CUSTOMER SECURITY AWARENESS AND EDUCATION

Banking online can be a way to save you, the customer, time and money. At Citizens Bank of Cape Vincent, we want you to know that our online banking system is secure and your personal and financial information are protected.

Citizens Bank of Cape Vincent is committed to protecting your personal information. We will never request personal information by telephone, mail e-mail r texting messaging including account numbers, personal identification information, passwords, or any other confidential information. The bank's goal is to safeguard your confidential information and we will continue to work diligently to do so.

INTERNET BANKING SECURITY

The following are some tips to protect your confidential information:

- Never share or give out your access ID, user name, password, or security challenge questions and answers.
- Do not use personal information as your access ID, user name or password.
- Create difficult passwords that include letters, numbers, upper and lower case letters (case – sensitive) and special characters.
- Change your password frequently.
- Avoid using public computers to access your internet banking.
- Do not provide any personal information to web sites that no not use encryption or other secure methods of protection.
- Ensure that your computer is equipped with up to date anti-virus and malware software protection.

COMMERCIAL INTERNET BANKING SECURITY

In addition to the information provided regarding Internet Banking Security, commercial and small business account holders should implement additional measures in order to further protect their online banking security.

The following are examples of such measures:

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

WHAT IS IDENTITY THEFT?

Identity theft occurs when someone uses your personal information such as your social security number or account number without your permission, to commit fraud or other crimes. Help protect yourself by:

- Immediately reporting lost or stolen checks and credit/debit cards.
- Never giving out any personal information.
- Shred all documentation that contains confidential information (i.e. bank statements, credit card statements, bills and invoices that contain any personal information, as well as any expired credit cards or paystubs.
- Check your credit report annually.

WHAT IS PHISHING?

In a typical phishing attempt you will receive an e-mail that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the e-mail may appear to come from a government agency, including one of the federal institution regulatory agencies.

The e-mail will warn you of a serious problem that requires your immediate attention and encourage you to click on a button to go to the institution's website.

You then could be redirected to a phony website that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual website. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information.

In either case, you may be asked to update your account information or to provide information for verification purposes such as your social security number, account number, password, or the information you use to verify your identity when speaking to the real financial institution, such as your mother's maiden name or your birthplace.

If you provide the requested information, you could find yourself a victim of identity theft.

HOW TO PROTECT YOURSELF

- Never provide your personal information in response to an unsolicited request.
- If you believe that the contact may be legitimate, contact the financial institution yourself.
- Never provide your password over the telephone or in response to an unsolicited internet request (Citizens Bank of Cape Vincent would never ask you to verify your account information online).
- Review account statements regularly to ensure all charges are correct.

- Any consumer may request one free copy of their credit report per year. Reviewing your credit report can help you find out if someone has stolen your identity. You can contract 877-322-8228 for a copy of your free annual credit report from one of the three major credit bureaus, Transunion, Equifax and Experian.

WHAT TO DO IF YOU FALL VICTIM

- Contact your financial institution immediately and alert them to the situation at 315-654-2115.
- If you have disclosed sensitive information in a phishing attack, you should also contact at least one of the three major credit bureaus and discuss whether you need to place a fraud alert on your credit file. The fraud alert will help prevent the thieves from opening a new account in your name. The bureaus contact information are listed below for your convenience.

    - **Equifax**
      866-349-5191
      PO Box 740256
      Atlanta, GA 30374

    - **Experian**
      888-397-3742
      PO Box 1017
      Allen, TX 75013

    - **TransUnion**
      800-680-7289
      PO BOX 2000
      Chester, PA 19016

HOW DOES REGULATION E APPLY TO YOUR ACCOUNTS WITH INTERNET ACCESS?

Regulation E protects individual consumers engaging in electronic fund transfers (EFT). Business accounts are not protected by this regulation.

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 (ATM) transfers).
- 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.
- Electronic check conversion.

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, trust, 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 COVERED?

Any fraudulent or unauthorized EFTs are protected. For a description of what an EFT is under Regulation E please refer to "What is an EFT?" above.

WHAT ARE THE APPLICABLE PROTECTIONS PROVIDED TO CONSUMERS UNDER THE ACT FOR CONSUMERS WHO USE INTERNET BANKING AND/OR BILLPAY?

If you believe an unauthorized EFT has been made on your account, contact Citizens Bank of Cape Vincent immediately. If you notify the bank within two (2) business days after you learn of the unauthorized transaction the most you can lose is $50. Failure to notify the bank within two (2) business days may result in additional losses.

No Liability Limit

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 the bank within 60 days after the bank mailed the first statement in 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 par 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 institutions* – 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 account 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.
- *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 plan or other written plan in which periodic or recurring transfers are contemplated
    - Small institutions – Any pre-authorized transfer to or from an account if the assets of the account holding financial institution were $100 million or less on the preceding December 31. If assets of the account holding institution subsequently exceed $100 million, the institution's exemption for preauthorized transfers terminates one year from the end of the calendar year in which the assets exceed $100 million.

REGULATION E-COVERAGE IN DETAIL

For a complete detailed explanation of protections provided and not provided under Regulation E, please visit the following link as provided by the FDIC: http://www.fdic.gov/regulations/laws/6500-3100.htm/

HOW REGULATION E APPLIES TO A NON-CONSUMER USING INTERNET BANKING AND/OR BILL PAY?

A non-consumer (business customer) using Internet banking and/or bill pay is not protected under Regulation E because the non-consumer account is not protected by Regulation E. Special consideration should be made by the business to ensure that adequate internal security controls are in place that commensurate with the risk level that the business is willing to accept.

Precautions a non-consumer should take because they are not protected by Regulation E

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

FOR ORE INFORMATION AND TIPS ON HOW TO SAFEGUARD YOUR ON-LINE SECURITY, THE FOLLOWING VIDEOS AND LINKS ARE AVAILABLE TO YOU

Avoiding ID Theft: http://www.FDIC.gov

Internet Crime Complaint Center: http://www.lc3.gov

U.S. Department of Justice: http://www.Justice.gov/criminal/faud/websites/idtheft.html

Protecting your Workplace: http://www.us-cert.gov/reading room/distributablt.html

Securing Your PC and Protecting Kids Online: http://www.onguardononline.gov

Federal Trade Commission: http://www.ftc.gov/

Federal Bureau of Investigation: http://fbi.gov/

CITIZENS BANK OF CAPE VINCENT ASSOCIATION CONTACT INFORMATION

Customers may contact any one of the following bank employees in the event you notice suspicious account activity or experience customer information security-related events:

Cape Vincent Office: 315-654-2115

Erika Ward

Teresa Hazlewood

Mary Titus

Chaumont Office: 315-649-2265

Paula Cadwell

LouAnne Thompson

LaFargeville Office: 315-658-2600

Debra Montondo

Caralee Handschuh