounts on a regular basis. Use the electronic account alerts to send to your email or mobile device on account activity. Regularly review your statements with online banking. This will enable you to spot any suspicious activity.

• A benefit to using mobile banking is that it can actually help deter some fraud because it gives a customer an easy way to check their accounts on a regular basis and notify First FarmBank quickly if they see suspicious activity.

If at any time you do notice suspicious activity on your accounts, please notify a First FarmBank representative immediately at our main location 970.346.7900.