Online Banking Customer Awareness and Education Program

Electronic Fund Transfers: Your Rights and Responsibilities (Regulation E Disclosure)

Indicated below are types of Electronic Fund Transfers we are capable of handling, some of which may not apply to your account. Please read this disclosure carefully because it tells you your rights and obligations for the transactions listed. You should keep this notice for future reference.

Electronic Fund Transfers Initiated By Third Parties: You may authorize a third party to initiate electronic fund transfers between your account and the third party's account. These transfers to make or receive payment may be one-time occurrences or may recur as directed by you. These transfers may use the Automated Clearing House (ACH) or other payments network. Your authorization to the third party to make these transfers can occur in a number of ways. For example, your authorization to convert a check to an electronic fund transfer or to electronically pay a returned check charge can occur when a merchant provides you with notice and you go forward with the transaction (typically, at the point of purchase, a merchant will post a sign and print the notice on a receipt). In all cases these third party transfers will require you to provide the third party with your account number and financial institution information. This information can be found on your check as well as on a deposit or withdrawal slip. Thus, you should only provide your financial institution and account information (whether over the phone, the Internet, or via some other method) to trusted third parties whom you have authorized to initiate these electronic fund transfers. Examples of these transfers include, but are not limited to:

- Preauthorized credits: You may make arrangements for certain direct deposits to be accepted into your checking or savings.
- Preauthorized payments: You may make arrangements to pay certain recurring bills from your checking or savings.

ATM card transactions: types of transactions: You may access your account(s) by ATM using your ATM card and your personal identification number (PIN) to:

- Withdraw cash from checking or savings
- Transfer funds from checking to savings
- Transfer funds from savings to checking
- Get balance information about checking or savings

Some of these services may not be available at all terminals.

Limits and fees: Please refer to our fee disclosure for information about fees and limitations that may apply to these electronic fund transfers.
ATM Operator/Network Fees: When you use an ATM not owned by us, you may be charged a fee by the ATM operator or any network used (and you may be charged a fee for a balance inquiry even if you do not complete a fund transfer).

Documentation

Terminal transfers: You can get a receipt at the time you make a transfer to or from your account using an automated teller machine.

Preauthorized credits: If you have arranged to have direct deposits made to your account at least once every 60 days from the same person or company:

- The person or company making the deposit will tell you every time they send us the money.
- You can call us at (731) 669-3900 to find out whether or not the deposit has been made.

Periodic statements: You will get a monthly account statement from us for your checking account(s).

Preauthorized Payments

Right to stop payment and procedure for doing so: If you have told us in advance to make regular payments out of your account, you can stop any of these payments. Here is how:
Call or write us at the telephone number or address listed in this disclosure in time for us to receive your request three business days or more before the payments is scheduled to be made. If you call, we may also require you to put your request in writing and get it to us within 14 days after you call.

Notice of varying amounts: If these regular payments may vary in amount, the person you are going to pay will tell you, 10 days before each payment, when it will be made and how much it will be. (You may choose instead to get this notice only when the payment would differ by more than a certain amount from the previous payment, or when the amount would fall outside certain limits that you set.)

Liability for failure to stop payment of preauthorized transfer: If you order us to stop one of these payments three business days or more before the transfer is scheduled, and we do not do so, we will be liable for your losses or damages.

Financial Institution's Liability

Liability for failure to make transfers: If we do not complete a transfer to or from your account on time or in the correct amount according to our agreement with you, we will be liable for your losses or damages. However, there are some exceptions. We will not be liable, for instance:

1.) If, through no fault of ours, you do not have enough money in your account to make the transfer.
2.) If you have an overdraft line and the transfer would go over the credit limit.
3.) If the automated teller machine where you are making the transfer does not have enough cash.
4.) If the terminal or system was not working properly and you knew about the breakdown when you started the transfer.
5.) If circumstances beyond our control (such as fire or flood) prevent the transfer, despite reasonable precautions that we have taken.
6.) There may be other exceptions stated in our agreement with you.

Confidentiality

We will disclose information to third parties about your account or the transfers you make:

1.) Where it is necessary for completing transfers; or
2.) In order to verify the existence and condition of your account for a third party, such as a credit bureau or merchant; or
3.) In order to comply with government agency or court order; or
4.) If you give us written permission.

Unauthorized Transfers

(a) Consumer liability. Tell us AT ONCE if you believe your card and/or code or password has been lost or stolen. Telephoning is the best way of keeping your possible losses down. You could lose all of the money in your account (plus your maximum overdraft line of credit). If you tell us within four business days, you can lose no more than $50 if someone used your card or password without your permission. (If you believe your card and /or code or password has been lost or stolen, and you tell us within four business days after you learn of the loss or theft, you can lose no more than $50 if someone used your card and /or code without your permission.)

