

**TIPS FOR FRAUD PREVENTION  
AND  
SAFEGUARDING FINANCIAL INFORMATION**

Central Illinois Bank is committed to protecting your personal and account information. We have account monitoring systems and other controls in place to recognize and stop fraud. Below are tips and useful information to help you protect your personal and business information.

**Account and Check Fraud**

Precautions and steps listed here can be performed to reduce the risk of account and check fraud from happening.

1. Safeguard the checks you carry with you. Never leave your checkbook in your vehicle.
2. Never sign blank checks or give signed blank checks to someone else to complete.
3. Report lost or stolen checks to the bank immediately, regardless of how many checks are involved or how certain you are of whether or not the checks are lost or stolen.
4. Safeguard your reserve supply of checks, and again, report lost or stolen checks to the bank immediately.
5. Balance your checkbook promptly upon receipt of the statement. Report immediately to the bank any forgeries, unauthorized entries, and anything else unusual.
6. Shred anything you throw away that contains an account number or any other account information (e.g. deposit slips, deposit receipts, account statements, old checks and deposit tickets you no longer intend to use, ATM receipts, etc.).
7. If you choose to close your account, shred all checks or bring to the bank to shred and notify the bank immediately of the account closing.
8. Never give your account information or personal information to someone on the phone unless you made the call. No bank will ask you for information it already knows.

If you believe you are the victim of check fraud, contact your bank immediately for assistance.

**TIPS FOR FRAUD PREVENTION  
AND  
SAFEGUARDING FINANCIAL INFORMATION**

**Identity Theft**

Precautions and steps listed here can be performed to reduce the risk of identity theft from happening.

1. Never give your account information, credit card information or personal information to anyone over the phone or online unless you initiated the call/service and know the party is legitimate. No bank or credit card company will ask you for information it already knows.
2. Shred all credit card or bank statements. Do not just throw away. The same applies to credit card offers received in the mail.
3. Never include your social security number, driver's license number or date of birth on any sensitive documents.
4. Place all outgoing mail in an official postal mailbox. Rural residential mail boxes are prime targets for thieves.
5. Be aware of any missed bills and report them immediately.
6. Use a bank safe deposit box to store and protect important documents.
7. Review your credit report at least once a year.

If you believe you are a victim of Identity Theft:

- a. Call the toll free number of any of the three major credit bureaus to place a fraud alert on your credit report (Equifax 1-800-525-6285, Experian 1-888-397-3742, TransUnion 1-800-680-7289).
- b. Review your credit report.
- c. Close any accounts that have been tampered with or opened fraudulently.
- d. Contact your bank so an alert can be placed on your record.
- e. File a police report.
- f. File a complaint with the FTC at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.

For more information about Identity Theft and what you can do to prevent it from happening to you, visit the Federal Trade Commission website at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.

**TIPS FOR FRAUD PREVENTION  
AND  
SAFEGUARDING FINANCIAL INFORMATION**

**Online Fraud**

Precautions and steps listed here can be performed to reduce the risk of online fraud from happening.

There are many fraudulent websites and scams that take place online. Always attempt to know who you are doing business with. If the offer sounds too good to be true, it probably is a fraud. If you have won something without doing anything, it probably is a fraud. The following are just some of the scams online with tips to prevent you from falling victim.

