

Internet Privacy Policy

This Internet Privacy Policy explains how we may collect information from you when you visit our web site or when you use our online financial services.

We recognize the importance our customers place on the privacy and security of their personal information. Our goal is to protect your personal information in every way that we interact with you, whether it's on the telephone, in our lobby, at one of our ATMs, or on the Internet.

We think it is important for you to be informed of the policies, procedures, and security measures that we have in place to safeguard your personal and confidential information. With that in mind, we have developed this Internet Privacy Policy to help you to understand the steps we take to protect your personal information when you utilize our online financial services.

Below are several definitions of terms used within this policy:

Customer Information - Customer Information refers to personally identifiable information about a consumer, customer or former customer of this Institution.

Internet Protocol (IP) Address - an IP address is a unique address that devices use in order to identify and communicate with each other on a computer network. An IP address can be thought of as a street address or a phone number for a computer or other network device on the Internet. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. We may use IP addresses to monitor login activity and for identification purposes when necessary for security investigations.

Cookie - a Cookie is a very small text file sent by a web server and stored on your hard drive, your computer's memory, or in your browser so that it can be read back later. Cookies are a basic way for a server to identify the computer you happen to be using at the time. Cookies are used for many things from personalizing start up pages to facilitating online purchases. Cookies help sites recognize return visitors and they perform a very important function in secure Internet banking.

"Session" Cookies are used to monitor session activity within our Internet banking product. These Cookies are encrypted and only our Service Provider can read the information in these Cookies. The session Cookie facilitates the processing of multiple transactions during a session without requiring you to reenter your passcode for each individual transaction. Session Cookies used within our Internet banking product do not pass to your computer's hard drive. Instead, the Cookie is stored in your computer's memory, identifying only your computer while you are logged on. When you log off, or close your browser, the Cookie is destroyed. A new Cookie is used for each session; that way, no one can use the prior Cookie to access your account. For additional security, the Cookie expires after 10 minutes of inactivity. It must then be renewed by reentering your passcode. We do not use this Cookie to collect or obtain personal information about you.

An encrypted non-expiring Cookie is also used within our Internet banking product for the identification of this Institution.

Service Provider - In order to provide a full range of online financial services, we may use various third party providers. These third parties provide services such as: website hosting, Internet banking, bill payment, and account aggregation. Third party providers are referred to within this policy as “Service Providers”.

Information Collected on the Internet

If you are just browsing through our website, we do not request any personally identifiable Customer Information, nor do we collect unique identifying information about you unless you voluntarily and knowingly provide us that information, such as when you send us an email or complete an application online. If you provide us this information, it is only used internally and in furtherance of the purpose for which it was provided.

As part of providing online financial products or services, we may obtain information about our customers and website visitors from the following sources:

- Information we receive from you on applications, emails, or other forms;
- Information about your transactions with this Institution and our affiliates;
- Information we receive from a consumer-reporting agency; and
- Information that is generated electronically when you visit our website or use our online financial services.

Service Providers hosting our website and Internet banking service may collect general information on our website visitors for security and statistical purposes. Such information may include:

- The Internet address (referral site) which brought you to our web site;
- The date and time you access our site;
- The name and version of your web browser;
- Your Internet Protocol (IP) address;
- The pages visited in our website; and
- The duration of your online session.

Our Service Providers may use Cookies to collect some the above information. In some cases you must accept cookies in order to view our website.

When you click on advertisements in our website or advertisements on linked 3rd party web sites, you may receive another Cookie; however, you do not have to accept any Cookies from third party advertisements.

As mentioned previously, our Service Provider(s) may also use Cookies within our Internet banking and bill payment products. You must accept these Cookies in order to utilize the service. These Cookies do not store any personally identifiable information; they simply provide another level of security.

Use of Information Collected

- We may disclose the information that we collect, as described above, with Service Providers acting on our behalf to provide online financial services such as: Internet banking and bill payment.

- We may also disclose Customer Information when required or permitted by law. For example, Customer Information may be disclosed in connection with a subpoena or similar legal process, fraud prevention, or security investigation.
- We may also share Customer Information outside this Institution when we have your consent, such as when you request a specific product like insurance or an investment product from a third party financial services provider.
- We may also disclose aggregate (not personally identifiable) Customer Information with Service Providers or financial institutions that perform marketing and research services on our behalf and with whom we have joint marketing agreements. Our contracts require all such Service Providers/or financial institutions to protect the confidentiality of your Customer Information to the same extent that we must do.
- We do not disclose any Customer Information about our customers, former customers, website visitors to anyone, except as permitted or required by law.
- We do not sell any of your personal information.

Account Aggregation

Account aggregation sites allow you to consolidate account information from several sources into one online location. In order to provide this service, an aggregation provider may request your passcode and login information. You should ensure that the aggregation provider has appropriate policies to protect the privacy and security of any information that you provide.

If you provide information about your First National Bank accounts to an aggregation provider, we will consider all transactions initiated by an aggregator using the access or login credentials that you provide, to be authorized whether or not you were aware of a specific transaction.

If you decide to revoke the authority given to an aggregation provider, we strongly recommend that you also change your online passcode with this Institution. This will help ensure that the aggregation company cannot continue to access your account(s) with us.

