Electronic Banking Security Information for Our Customer

First National Bank of Stanton is committed to maintaining the privacy and security of your personal and private information when submitted via www.fnbstanton.com.

First National Bank of Stanton uses firewalls that act as a shield between the internet and the banks internal systems. These barriers help to ensure that all internal information is secure.

In Online Banking, our system encrypts all of your information making it unreadable, especially during transmission. For your security and ours, First National Bank of Stanton uses industry-standard encryption.

Important notice regarding use of cookies: By continuing to use this site, you agree to our use of cookies as described in our Digital Privacy Policy.

When you login to Online Banking your unique ID and password are encrypted using Secure Sockets Layer (SSL) technology. This necessary precaution is intended to deter anyone other than yourself from accessing your personal information.

While we work very hard to protect and secure your accounts, you also have a very important role to play in preventing unauthorized activity on your account too.

To help protect any information that you enter into your computer, we highly recommend that you:

1. Install security software on your personal computer (PC), including anti-virus software and spyware detection software.
2. Always log out when finished using your Online Banking Session.
3. Do not write down or share your login credentials or any other personal information.
4. Never respond to a “supposed” email from First National Bank of Stanton that requests that you send non-public personal information. First National Bank of Stanton will never contact you through email. We will never ask you to send us your personal or account related information via e-mail. If you receive such a suspicious email, please report it to www.consumer.ftc.gov immediately.
5. Never provide personal information in response to unsolicited text messages, emails or telephone calls even if they appear to be from a legitimate business. You should never click on links provided in unsolicited e-mails or text messages. First National Bank of Stanton does not send unsolicited electronic messages asking you for your personal information.
6. If you wish to contact First National Bank of Stanton by email or through our “contact us” page at www.fnbstanton.com, never include any personal information such as account number, passwords, Social Security Number, birth date or any other personal identifiable information.

Tips to Report Suspicious Activity
If you have any questions about the validity of communication that claims to be from First National Bank of Stanton or another financial institution, you should contact the institution immediately by telephone or in person. Our customer service number is 432.756.3361.

If a scammer does take advantage of you online, report it to the Federal Trade Commission at www.ftc.gov. The FTC enters Internet, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

If you receive deceptive email, such as a message for your information, forward it to the entity that is being wrongfully impersonated, and forward to www.ftc.gov. Be sure to include the full header of the email, including all routing information.

The Anti-Phishing Working Group, a consortium of Internet Service Providers, security vendors, financial institutions and law enforcement agencies, use these reports to fight phishing.

Be Cautious with Text Messages

If you receive a text message that claims your bank debit card has been or will be deactivated for security reasons, this message is fraudulent and an attempt to steal your identity. These text messages may claim that you must call an 800-number and provide personal information to reactivate your cards.

- Assume unsolicited text messages are fraudulent.

- Become familiar with the customer communications policies of businesses you use.

- Upon receipt of an unsolicited text message, call the actual business at a telephone number that appears on a statement, a credit card, or the telephone directory.