If you do NOT tell us within four business days after you learn of the loss or theft of your card and/or code or password, and we can prove we could have stopped someone from using your card and/or code without your permission if you had told us, you could lose as much as $300.

Also, if your statement shows transfers that you did not make, tell us at once. If you do not tell us within 60 days after the statement was mailed to you, you may not get back any money you lost after the 60 days if we can prove that we could have stopped someone from taking the money if you had told us in time.

If a good reason (such as a long trip or hospital stay) kept you from telling us, we will extend the time period.

(b) Contact in event of unauthorized transfer. If you believe your card and/or code or password has been lost or stolen, call or write us at the telephone number or address listed in this disclosure. You should also call the number or write to the address listed in this disclosure if you believe a transfer has been made using the information from your check without your permission.

Error Resolution

In case of errors or questions about your electronic transfers, call or write us at the telephone number or address listed in this disclosure, as soon as you can, if you think your statement or receipt is wrong or if you need more information about a transfer listed on the statement or receipt. We must hear from you no later than 60 days after we sent the FIRST statement on which the problem or error appeared.

(1) Tell us your name and account number (if any).

(2) Describe the error of the transfer you are unsure about, and explain as clearly as you can why you believe it is an error or why you need more information.

(3) Tell us the dollar amount of the suspected error.

If you tell us orally, we may require that you send us your complaint or question in writing within 10 business days.

We will determine whether an error occurred within 10 business days (20 business days if the transfer involved a new account) after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days (90 days if the transfer involved a new account, a point-of-sale transaction, or a foreign-initiated transfer) to investigate your complaint or question. If we decide to do this, we will credit your account within 10 business days (20 business days if the transfer involved a new account) for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within 10 business days, we may not credit your account. Your account is considered a new account for the first 30

days after the first deposit is made, unless each of you already has an established account with us before the account is opened.

We will tell you the results within three business days after completing our investigation. If we decide that there was no error, we will send you a written explanation.

You may ask for copies of the documents that we used in our investigation.

If you have inquiries regarding your account, please contact us at:

Centennial Bank
PO Box 308
Trezevant, TN 38258
BUSINESS DAYS: Monday, Tuesday, Wednesday, Thursday and Friday
Holidays are not included.
PHONE: (731) 669-3900

Notice of ATM/Night Deposit Facility User Precautions

As with all financial transactions, please exercise discretion when using an automated teller machine (ATM) or night deposit facility. For your own safety, be careful. The following suggestions may be helpful.

1. Prepare for your transactions at home (for instance, by filling out a deposit slip) to minimize your time at the ATM or night deposit facility.
2. Mark each transaction in your account record, but not while at the ATM or night deposit facility. Always save your ATM receipts. Don't leave them at the ATM or night deposit facility because they may contain important account information.
3. Compare your records with the account statements you receive.
4. Don't lend your ATM card to anyone.
5. Remember, do not leave your card at the ATM. Do not leave any documents at a night deposit facility.
6. Protect the secrecy of your Personal Identification Number (PIN). Protect your ATM card as though it were cash. Don't tell anyone your PIN. Don't give anyone your information regarding your ATM card or PIN over the telephone. Never enter your PIN in any ATM that does not look genuine, has been modified, has a suspicious device attached, or is operating in a suspicious manner. Don't write your PIN where it can be discovered. For example, don't keep a note of your PIN in your wallet or purse.
7. Prevent others from seeing you enter your PIN by using your body to shield their view.
8. If you lose your ATM card or if it is stolen, promptly notify us. You should consult the other disclosures you have received about electronic fund

transfers for additional information about what to do if your card is lost or stolen.

9. When you make a transaction, be aware of your surroundings. Look out for suspicious activity near the ATM or night deposit facility, particularly if it is after sunset. At night, be sure that the facility (including the parking are and walkways) is well lighted. Consider having someone accompany you when you use the facility, especially after sunset. If you observe any problem, go to another ATM or night deposit facility.
10. Don't accept assistance from anyone you don't know when using an ATM or night deposit facility.
11. If you notice anything suspicious or if any other problem arises after you have begun an ATM transaction, you may want to cancel the transaction, pocket your card and leave. You might consider using another ATM or coming back later.
12. Don't display your cash; pocket it as soon as the ATM transaction is completed and count the cash later when you are in the safety of your own car, home, or other secure surroundings.
13. At a drive-up facility, make sure all the car doors are locked and all of the windows are rolled up, except the driver's window. Keep the engine running and remain alert to your surroundings.
14. We want the ATM and night deposit facility to be safe and convenient for you. Therefore, please tell us if you know of any problem with a facility. For instance, let us know if a light is not working or there is any damage to a facility. Please report any suspicious activity or crimes to both the operator of the facility and the local law enforcement officials immediately.

