Internet-Related Fraud and Identity Theft

A GUIDE TO PROTECTING YOUR ACCOUNTS

Internet-related fraud schemes and Identity Theft present a real and immediate risk to you-our valued customers. You can help protect your identity and private information by practicing good security habits and reporting any suspicious activity to the bank.

<u>Internet-Related Fraud</u>
Internet scammers try to steal financial information from unsuspecting victims by using fraudulent e-mails that try to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information.

The scammers will send pretend emails that look like they are from businesses the potential victim deals with - for example, their Bank, a Government authority, an Internet service provider, or an online payment service. The e-mails are written with a sense of urgency and concern. The scammers tell recipients that they need to "update" or "validate" their billing information to keep their accounts active, and direct them to a "look-alike" Web site of the legitimate business, further tricking consumers into thinking they are responding to a bona fide request. Unknowingly, consumers submit their financial information - not to the businesses - but to the scammers, who use it to steal money from your accounts.

Listed below are some things that you can do to help protect your personal information:

- If you get an e-mail that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the e-mail. Instead, contact the company cited in the e-mail using a telephone number or Web site address you know to be genuine.

- Should you receive an e-mail that appears to come from our bank asking for personal or confidential information, please report the incident to the bank at 618-566-8800. <u>Citizens Community Bank does not use e-mail as a way to confirm, update or validate any personal or confidential information about you or your accounts.</u>

- Before submitting any type of financial information through a Web site, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.

- Never give your personal data over the phone, through the mail or via an e-mail solicitation unless you have initiated the contact.

- Protect your account numbers, card numbers, PINs and passwords.

- Always check with one of our branches should you have any questions concerning any solicitation of your personal or account information. We are always here to help you in any way we can.

- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

- If you have replied to a suspicious e-mail and provided private information about your Citizens account, please contact us immediately at 618-566-8800.

<u>IDENTITY THEFT PROTECTION</u>
Up to 500,000 individuals are victims each year of identity theft, a fast-growing form of fraud. Fortunately, a few simple steps can help protect you from becoming a statistic.

Identity Theft or Account Takeover Fraud involves criminals stealing a person's personal information and assuming their identity by applying for credit in their name, running up huge bills, defaulting on creditors and generally destroying the victim's credit record. The loss of a purse or wallet can be devastating.

You can take the following steps to avoid becoming a victim of identity theft:

- Don't give your Social Security or account numbers to anyone over the phone unless you initiated the call.
- Tear up or shred receipts, old bank statements and unused credit card offers before throwing them away. Thieves could steal information from your trash and use it to obtain credit in your name.
- Review your bank and credit card statements as soon as you receive them to check for unauthorized transactions.
- Protect your PINs and computer passwords; consider using a combination of letters and numbers and change them often. Never carry this information with you!
- Order copies of your credit report once a year to ensure accuracy. To do so, call any of the three national credit reporting agencies:
  Trans Union- Credit Report (800) 888-4213   to report fraud (800) 680-7289
  Experian -   Credit Report (888) 397-3742   to report fraud (888) 397-3742
  Equifax -   Credit Report (800) 685-1111   to report fraud (800) 525-6285
- Report any suspected fraud to your bank and credit card issuers immediately so they can start to close accounts and clear your name immediately. You may also contact the Federal Trade Commission's ID Theft Consumer Response Center toll free at (877) IDTHEFT (877-438-4338).

Restoring your identity can be a tremendous inconvenience. Protect yourself against this crime by protecting your personal information.

Citizens Community Bank - and the entire banking industry – has a tradition of customer trust. Helping customers prevent and resolve cases of identity theft is another way we can continue this tradition.

Should you have any questions or need to report suspected fraud, please contact us at 618-566-8800.

Thank you for choosing us as your financial partner.