Protect yourself from becoming a victim of fraud by using these best practices!

Online Fraud Prevention

- Make sure the security features of your computer software, including your web browser, are up-to-date.
- When reviewing your email, always be vigilant of scams. Keep in mind that forging emails and creating fraudulent websites have become easier for criminals because of the advancements in technology.
- Confirm any and all requests you receive for personal, financial or account information. Always be leery of requests that say it is urgent that you provide information.
- Be sure to call a company to confirm that they have indeed requested personal or account information from you to verify your account. You may also want to go to the company's website to confirm any requests that appear to be from them.
- Never share your login identification or passwords with anyone. Make sure you choose passwords that are difficult for others to guess and use different passwords for each of your accounts. Also, take advantage of the option to change your password.
- Be careful before you provide your e-mail address to any questionable web sites. Sharing your e-mail address makes you more likely to receive fraudulent e-mails.

Fake Check Scams

- The checks you would receive in the scams look so real that many times a bank teller would not spot them as fake. Some are phony cashiers checks, others may look as if they are from a business. The business name on the checks may be real, but the checks are usually counterfeited by the people pulling the scam.
- Under federal law, banks must make the funds you deposit available quickly - usually within one to five days. However, just because you can withdraw the money doesn't mean the check is good, even if it is a cashiers check. Forgeries often take time to be discovered.
- **Unfortunately, you are responsible for the check you deposited if it is discovered later to be fraudulent.** That is because you are in the best position to determine how risky the transaction is with the other person. If the check bounces, you owe the bank the money you withdrew. The bank may be able to take it from your accounts.

- Fake check scammers often scan newspapers and online advertisements for people listing items for sale, and check postings on online job sites for people seeking employment. They place their own ads with phone numbers or email addresses for people to contact them. They may even call or send emails or faxes to people randomly.
- Remember, there is no legitimate reason for someone who is giving you money to ask you to wire money back. This action is a clear sign that it is a scam.
- **If you think someone is trying to pull a fake check scam, don't deposit it and call us immediately to report it at 618-939-6194.**

ATM/Debit Card Fraud

- Do not talk to other people about your ATM account and how much money you have in it unless they are authorized users on the account.
- Don't lay your ATM or Debit card around the house, car, work, or any other place where someone could steal and use it.
- Examine ALL of your statements you receive from the bank for anything out of the ordinary like an unknown purchase or cash withdrawal.
- **DO NOT** let anyone know your Personal Identification Number (PIN).
- Be careful that no one sees you type in your PIN when you initiate any type of transaction. Use your body to shield the debit card or ATM keyboard when making transactions.
- Never use common numbers like your birth year or your SSN to determine your Personal Identification Number.
- Make sure that you receive YOUR debit card after a transaction by looking at the name on the front of the card.
- **If your debit card is lost or stolen, contact First National Bank Customer Service immediately to report it at 618-939-3792 during business hours or 800-528-2273 after business hours.**

Identity Theft

- Give your social security number only when it is absolutely necessary. Most businesses only need the last 4 digits if you can provide them with other information.
- Shred receipts or statements that you no longer need. This will make it harder for someone to get personal information.
- Do not give ANY personal information to anyone over the phone or internet unless you initiated the contact.
- Do not let billing statements or credit card advertisements stay in your mailbox. This gives criminals easy access to your information without them entering your home or your computer.
- Review your credit report.

Please contact us at 618-939-6194 if you become aware of a scam or believe you are a victim of any of these types of fraud. You may also contact us if you have any questions regarding fraud.