Email Policies

When you enroll for our online services, we will send you a welcome email. We may also send emails marketing various products and services offered by this Institution. We will always provide you an opportunity to opt-in or opt-out of marketing related emails.

We will also send security related email notices when you sign-up for email (“notify me”) alerts on your account(s) or whenever you change your passcode, security question, or email address.

If you agree to accept electronic disclosures and/or online account statements, we may also send you notices of important account updates through email. For example, if you have agreed to accept disclosures electronically, we may send you an email with updates to this privacy policy and/or we may send you a notice that your account statement

is available for viewing on our website. For more information on how to enroll for electronic disclosures, please contact us at 580-326-9641.

Beware of Phishing Attempts and Internet Scams

While email is convenient and has a good business use, it can also be misused by criminals for scams and various other fraudulent purposes. “Phishing emails” are frequently used by criminals to entice the recipient to visit a fraudulent website where they try to convince the recipient to provide personal information, such as ATM card numbers, account numbers, Social Security numbers, access Ids and passcodes. Some of these fraudulent websites may also be virus laden and can be used to download mal-ware to your computer. Fraudulent websites often look identical to a legitimate site, so it’s important to look very closely at the website address.

Below we have listed a few tips to help protect your personal information on the Internet:

- Always be wary of links in emails, especially any links in emails purporting to be from this Institution.
- Please remember that if we send you an email, we will never ask for personal information such as your account number, ATM card number, PIN number, or social security number.
- Bookmark financial websites and use these bookmarks every time you visit the website.
- Whenever you enter personal information like your access ID or passcode, always look for the lock symbol, or https: in the address bar. Always click on the lock symbol and review the certificate details.
- Update your Internet browser! Most browsers now offer free anti-phishing tool bars that can help alert you of fraudulent websites.
- If you send us an email, please do not include any confidential, personal or sensitive information in the email message, as email messages are generally not secure. We do offer secure messaging through our Internet Banking product and you may use this secure messaging feature if you need to send us sensitive or confidential information.
- Make sure that your computer always has up-to-date versions of both anti-spyware and anti-virus software.
- If you receive an e-mail that you think could be a scam, delete it immediately or forward the email to spam@uce.gov.
- If you have any questions about the legitimacy of an email, especially an email from this Institution, you can also call us at this number 580-326-9641 or forward the email to webmaster@sfnb.net.

External 3rd Party Links

Our website may include links to other 3rd party web sites. These links to external 3rd parties are offered as a courtesy and a convenience to our customers. When you visit these sites, you will leave our website and will be redirected to another site.

This Institution does not control linked 3rd party web sites. We are not an agent for these third parties nor do we endorse or guarantee their products. We make no representation or warranty regarding the accuracy of the information contained in linked sites. We suggest that you always verify the information obtained from linked websites before acting upon this information. Also, please be aware that the security and privacy policies on these sites may be different from our policies, so please read third party privacy and security policies closely.

If you have questions or concerns about the privacy policies and practices of linked 3rd parties, please review their websites and contact them directly. This privacy policy applies solely to the Customer Information collected by this Institution.

Security

This Institution and our Service Providers have developed strict policies and procedures to safeguard your Customer Information. Our policies require confidential treatment of your personal information. We restrict employee access to your personal information on a "need to know" basis and we take appropriate disciplinary measures to enforce employee privacy and confidentiality responsibilities. We have established training programs to educate our employees about the importance of customer privacy and to help ensure compliance with our policy requirements.

Furthermore, this Institution and our Service Providers maintain strong physical, electronic and procedural controls to protect against unauthorized access to customer information. Our computer systems are protected in the following ways:

- Computer anti-virus protection detects and prevents viruses from entering our website, email, and computer network systems.
- Firewalls and intrusion prevention systems block unauthorized access by individuals or networks.
- We use encryption technology, such as Secure Socket Layer (SSL), to protect the transmission of your confidential information. Whenever you login to our Internet banking product or schedule an online transaction through our system, the communication is encrypted. Encryption scrambles transferred data so it cannot be read by unauthorized parties.
- We use strong multi-level authentication and behavior analysis to help prevent unauthorized access to your accounts. Multi-level authentication can help prevent access by someone who may have stolen your login credentials.
- We provide secure email through our Internet Banking product to help ensure that your communications with us are confidential.

We continually monitor technological advances and upgrade our systems to ensure your information remains secure.

Privacy of Children

COPPA, the Children's Online Privacy Protection Act, protects children under the age of 13 from the collection of personal information on the Internet. This financial institution respects the privacy of children. We do not knowingly

collect names, emails addresses, or any other personally identifiable information from children. We do not knowingly market to children, nor do we allow children under 13 to open online accounts.

Privacy Updates

This policy maybe updated from time-to-time as new products and features may require changes to our Internet Privacy Policy. The effective date of our policy will always be clearly displayed. If we make any changes regarding the use or disclosure of your personal information, we will provide you prior notice and the opportunity to opt-out of such disclosure if required by law.

Questions

If you have any questions about our privacy policy or concerns about our privacy practices, please contact us at (918) 653-3200.

Effective Date: June 1, 2021