1. Lottery/Sweepstakes – You receive an email notifying you, “Are a Winner”, yet you never entered a lottery or sweepstakes (that you can remember). Don’t fall for it. Do not respond no matter how good it may sound. If you really believe you are a genuine winner, ask your bank for assistance.
2. Employment Opportunities – You respond to a “work at home” ad where you will be sent “up front” money to set up your office. Once the check arrives, you are then instructed to send back a portion of it. Or, your responsibilities are to reship packages you receive to other addresses for which you will be paid a fee. Don’t fall for it. Ask your bank for assistance.
3. 419 Scams – You receive an email from an unknown party who requests assistance in placing large amounts of money into an overseas bank account. For your assistance, you are promised large amounts of money. Don’t fall for it. Do not provide any of your personal or account information. Ask your bank for assistance.
4. Phishing – Never give your personal information or account or credit card information to anyone who requests it online unless you know you are dealing with a legitimate business. Never go into a link that is provided in an email. Go directly to that website instead of linking in from an unsolicited email. Remember, your bank and credit card company will never ask you for information it already has. Ask your bank for assistance.
5. Online Purchases – Be wary of non-local sellers of hard to find items that require payment only via MoneyGram. Instead, only deal with sites that accept a credit card. And never use your debit card online for purchases, always use a credit card. Ask your bank for assistance.
6. Online Romance Fraud – In most cases, the person lives in another country. He or she will pretend romantic intentions to gain your trust and affection and then use you to gain access to your money, bank accounts, credit cards or by getting you to commit financial fraud on their behalf (by sending you a counterfeit check to deposit with a request to send funds back to them). Ask your banker for assistance before making any commitments to send, wire or deposit items sent to you by this scammer.

If you believe you are a victim of Online Fraud:

- a. Contact your bank for assistance if you believe your accounts are at risk.
- b. File a police report.
- c. File a complaint with the Internet Crime Complaint Center at <http://www.ic3.gov>.

For more information about Online Fraud and what you can do to prevent it from happening to you, visit the Internet Crime Complaint Center website at <http://www.ic3.gov>.

**TIPS FOR FRAUD PREVENTION  
AND  
SAFEGUARDING FINANCIAL INFORMATION**

**Phone/Mail Solicitation Fraud**

Precautions and steps listed here can be performed to reduce the risk of phone/mail solicitation fraud from happening.

1. You receive mail notifying you, "Are a Winner", yet you never entered a lottery or sweepstakes (that you can remember). Don't fall for it. Do not respond no matter how good it may sound. If you really believe you are a genuine winner, ask your bank for assistance.
2. You receive mail from an unknown party who requests assistance in placing large amounts of money into an overseas bank account. For your assistance, you are promised large amounts of money. Don't fall for it. Do not provide any of your personal or account information. Ask your bank for assistance.
3. You receive an unsolicited check from an unknown party in the mail; bring it to the attention of someone at your bank before depositing such an item to your account. Ask your bank for assistance. It very well may be counterfeit.
4. Voice Phishing a/k/a Vishing - you receive a phone call (or text message) from someone who says they are an employee of your bank or your credit card company and ask to confirm information on your account. Don't fall for it. Your bank or credit card company has no reason to ask you for this information since it already has it. Report any such calls to your bank.
5. Register your home and cell phone numbers with the Federal Do Not Call Registry at 1-888-382-1222.

If you believe you are the victim of phone/mail solicitation fraud, contact your bank immediately for assistance.

If you believe you are a victim of mail theft, mail fraud, a false change of address, or Identity Theft via mail fraud, file a complaint with the U.S. Postal Inspection Service at <http://postalinspectors.uspis.gov>.

For more information about mail fraud and what you can do to prevent it from happening to you, visit the U.S. Postal Inspection Service website at <http://postalinspectors.uspis.gov>.

**TIPS FOR FRAUD PREVENTION  
AND  
SAFEGUARDING FINANCIAL INFORMATION**

**Credit Card/Debit Card Fraud**

Precautions and steps listed here can be performed to reduce the risk of credit card/debit card fraud from happening.

1. Never give your account number to someone who says they are an employee of your bank or your credit card company and ask to confirm information on your account. Don't fall for it. Your bank or credit card company has no reason to ask you for this information since it already has it. Report any such calls to your bank or credit card company.
2. Never write your PIN on your card.
3. Always use your debit card as a credit card (signature) transaction when using it at a merchant instead of using it as a debit card (PIN) transaction.
4. Report a lost or stolen card immediately to your bank or credit card company.
5. Promptly reconcile your statements and report any unauthorized charge.

If you believe you are the victim of credit card/debit card fraud, contact your bank immediately for assistance.

If you need assistance or more information, stop in any of our convenient branches or email us at [contact@cibmarine.com](mailto:contact@cibmarine.com). Never send your account information via an email system other than the email system within your secure online banking website.