Accessing Online Banking

You will access your accounts linked to Online Banking by using your password. Your password is confirmation of your identity and must be used when accessing Online Banking. You are responsible for the security of your password. You should keep your password confidential to reduce the chance that your account(s) will be accessed by unauthorized individuals.

Electronic Communication with Centennial Bank

Users of Online Banking may communicate with Centennial Bank via email. When communicating with Centennial Bank electronically, you agree that you will not use the service for any purpose that is unlawful, obscene, abusive, defamatory or threatening. You further agree that transmissions of confidential business and sensitive personal information is at your sole risk and that we reserve the right to monitor and review transmissions online and in storage, and to remove or reject any material which we, at our sole discretion, believe may be unlawful or objectionable, without prior notice to the user.

Terms and conditions for Account Transfers

Online Banking may be used to transfer funds between the following account types if linked to Online Banking:

- Checking Accounts
- Savings Accounts
- NOW Accounts
- MMA Accounts

Online Banking may be used to make loan payments to the following loan types if linked to Online Banking:

- Installment Loans

You may access all account types and lines of credit if linked to Online Banking to:

- View account balances, history and other information.

Fraud Prevention and Risk Reduction

User ID and Password Guidelines

- Create a “strong” password with at least 8 characters that includes a combination of mixed case letters and numbers.
- Change your password frequently. Centennial Bank requires that you change your password every 90 days.
- Never share your username and password information with third-party providers. Centennial Bank will never ask for your Password. Centennial Bank will also never contact you on an unsolicited basis and ask for your Online Banking credentials.
- Do Not use an automatic login feature that saves usernames and passwords.
- Memorize your password and do not write it down.
- You are responsible for keeping your password account data confidential. You are solely responsible for controlling the safekeeping of and access to, your password. When you give someone your password, you are authorizing that person to use your Online Banking. You are responsible for all transactions performed using your password, even if you did not intend or authorize them. In addition, fraudulent transactions initiated using your password will be charged against your account(s).

General Guidelines

- Do not use public or other unsecured computer for logging in to Online Banking.
- Check your last login date/time every time you log in.
- Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to Centennial Bank.
- View transfer history.
- Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.
- Whenever possible, register your computer to avoid having to re-enter challenge questions and other authentication information with each login.
- Never leave your computer unattended while logged in to Online Banking.
- Never conduct banking transactions while multiple browsers are open on your computer.
- Commercial Online Banking customers should consider performing a risk assessment and controls evaluation periodically.

Tips to Avoid Phishing, Spyware and Malware

- Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, and similar information. Opening file attachments or clicking on web links in suspicious e-mails could expose your system to malicious code that could hijack your computer.
- Never respond to a suspicious e-mail or click on any hyperlink embedded in a suspicious e-mail. Call the purported source if you are unsure who sent an e-mail.
- If an e-mail claiming to be from Centennial Bank seems suspicious, check with us by calling (731) 669-3900.
- Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Update all of your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.
- Ensure computers are patched regularly, particularly operating system and key application with security patches.
- Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers.

- Check your settings and select, at least, a medium level of security for your browsers.
- Clear the browser cache before starting an Online Banking session in order to eliminate copies of Web pages that have been stored on the hard drive. How the cache is cleared depends on the browser and the version you are using. This function is generally found in the browser's preferences menu.

Tips for Wireless Network Management

Wireless networks can provide an unintended open door to your business network. Unless a valid business reason exists for wireless network use, it is recommended that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:

- Change the wireless network hardware (router/access point) administrative password from the factory default to a complex password. Save the password in a secure location as it will be needed to make future changes to the device.
- Disable remote administration of the wireless network hardware (router/access point).
- If possible, disable broadcasting the network SSID.
- If your device offers WPA encryption, secure your wireless network by enabling WPA encryption of the wireless network. If your device does not support WPA encryption, enable WEP encryption.
- If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network.

Financial Institution Contacts

If you notice or suspect any suspicious account activity or information security-related events contact any of the employees below as soon as possible:

Misty Sharp
Bank Secrecy Act Officer
Centennial Bank
PO Box 308
Trezevant, TN 38258
(731) 669-3900
msharp@mycentennial.bank

Whitney McCullar
Chief Operating Officer
Centennial Bank
PO Box 308
Trezevant, TN 38258
(731) 669-3900
wmccullar@mycentennial.bank