PRIVACY POLICY FOR ONLINE BANKING

PROTECTING YOUR FIRST RESOURCE BANK ONLINE TRANSACTIONS

To ensure that your online banking payment transactions remain confidential and secure, First Resource Bank Digital Banking employs state-of-the-art technology. First Resource Bank Digital Banking includes several levels of security measures to prevent unauthorized users from accessing your information or gaining access to our network. Security measures include firewalls, screening/filtering routers, encryption, password protection and other methods.

Firewalls and Screening/Filtering Routers – Firewalls and screening/filtering routers are "gateways" that verify the source, destination and protocol of each data packet and determine whether or not to send the packet through. This ensures that you will only receive information pertaining to First Resource Digital Banking.

Encryption – Once you enter First Resource Bank Digital Banking we use encryption to protect your data from being altered or monitored en route to your computer. Second Socket Layer (SSL) encryption provides a secure channel for data transmission across computer networks using public key cryptography. Public key cryptography is a technique that uses a pair of keys, one is public and one is confidential, for encryption and decryption. Certain pages in our web site are protected by public key cryptography. To see if the page you are on is protected, check the "URL" or web address at the top of the screen. If the address begins with "https" then you are using a secure screen.

Security authentication tokens are recreated on every login. Each token will be tied to the TLS session ID of the connection. Since each application must negotiate its own session when it initiates a connection, the authentication token cannot be shared even among different applications or browsers on the same device. In the unlikely case that the authentication token is compromised, this measure severely limits its usefulness. In addition, authentication tokens are not available to browser scripts and can only be obtained by intercepting the HTTP connection stream.

User Authentication – First Resource Bank Digital Banking uses MFA (multi-factor authentication) to restrict entrance to the system. As a First Resource Digital Banking user, you must verify your identity via a username/password prompt - along with an OTP (one-time passcode) to enable use of the system. For your own security and privacy, it is recommended that you memorize your username, password and destroy all written references to your password or OTP codes. You are responsible for keeping your

password and OTP codes confidential. Do not give your OTP codes to anyone. First Resource Bank employees will never ask you for your password or OTP codes.
Our digital banking solution keeps tabs on the devices and browsers that you use while signing into your accounts by using device IDs and browser fingerprinting. Whenever end users attempt to sign in on a device that the service doesn't recognize, you will be asked to prove your identity using 2FA (Two Factor Authentication) in case your credentials have been compromised.

Session Timeouts - Digital Banking users are logged out after 10 minutes of inactivity. After 9 minutes of inactivity, we display an alert with a 60 second countdown prompting the user to click anywhere in the window to acknowledge that they're still actively browsing. If they fail to do so and the session times out, we sign the user out, destroy their local data, and take them back to the sign in view. Active users will be forced to log out after 24 hours.

INFORMATION WE OBTAIN FROM VISITORS BROWSING AND VIA COOKIES

For a more effective web site, we use "cookies" as part of our interaction with your browser. A "cookie" is a commonly used small text file placed on your hard drive by our Web page server. By configuring your preferences or options in your browser, you determine if and how a cookie will be accepted. We use cookies to determine if you have previously visited our web site and for a number of administrative purposes. These cookies do not collect personally identifiable information, and we do not combine information collected through cookies with other personal information to determine who you are or your email address.

If the use of cookies is a concern to you, then please set your browser to alert you accordingly. Newer browser versions allow you to be alerted or to automatically refuse cookies. You may need to download a more current version of your web browser from your service provider in order to obtain this option.

CHILDREN VISITING OUR WEB SITE

We do not market to or knowingly solicit data from children. We recognize that protecting children's' identities and privacy online is important and that the responsibility to do so rests with both the online industry and with parents.

EXTERNAL LINKS

First Resource Bank is not responsible for the information practices employed by sites linked to or from our web site. In most cases, links to non-First Resource Bank web sites are provided solely as pointers to information on topics that may be useful to the users of the First Resource Bank web site. If you are asked to provide information on one of those web sites, we strongly urge that you study carefully their privacy policies.

PRIVACY COMMITMENT TO YOU

Trust us to keep you informed of how we protect your privacy and limit the sharing of information you provide to us – whether it is at our branch, over the phone or through the Internet.

HOW TO CONTACT US

If you have other questions or concerns about our privacy policies, please call us at (610)363-9400 or send us an email at info@firstresourcebank.com