Customer Awareness for Security and Fraud Prevention

Identity theft continues to be a growing problem in our society today. All consumers must manage their personal information wisely and cautiously to minimize risk. You can guard against identity theft by following a few simple rules:

- ✓ Never reveal personal indentifying information unless you are sure of how it will be used and whether it will be shared with others. Ask for the businesses Privacy Policy to review how personal information will be used and shared.
- ✓ Never give out personal information on the phone, through the mail, or over the Internet unless you have initiated the contact and you know who you are dealing with.
- ✓ Review your billing cycles on all bills. A missing credit card bill could signal that an identity theft may have gotten access to your account and changed the billing mailing address.
- ✓ Guard your outgoing mail by placing it in post office collection boxes or at your local post office.
- ✓ Add passwords to your credit card, bank and phone statements.
- ✓ Do not provide user names and passwords to anyone for any reason.
- ✓ Keep papers with personal information in a safe place. Shred your charge receipts, copies of credit applications, physician statements, insurance forms, bank checks and statements you are discarding, expired charge cards and credit offers you receive in the mail. Many communities have a “Shred Day”.
- ✓ Keep all personal information in your home in a secure place not easily discovered by a burglar.
- ✓ Verify who has your personal information at your place of employment and verify that these records are kept in a secure location.
- ✓ Maintain an accurate record of all credit cards that you carry with you. Include in the record the names on the credit cards, account number, expiration date and phone number to call in case the credit card is lost or stolen. If your credit cards are lost or stolen call the company as soon as you realize the credit card is not in your possession. Cancel the credit card immediately.
- ✓ Do not carry your social security card with you. Give your social security number only when it is absolutely necessary. Use another identifier when possible.
- ✓ Check your credit report at least once a year to make sure it is accurate and includes only activities you have authorized.

If you suspect any of the following please contact us immediately:

- ✓ Fraudulent activity on your account
- ✓ Unauthorized check or paper draft activity on your account
- ✓ Unauthorized ACH withdrawals on your account
- ✓ Unauthorized debit card transactions on your account
- ✓ Unauthorized wire transfers on your account
- ✓ Lost or stolen checks
- ✓ Lost or stolen debit or ATM card

You may call our toll free number at 866-877-4892, Monday to Friday from 8:30 a.m. to 4:30 p.m. To report a lost or stolen MidCoast Community Bank debit or ATM card after normal business hours and on holidays please call 800-554-8969.

Credit Bureaus

Equifax

Web Site: www.equifax.com
To report fraud call 800-525-6285
To order your credit report you may call 800-885-1111 or send a letter to:
P.O. Box 740241
Atlanta GA 30374

Experian

Web Site: www.experian.com
To report fraud call 888-397-3742
To order your credit report you may call 888-397-3742 or send a letter to:
P.O. Box 2104
Allen TX 75013

TransUnion

Web Site: www.tuc.com
To report fraud call 800-680-7289
To order your credit report you may call 800-916-8800 or send a letter to:
P.O. Box 1000
Chester PA 19022

Debit and ATM Card Fraud

You should never loan your debit or ATM card to anyone. Never write your ATM PIN on your ATM card. Never give your debit or ATM card number over the phone or Internet unless you have initiated the transaction. Carry only the cards you use frequently. Never leave your wallet or purse unattended or in a parked vehicle.

Internet Fraud

Internet purchases have increased significantly over the past several years. You can buy just about anything on the Internet with a credit or debit card. Purchasing on the Internet is convenient; however, care must be taken when using a credit or debit card to purchase goods and services on the Internet.

- ✓ Learn as much as possible about the products and seller.
- ✓ Read and understand the retailers' return and refund policy.

- ✓ Choose a secure password to protect your account information. Include upper case, lower case, a special character and a number in your password, if possible.
- ✓ Passwords should be changed frequently.
- ✓ Only order from retailers that offer a secure checkout and payment process.
- ✓ If an offer sounds highly suspicious or too good to be true, it probably is.

Securing On Line Transactions

- ✓ Select a User ID, Passcode, and Security Questions that are difficult to guess, but easy for you to remember. Avoid using family member names, local sports names, birth dates, anniversaries, addresses or phone numbers.
- ✓ Do not share your Internet Banking User ID or Passcode with anyone. Never use information that could be readily found in your wallet or purse, such as your house number or date of birth. Memorize you Internet Banking User ID or Passcode instead of writing it down.
- ✓ Internet Banking is a good way for you to monitor your accounts. You have direct access to your accounts and transactions 24 hours a day with any Internet connection.
- ✓ Never provide your financial information to an unfamiliar website.
- ✓ Don't leave your computer during an Internet Banking session. Always "sign-off" of Internet Banking when you complete a session or leave your computer.
- ✓ Review monthly financial statements promptly and report any discrepancies immediately. Never ignore suspicious charges on your statements. If doubtful or unauthorized charges appear on your bills or statements, call immediately to resolve the discrepancy.
- ✓ Shred unnecessary financial documents, including old bank statements, invoices, and unwanted pre-approved credit offers.

Cell Phone Text Messages

Beware of text messages received on your cell phone telling you to use your computer to access the web address given in the text message. You are told that unless you comply you will be charged or subscribed to a service. Once you use your computer to go to the web address given, your computer may be compromised with a Trojan Horse program and your data security may be at risk.

Lottery Scam

A typical lottery scam begins with an unexpected e-mail notification that you have won a large sum of money in a lottery. The email is often originating from a free e-mail account such as Yahoo, Hotmail, MSN, etc. Scammers will often use the names of legitimate lottery organizations, thereby trying to make themselves look legitimate. You are usually told to keep the notice secret and to contact a claims agent to validate. After contacting the "agent" you are asked to pay a processing fee or transfer charge so the winnings can be distributed. Of course, you never hear from them again.

Peer-to-Peer File Sharing (P2)

Peer-to-peer (P2P) developers have created decentralized, encrypted, anonymous networks that can find their way through corporate and residential firewalls. Criminals actively search P2P networks for personal information they can use to commit identity theft. There are several ways for confidential data to find its way to a P2P network, including instances where users accidentally share folders containing such data. Examples include users storing music and other data in the same folder that is shared, or users unknowingly downloading malware that exposes their file directories to the network.

Pharming

Pharming is a variation of phishing in which a malicious code is installed on a personal computer or server, misdirecting users to fraudulent websites without their knowledge or consent. Once on the fraudulent site, the user will be asked to submit confidential information and the attackers will capture this information for illegal use.

Vishing

Vishing (or "voice phishing") are attacks in which bank customers are contacted by e-mail or sometimes automated phone call and told that their checking accounts have been compromised. Instead of being referred to a website, as in phishing scams, customers are urged to call a local or toll-free number. The number connects to an automated response system that answers the call and asks you to input account information and/or your Social Security number to clear up the "problem."

Secure Your PC

Install a firewall. A firewall is software or hardware that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to your computer, depending on your firewall settings. Even if you think there's nothing on your computer that would interest anyone, a worm could completely disable your computer, or someone could use your computer to help spread worms or viruses to other computers without your knowledge.

Install anti-virus and keep the definitions updated. This software and definitions can be downloaded to your PC from an anti-virus website such as Symantec or Avast.

Never open attachments in emails that you do not recognize the sender of the email. Delete the email immediately and empty you deleted email folder.

Revised 3-2013