Online Banking Customer Awareness and Education Program

Centennial Bank is committed to protecting its customers' information. Centennial Bank will NEVER request personal information by phone, email or text messaging including account numbers, personal identification information, passwords or any other confidential customer information. Our top priority is to safeguard your confidential information and we work diligently to do so.

Internet Banking Security
Centennial Bank uses the latest technology to secure your information when transmitted over the Internet. Encryption standards such as TLS and trusted certificates are used to protect your information when transferred between your computer and Centennial Bank.

In addition to the security features managed by Centennial Bank, here are some things you can do to protect your information:

- Watch out for suspicious emails that ask for your personal information. If you receive an email from us and are unsure whether it is legitimate, then please contact us and we will be glad to assist you.
- Never share or give out your Access ID, User Name, Passwords, or Security Challenge Questions & Answers.
- Do not use personal information as your Access ID, User Name or Passwords.
- Create hard-to-guess passwords that include upper & lower case letters, numbers and special symbols.
- Change your passwords frequently and don't use the same ones from before.
- Avoid using public computers and WiFi to access your Internet Banking portal.
- Do not provide any personal information to web sites that do not use encryption or other secure methods of protection.
- Ensure that your computer is equipped with up-to-date Anti-Virus software.
- Ensure your computer and mobile device have the latest software version.

Commercial Banking Internet Security
In addition to the information provided regarding "Internet Banking Security", Commercial & Small Business account holders should institute additional measures in order to further protect their online banking information. For example:

- Perform your own annual internal risk assessment & evaluation on all online accounts.
- Establish internal policies regarding employee internet usage.
- Ensure all company computers are equipped with up-to-date antivirus protection software.

What is Identify Theft?
Identify theft occurs when someone uses your personal information such as your Social Security number, account number or credit number, without your permission, to commit fraud or other crimes. Protect yourself by:

- Reporting lost or stolen checks or credit cards immediately
- NEVER give out any personal information
- Shred all documentation that contains confidential information (i.e. bank and credit card statements, bills and invoices that contain personal information, expired credit cards and pay-stubs).
- Check your credit report annually

Check Your Credit

Any consumer can request one free copy of his or her credit report every year. Reviewing your credit report can help you find out if someone has opened unauthorized financial accounts, or taken out unauthorized loans, in your name.

Contact the three major credit bureaus - Equifax (1-800-685-1111), Experian (1-888-397-3742) and Trans Union (1-800-916-8800) to request a copy.

How to Contact Us

The Internet Banking Department can be reached at our toll free number 1-877-389-6479 or directly by email at operations@mycentennial.bank. In addition do not hesitate to contact us immediately to report any of the following:

General Internet Banking inquiries, Lost or stolen Access ID, User Name or Password, Receipt of suspicious or fraudulent mail, email or websites related to Centennial Bank

How Does Regulation E Apply to Your Accounts with Internet Access?

Regulation E protects individual consumers engaging in electronic fund transfers (EFT). Non-consumer (or business) accounts are not protected by Regulation E.

What is an EFT?

The electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions initiated through electronic-based systems. The term includes, but is not limited to:

- Point-of-sale transfers
- Automated Teller Machine transfers (ATM)
- Direct deposits or withdrawal of funds
- Transfers initiated by telephone
- Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal
- Transfers initiated through internet banking/bill pay

How does Regulation E apply to a consumer using internet banking and/or bill pay?

Regulation E is a consumer protection law for accounts established primarily for personal, family, or household purposes. Non-consumer accounts, such as Corporations, Partnerships, Trusts, etc. are excluded from coverage. Regulation E gives consumers a way to notify their financial institution that an EFT has been made on their account without their permission.

Is Your Account Protected?

Any fraudulent or unauthorized EFTs are protected. For a description on what an EFT is under Regulation E please refer to the section “What is an EFT?” above. Further information on Regulation E and how it applies to your account here at Centennial Bank is available on our website at **www.mycentennial.bank.**

What are the applicable protections provided under Regulation E for consumers who use internet banking and/or bill pay?

If you believe an unauthorized EFT has been made on your account, contact us immediately. If you notify us within 2 business days after you learn of the loss or theft of your ATM/debit card or Personal Identification Number (PIN), the most you can lose is $50. Failure to notify the bank within 2 business days may result in additional losses.

Unlimited Liability:

Unlimited loss to a consumer account can occur if:

- The periodic statement reflects an unauthorized transfer of money from your account, and you fail to report the unauthorized transfer to us within 60 days after we mailed your first statement on which the problem or error appeared.

