SECURITY & PRIVACY

Security

Community Bank Credit Card Services is an online payment system that provides you with information about your credit card account, including transaction activity, and permits you to make one-time payments or set up recurring automatic payments of your credit card bill. Payments made through Community Bank Credit Card Services result in electronic funds transfers from the depository account you choose and establish on file. Electronic transfers from consumer accounts are covered by Regulation E, which may limit your liability for unauthorized transfers where you give timely notice.

Access to Community Bank Credit Card Services is through a unique name known as your User ID and a password that you create when you sign up. You should never share this information and should keep it confidential and stored in a secure location. We use this information to authenticate your identity when you log on to the site to prevent unauthorized access. We will never email you and ask you for your user ID, password or other personal information. We will email you upon setup to your email address on file with a confirmation code for you to complete your sign on process.

We will capture your IP Address during the enrollment process as well as other attributes to create a device fingerprint. We will allow up to 5 different IP addresses. This enhanced security feature is offered to protect the user and all of your security information. We reserve the right to restrict certain IP addresses to prevent fraud.

To protect the information you provide through the site, we use strong encryption and secure socket layering. Encryption refers to the practice of scrambling data so unauthorized parties cannot decipher it and obtain your personal information. We require that your browser use 128 bit encryption. We automatically disconnect you after a period of inactivity. We also limit the type of transfers you may make through the site. You may only pay your credit card bill through the site and cannot make transfers to any other account.

You too can mitigate the risk or unauthorized access to your accounts by doing the following:

- Create strong and different passwords from those used for other online activity.
- Change your passwords periodically.
- Avoid using easily available information such as your date of birth, first or last name only, last 4 digits of your social security number.
- Keep passwords secure and never store them in a location where others can view them. Never use “Remember Me” to store user IDs and passwords on public computers.
- For business accounts, periodically perform a risk assessment and evaluate controls in place to detect and prevent unauthorized or fraudulent charges and payments.
- Phishing scams send fraudulent emails or pop up messages that appear to come from legitimate sources. They may ask you to verify personal information to steal your log-in

password and credentials. Never provide personal information or account information through email.
- Maintain a secure session and detect potentially fraudulent transactions, update your security software and run a system scan weekly.
- Set up text message alerts if offered with your payment/deposit holding financial institution and/or your card account financial institution.
- Look for the secure site symbol on your browser. "Https" indicates a secure website where your online information is encrypted.
- Download the latest version of your web browser to safely surf the web.
- Update your operating system to ensure you have the latest security updates.
- Back up your data regularly using a removable storage device.
- Make wireless network security a priority at home and on the road.
- Review your credit card statement and online activity and ensure that all transactions and payments posted are valid authorized transactions. Confirm your billing address and account balance are accurate.
- Avoid giving out personal information over the phone and if you do, make sure you know and understand why it is required and how it will be used.
- Shared documents containing personal information such as credit card and other bank statements.
- Have the post office hold your mail when away from home and traveling.

Identity Theft – To report the theft of your identity, please call (304) 485-7991

Lost or Stolen Card – To report a lost or stolen card, please call (866) 563-1335

For further information relating to credit card fraud or identity theft, visit http://www.ftc.gov/bcp/menus/consumer/data.shtm

Privacy

We collect the following types of information through your use of this site:
- Information about you such as your name, address, social security number, mother's maiden name;
- Information about your transactions with us, and others, such as your account balance, payment history, parties to transactions and credit card usage;

We use this information to:
- Provide services to you
- To verify transactions,
- Authenticate your identity

We will not share or disclose any of the personally identifiable information about you to third parties other than what is required to provide services to you through this site.