COMMUNITY FIRST BANK

Safeguarding Your Financial Information

At Community First, our highest priority is the protection of your personal and financial information, and we go to great lengths to maintain your privacy and security. There are also steps that you can take to protect yourself, which are provided below. Please review this information carefully and save it as a reference. As always, thank you for banking with Community First.

ONLINE BANKING

General Tips

- Community First ***will never*** initiate contact with you to request your logon credentials or any other confidential information. Do not give that information to anyone over the telephone.
- When using Online Banking, ensure that the "secure site" (padlock) icon is visible.
- Remember to change your password periodically.
- Maintain the confidentiality of your password.
- Ensure that your firewall is active.
- Log off from the Online Banking site once your banking is complete.
- Review you bank statements in a timely manner.
- Always double-check the website URL to ensure that it is correct and not misspelled.
- Keep your security software up to date.

Personal Banking Customers

- Ensure the strength of your password by incorporating both upper- and lower-case letters, numbers and special characters.
- When shopping online, follow the steps provided by your credit card vendor to use your secure code for protection against unauthorized use of your card.
- For more information, visit ***www.fdic.gov/bank/individual/online/safe.html.***

Business Customers

- Evaluate your online banking risks and related controls via:
  - Internal/external control assessment
  - Firewall intrusion testing
  - Safeguarding of passwords/password-protected software
  - Prompt deletion of system access for former employees
  - Dual control access
  - Employee background checks/credit bureau report review

To learn more about safe online banking, visit:

- ***www.consumerfinance.gov***
- ***www.ftc.gov***
- ***www.usa.gov***
- ***www.idtheft.gov***

MOBILE BANKING

- Make sure that your telephone app is downloaded from a reputable source.
- If your phone is lost or stolen, notify Community First as soon as possible.

REPORTING LOST OR STOLEN CREDIT OR DEBIT CARDS

- If your credit cards are stolen, file a report with the police, and cancel the cards immediately.
- Report missing cards to one of the three major credit reporting agencies, and file a fraud alert in your credit report:
  - Equifax (800) 525-6285
  - Experian (888) 397- 3742
  - TransUnion (800) 680-7289
- Report the loss to Community First, and consider opening new accounts and/or stopping payments on any outstanding transactions.
  - Credit Cards (800) 325-3678
  - Debit Cards (800) 472-3272
- Contact Community First, and we will notify our check verification service. One of the companies that accepts reports of check fraud directly from consumers is:
  - TeleCheck (800) 710-9898
- Get a new card (debit and/or credit) with a new number and password.

PREVENTING IDENTITY THEFT

- Pay attention to your statements.
- Do not give out personal information over the phone or through the mail or email unless you have initiated the contact.
- Safeguard or destroy (shred) personal information.
- When you make up your Personal Identification Number (PIN), do not use something a thief might guess (birth date, Social Security number, phone number, etc.).
- Order and review your credit report every year.
- Shop online only with trusted companies.
- Do not click on emails from unknown senders.

RECOGNIZING FRAUD

If you can answer YES to any of the following questions you may be the victim of fraud or identify theft.

- Have you been asked to wire funds to any other foreign country?
- Have you been asked to pay "upfront" money to receive a greater sum of money at a later date?
- Have you been informed via email or telephone that you were the winner in a lottery from a foreign country?
- Have you been offered pay or commission to facilitate in the transfer of money?
- If you recently sold an item over the Internet, is the amount of the check you received more than the selling price of the item? Were you asked to refund the difference? Is the check drawn on an individual or business different from the person buying your item or product?
- Have you been invited to participate in a "once in a lifetime" investment opportunity requiring a good faith down payment?
- Have you received text messages to your cell phone appearing to be from your bank to solicit personal information related to reactivating your ATM card?
- Have your used your PIN at an ATM that has a suspicious device attached or appears otherwise modified or less than genuine?

To report any Suspicious Account Activity or Security Events, contact Community First at:

CFB Operations Department
Attn: Senior Operations Officer
PO Box 1097
Walhalla, SC 29691
(864) 638-4603
customerservice@c1stbank.com

To learn about online fraud, go to ***www.fraudwatchinternational.com***.

OTHER INFORMATION

For consumer mortgage loan information requests or reporting suspected errors, please write:

Community First Bank
Attn: Loan Administration
449 Highway 123 Bypass
Seneca, SC 29678

For Community Reinvestment Act (CRA) comments, please write:

Community First Bank
Attn: CRA Officer
PO Box 1097
Walhalla, SC 29691

REGULATION E – CONSUMER ACCOUNTS ONLY

The Consumer Financial Protection Bureau is the governing agency that regulates electronic fund transfers under Regulation E. This regulation provides certain consumer protections for your demand accounts as long as you report any unauthorized activity in accordance to the following guidelines:

- You will have $50 liability for unauthorized transfers reported within two (2) business days of learning of the loss or theft of an access device.
- Notification after two (2) business days increases your maximum amount of liability to $500 U.S.
- If you do not tell us within 60 days after the account statement was sent or made available, you could be liable for the full amount of any amount you lost after the 60 days.

COMMUNITY FIRST BANK