Exclusions from Protection

The term EFT does not include:

- *Checks* – Any transfer of funds originated by check, draft or similar paper instrument or any payment made by check, draft or similar paper instrument at an electronic terminal.
- *Check Guarantee or Authorization* – Any transfer of funds that guarantees payment or authorizes acceptance of a check, draft or similar paper instrument but does not directly result in a debit or credit to a consumer’s account.
- *Wire or other similar transfers* – Any transfer of funds through a wire transfer system that is used primarily for transfers between financial institutions or between businesses
- *Securities and Commodities Transfers* – Any transfer of funds for the primary purpose of the purchase or sale of a security or commodity, if the security or commodity is:
    - Regulated by the Securities and Exchange Commission or the Commodity Futures Trading.
    - Purchased or sold through a broker-dealer regulated by the Securities and Exchange Commission or through a futures commission merchant regulated by the Commodity Futures Trading Commission.
    - Held in Book-entry form by a Federal Reserve Bank or federal agency
- *Automatic transfers by account-holding institution* – Any transfer of funds under an agreement between a consumer and a financial institution which provides that the institution will initiate individual transfers without a specific request from the consumer:
    - Between a consumer’s accounts within the financial institution.
    - From a consumer’s account to an account of a member of the consumer’s family held in the same financial institution.
    - Between a consumer’s account and an account of the financial institution, except that these transfers remain subject to § 205.10(e) regarding compulsory use and

sections 915 and 916 of the act regarding civil and criminal liability. (Refer to “Coverage in Detail” section below)

- *Telephone-initiated transfers* - Any transfer of funds that:
  - Is initiated by a telephone communication between a consumer and financial institution making the transfer; and
  - Does not take place under a telephone bill payment or other written plan in which periodic or recurring transfers are contemplated.

Regulation E – Coverage in Detail
For a complete detailed explanation of protections provided under Regulation E; please visit the Consumer Financial Protection Bureau’s (CFPB’s) website:

- *CFPB – Electronic Funds Transfers Act (Regulation E)*
  http://www.consumerfinance.gov/eregulations/1005

How does Regulation E apply to a non-consumer using internet banking and/or bill pay?
A non-consumer (business account) customer using internet banking and/or bill pay is not protected under Regulation E. As such, special consideration should be made by the business customer to ensure adequate internal security controls are in place that commensurate with the risk level that the customer is willing to accept.

As a non-consumer customer you should perform periodic assessments to evaluate the security and risk controls you have in place. The risk assessment should be used to determine the risk level associated with any internet activities you perform and any controls you have in place to mitigate these risks.

Mobile Banking Safety Tips
Managing your finances using a smartphone or tablet can be very convenient.
However, you should consider these safety tips to protect your account information:
Be proactive in protecting your smartphone and/or tablet by installing anti-malware software on the device.

1. Research any application (app) before you download it. Fraudulent apps are often designed with names that look like real apps. It’s best if you access an app using a link from the provider’s website.
2. Create a strong password or PIN for your mobile app and your device.
   - Use at least eight characters
   - Do not use your username, real name or company name
   - Do not use a complete word
   - Make it significantly different from previous passwords
   - Use a character from each of the following categories (some apps may limit symbols)
     - Uppercase letters
     - Lowercase letters
     - Numbers

3. Use an auto-lock or time-out feature so your device will lock when it is left unused for a certain period of time.
4. Upgrade your device to the latest operating system version.
5. Do not jailbreak or root your mobile device. Doing so exposes the security controls and makes your device vulnerable to cyber-attacks.
6. Check your account history periodically to make sure there are no fraudulent transactions.
7. Take precautions in case your device is lost or stolen, before your device is lost or stolen. Avoid leaving your device unattended in public places.
8. Consult your wireless provider to see if they provide a service to remotely erase your device or turn off access to your device and/or account in the event your device is lost or stolen.
9. Always conduct your transactions in a safe environment. Use your cellular service or your own internet provider rather than unsecured/public Wi-Fi networks like those offered at coffee shops.
10. Don’t send account numbers or PIN in emails or text messages, because those methods are not necessarily secure.

Additional information and tips on how to safe-guard your online security are available at:

Consumer Information: Identity Theft
https://www.consumer.ftc.gov/features/feature-0014-identity-theft

Consumer Information: Wiring Money
https://www.consumer.ftc.gov/media/audio-0048-wiring-money

Protecting Your Business: Start With Security
https://www.ftc.gov/news-events/audio-video/business

Consumer Action: Complaints
https://www.usa.gov/consumer-complaints#item-212527

FDIC Consumer Protection
http://www.fdic.gov/consumers/

NACHA Fraud Resources
https://www.nacha.org/Fraud-Phishing-Resources

US Department of Homeland Security
http://www.us-cert.gov/home-and-business/

Federal Communication Commission - Business Cyber-planner
http://www.fcc.gov/cyberplanner

Federal Trade Commission: Identity Theft by Mobile Phone
https://www.consumer.ftc.gov/blog/identity-theft-mobile-phone

Federal Trade Commission: Tips for Using Public WiFi Networks
https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks