Marion Center Bank
Online Banking
Customer Awareness and Education

Marion Center 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. Fraudulent emails may be designed to appear as though they are originated by Marion Center Bank. **Do not respond** to any email communications which request any type of personal or confidential information and do not go to any links listed on that email. These communications are not originated by Marion Center Bank! Our top priority is to safeguard your confidential information and we work diligently to do so.

Checking Account Fraud

Although, we have safeguards in place and we constantly update our training programs, the best person qualified to guard against checking account fraud is you.
Here's how you can guard against it.

1. Make sure you destroy all old, unused checks, or special checks from credit card mailings that you do not intend to use. Ideally, these should be shredded.
2. Do not order checks with your social security number or driver's license number printed on them.
3. If you're newly ordered checks are late arriving, please contact us at 724-464-2265. When you receive your order, verify that the information is correct and that you have the correct number you ordered.
4. Remove mail promptly from your mailbox and store checks in a secure place.
5. Conceal checks from view when you mail them by wrapping them in paper or by using security envelopes.
6. Reconcile your account promptly.
7. If your checks are stolen, notify us immediately.

Identity Theft

You may find yourself the victim of identity theft by merely replying to an e-mail. Phishing (pronounced "fishing") involves the use of seemingly legitimate e-mail messages and Internet Web sites to deceive consumers into disclosing sensitive information, such as bank account information, social security numbers, credit card numbers, passwords and personal identification numbers (PINs). The message may claim to be from a business or organization that you deal with or even a government agency. The message may ask you to "update", "validate" or "confirm" your account information. Some phishing e-mails threaten a dire consequence if you don't respond.

How to protect yourself

1. NEVER provide your personal information in response to an unsolicited request, whether it is over the phone or the Internet. If you get an e-mail message or pop-up message that asks for personal or financial information, do not reply and don't click on the link in the message either. Legitimate companies will not ask for this information via e-mail. If you are concerned about your account, contact the company mentioned in the e-mail using a phone number you know to be genuine.
2. NEVER access our web page from a link provided by a third party.
3. Use anti-virus software, spy ware, and a firewall and keep them up to date.
4. Don't e-mail personal or financial information.
5. Review credit card and bank statements as soon as you receive them.
6. Be cautious about opening attachments or downloading any files from e-mails.
7. Contact the organization impersonated in the e-mail and advise them of the scam. You may notify the bank at 724-464-2265.

If you believe you have been scammed, file a complaint at www.ftc.gov and then refer to the information in our Online Security section pertaining to identity theft.

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 billpay?
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.

What are the applicable protections provided to consumers under the Act 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 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 we mailed your 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 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 for a detail explanation of protections provided under Regulation E)

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.
- Small institutions. Any preauthorized 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. . (Refer to “Coverage in Detail” section below for a detail explanation of protections provided under Regulation E)

Regulation E – Coverage in Detail

For a complete detail explanation of protections provided and not provided under Regulation E; please visit the following link as provided by the FDIC:

- FDIC – Electronic Funds Transfers (Regulation E) https://www.fdic.gov/regulations/laws/rules/6000-1350.html

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 adequate internal security controls are in place that commensurate with the risk level that the customer is willing to accept.

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

As a non-consumer 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 any internet activities the non-consumer customer performs and any controls in place to mitigate these risks.

For more information and tips on how to safe-guard your online security, take a look at the following videos and links:

Protecting Personal Information: A Guide for Business http://business.ftc.gov
Consumer Action: Complaints http://www.usa.gov/complaints/
FDIC Consumer Protection http://www.fdic.gov/consumers /
ID Theft https://www.identitytheft.gov/#/
NACHA Fraud Resources https://www.nacha.org/content/current-fraud-threats-0/
US Department of Homeland Security http://www.us-cert.gov/home-and-business/
Federal Communication Commission - Business Cyber-planner: http://www.fcc.gov/cyberplanner

Online Security Information

Marion Center Bank understands that the security of your personal account information is important to you. We also understand that our continued success as a financial institution relies on both our ability to offer banking services to you in a secure manner as well as your responsibility in keeping any access codes and passwords secure. To assist us in offering these Web-based banking services in a secure manner, we employ a number of measures, which are described below. These measures allow us to properly authenticate your identity when you access these services and protect your information as it travels between your PC and Marion Center Bank. With the proper safety measures in place, your online banking transactions remain safe and secure. The following measures have been taken to ensure your privacy.

Information Encoding

We use the latest encryption technology to ensure that your private information cannot be intercepted. Encryption is a way to rewrite something in code, which can be decoded later with the right "key." When you request information about your accounts, the request is sent encrypted to Marion Center Bank. We decrypt your request and send the requested information back to you in an encrypted format. When you receive the information, it is decoded so that you can read it.

Personally Selected Account Names

Marion Center Bank does not display your full account numbers over the Internet. We ask you to choose a "pseudo" name for each of your accounts. Example of pseudo name would be vacation account, checking account, and savings account. You can change your "pseudo" account name under the "Options" section of our online banking service.

Unique ID and Password

In order to access your accounts online, you must enter a unique User ID and Password. We strongly recommend that you choose a Password that you can remember (without writing it down) but does not use information that can be easily guessed by someone. Avoid the use of birthdays, children's names, etc. Do not reveal your User ID or Password to anyone.

Three (3) strikes and you're out

If an unauthorized person attempts entry into an end user's account by trying to guess a Log-In ID, the bank will disable the password on the third incorrect attempt, thus invalidating the Log-In combination. If you accidentally activate this security feature by unintentionally miss-keying a password three times, you would need to contact the Bank to reestablish access for that account. For example, a common mistake made by the end user is having the CAPS-LOCK on while keying in a password.

To further protect you, a timeout feature is used. This feature will automatically log you out of your current financial service session after a 10-minute inactivity period on our site.

Your Marion Center Bank passwords never expire. Passwords are required to have a combination of 9-17 characters and numbers. It must contain one Uppercase letter, one Lowercase letter, one number and one symbol. Multi Factor Authentication along with User ID and password and security questions are used to access online banking.

Email Communications

Please remember that email through this site is secure against interception, and you should be cautious when sending an email with personal information. If your information is very sensitive, or includes personal or confidential information-such as your bank account, charge card or Social Security number-you should contact us by postal mail or telephone.

How You Can Protect Your Internet Security

While Marion Center Bank works to protect your banking privacy, you will also play an important role in protecting your accounts. There are a number of steps you can take to ensure that your Marion Center Bank account information is protected, including:

- Keep your Password to yourself.
- Change your Password frequently.
- Remain at your computer until your Online Banking transactions are completed and log out. Log out of Online Banking prior to visiting other Internet sites.
- Don't use obvious numbers or easily accessible information for your log-in ID and Password.
- Ensure that no one is watching when entering your log-in ID and Password.
- Don't record your log-in ID and Password on paper. Try to memorize them, if possible.
- If you do record your log-in ID and Password, keep them in a safe, secure location.
- Do not share your log-in ID and Password with anyone.
- Review your account information often. Report any unusual activity immediately.
- NEVER give account information to anyone over the telephone unless you initiated the call.

If you notice suspicious or unusual activity on your Online Banking accounts, call the bank immediately.
For further help or suggestions about staying safe online visit these helpful links.

- Stay Safe Online
- Security Alerts

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 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 anti-virus protection software

Identity Theft

What to do if it happens to you

This guide provides victims of identity theft with the major resources to contact. Unfortunately, at this time victims themselves are burdened with resolving the problem. You must act quickly and assertively to minimize the damage.

In dealing with the authorities and financial institutions, keep a log of all conversations, including dates, names, and phone numbers. Note time spent and any expenses incurred, in case you are able to request restitution in a later judgment or conviction against the thief. Confirm conversations in writing. Send correspondence by certified mail, return receipt requested. Keep copies of all letters and documents.

1. Credit Bureaus

Immediately call the fraud units of the three credit reporting companies:

Equifax: P.O. Box 105069, Atlanta, GA 30348
Report fraud: Call (800) 525-6285 and write to address above.
Order credit report: (800) 685-1111. Web: www.equifax.com

Experian (formerly TRW): P.O. Box 9532, Allen, TX 75013
Report fraud: Call (888) 397-3742) and write to address above. Fax: (800) 301-7196
Order credit report: (888) 397-3742. Web: www.experian.com

Trans Union: P.O. Box 1426, Buffalo, NY 14231
Report fraud: (800) 680-7289 and write to address above.
Order credit report: (800) 632-1765. Web: www.transunion.com

Report the theft of your credit cards or numbers and request a credit report (free to identity theft victims). Ask that your file be flagged with a fraud alert. Add a victim's statement to your report. ("My ID has been used to apply for credit fraudulently. Contact me at [your phone number] to verify all applications.") Ask how long the fraud alert is posted on your file, and how you can extend it if necessary.

Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Request a free copy of your credit report annually from each of the three Credit Bureaus, so you can monitor any new fraudulent activity.

Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers). When you provide your police report to the credit bureaus, they must remove the fraudulent accounts from your credit report. (See #3 below.)

2. Creditors

Contact all creditors immediately with whom your name has been used fraudulently, by phone and in writing. You may be asked to fill out fraud affidavits. (No law requires these to be notarized at your own expense.) Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request" (better than "card lost or stolen" because it can be interpreted as blaming you.) Monitor your mail and bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

3. Law Enforcement

Report the crime to your local police or sheriff's department. You might also need to report it to police departments where the crime occurred. Give them as much documented evidence as possible. Make sure the police report lists the fraud accounts. Get a copy of the report. Keep the phone number of your investigator handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report in order to verify the crime. It is a violation of federal law (18 USC 1028) and the laws of many states to assume someone's identity for fraudulent purposes. Some police departments do not write reports on such crimes, so be persistent! Also, report to the Federal Trade Commission at (877) IDTHEFT. Web: https://consumer.gov.

4. Stolen Checks

If you have had checks stolen or bank/credit union accounts set up fraudulently; report it to the appropriate check verification companies (see below). Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account (not mother's maiden name). If your own checks are rejected at stores where you shop, contact the check verification company that the merchant uses.

5. ATM/Debit Cards

If your ATM or debit card has been stolen or compromised, report it immediately at 866.221.8610. Get a new card. Monitor your account statement. You may be liable if fraud is not reported quickly.

6. Fraudulent Change of Address

Notify the local Postal Inspector if you suspect an identity thief has filed a change of your address with the post office or has used the mail to commit fraud. (Call the U.S. Post Office to obtain the phone number). Find out where fraudulent credit cards were sent. Notify the local Postmaster for that address to forward all mail in your name to your own address. You may also need to talk with the mail carrier. (Web: www.usps.gov/websites/depart/inspect)

7. Secret Service Jurisdiction

The Secret Service has jurisdiction over financial fraud but, based on U.S. Attorney guidelines, it usually does not investigate individual cases unless the dollar amount is high or you are one of many victims of a fraud ring. To interest the Secret Service in your case, you may want to ask the fraud department of the credit card companies, banks and/or credit unions as well as the police investigator, to notify the Secret Service agent they work with. (Web: www.treas.gov/usss)

8. Social Security Number (SSN) Misuse

Call the Social Security Administration to report fraudulent use of your SSN. As a last resort, you might want to try to change your number, although we do not recommend it except for the most serious cases. The SSA will only change the number if you fit their fraud victim criteria. Also, order a copy of your Personal Earnings and Benefits Statement and check it for accuracy. The thief might be using your SSN for employment purposes. (Web: www.ssa.gov)

9. Passports

Whether you have a passport or not, write the passport office to alert them to anyone ordering a passport fraudulently.

10. Phone Service

If your long-distance calling card has been stolen or there are fraudulent charges on the bill, cancel the account and open a new one. Provide a password that must be used any time the account is changed.

11. Driver's License Number Misuse

You may need to change your driver's license number if someone is using yours as ID on bad checks or for other types of fraud. Call the state office of the Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license. Go to your local DMV to request a new number. Fill out the DMV's complaint form to begin the investigation process. Send supporting documents with the completed form to the nearest DMV investigation office.

12. Victim Statements

If the imposter is apprehended by law enforcement and stands trial, write a victim impact letter to the judge handling the case. Contact the victim-witness assistance program in your area for further information on how to make your voice heard in the legal proceedings.

Resources

To opt out of pre-approved offers of credit for all three bureaus, call (888) 5OPTOUT. You may choose a two year opt-out period or permanent opt-out status.

Remember, you are entitled to a free credit report if you are a victim of identity theft, if you have been denied credit, if you receive welfare benefits, or if you are unemployed.

Social Security Administration - Report fraud: (800) 269-0271. Order Earnings & Benefits Statement: (800) 772-1213. Web: www.ssa.gov

To remove your name from mail and phone lists

Direct Marketing Association (Web: www.dmachoice.org)

- Online registration $2 fee
- Mail Preference Service, $3 fee payable by check or money order to ANA no cash: DMAChoice, Consumer Preferences, P.O. Box 900, Cos Cob, CT 06807.

To report fraudulent use of your checks

- CheckRite: (800) 766-2748
- Chexsystems: (800) 428-9623
- CrossCheck: (800) 843-0760
- Equifax: (800) 437-5120
- International Check Services: (800) 526-5380
- SCAN: (800) 262-7771
- TeleCheck: (800) 710-9898

Other Useful Resources

- Federal Trade Commission (FTC)
  The FTC offers help to victims. File your case with the FTC Consumer Response Center, (877) IDTHEFT. Web: www.consumer.gov
- Privacy Rights Clearinghouse (PRC)
  3100 - 5th Ave., Suite B, San Diego, CA 92103. Phone: (619) 298-3396. E-mail: prc@privacyrights.org Web: www.privacyrights.org
- Identity Theft Resource Center
  Lists local victim support groups: www.idtheftcenter.org . E-mail: voices123@att.net
- FBI Internet Fraud Complaint Center www.ic3.gov
- U.S. Dept. Of Justice
  identity theft information, www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-Identity-fraud
- Identity Theft Survival Kit
  Phone: (800) 725-0807. Web: www.identitytheft.org

For further helpful hints about protecting yourself from fraud, identity theft and phishing visits these helpful sites.

- Internet Fraud Tips
- Consumer Information
- Anti-Phishing Working Group

Below is a glossary of terms commonly used in electronic banking:

Adware – The purpose of adware is to display ads. Some adware threats bombard you with so many ads you can hardly use the computer.
Keylogger – Basically, a form of spyware, a keylogger captures everything you type, including passwords and other sensitive information. Some keyloggers also capture screen shots, log your Web browsing history, record anything copied to the clipboard and more.
Malware – The term malware applies to any software whose purpose is malicious, including all other types described here.
Pharming – Hackers use malicious programs to route you to their own sites.
Phishing – Technique used by fraudsters to acquire username, password and other sensitive information through social engineering by masquerading as a legitimate website, message or other communication.
Ransomware – A malicious computer program that restricts or disables your computer then a “pop-up” window comes up requesting you to pay a fee to fix it.

Rootkit – Antivirus software can only remove threats that it can detect. Rootkit technology hides a threat's file and Registry traces so that most programs can't see them. Only specialized anti-malware technology can bring the hidden file into view.
Smishing – SMS (short message service) technology used to send text messages. This is often used on cellphones to get information.
Spyware – Spyware simply means malicious software that steals credit card numbers, passwords, and other sensitive personal information.
Trojan – Named for the Trojan Horse of legend, a Trojan is a seemingly benign program that does something nasty in secret. Trojans are the most common type of malware on the Android platform. While you play a Trojanized Android game, it may be sending your contacts to a server in Russia or making $10/minute phone calls.
Virus – A computer virus spreads by injecting its code into other programs or, less commonly, into the boot sector of a disk. When you execute the infected program, the virus code runs too. It may simply infect more files, or it may perform a "payload" action like wiping out your hard drive.
Vishing – It is another name for "voice phishing", which the fraudsters use recorded messages to telephones claiming they are the bank. They then trick you into giving your personal information.

How to contact us

The Retail Services Department can be reached at 724-464-2265 ext. 7791 or 7790. In addition, do not hesitate to contact us immediately to report any of the following: General Internet Banking inquiries, Lost or stolen User ID, User Name or Password, Receipt of suspicious or fraudulent mail, email or website related to Marion Center Bank.