Educate yourself on the various types of fraud so you don't become the victim!

Phishing (FISH-ing)

This scam uses authentic looking emails and web sites to trick recipients into giving personal financial information such as account numbers, credit card numbers, social security numbers, user names, and passwords. The messages sometimes ask the recipients to follow a link and enter the information for verification purposes.

Phishing emails are basically spam emails with the intent to do harm to your finances. Spammers use websites, newsgroups, guesswork and list trading to get your email address. A phisher gathers emails the same way without the help of a financial institution. They give their victims the impression that they are representing the credit card company or bank.

Because most people have grown increasingly aware of this scam, most phishing emails are deleted. However, the quantity of attacks has increased. Also, the technology the criminals use has become more sophisticated allowing them to reach more victims.

Check Fraud

If someone you don't know wants to pay you by check, but wants you to wire some of the money back, beware! It's a scam that could cost you thousands of dollars.

How do fake check scams work? There are many variations of the scams. They usually start with someone offering to:

- Buy something you advertised for sale.
- Pay you to work at home.
- Give you an advance on a sweepstakes you've won.
- Give you the first installment on the millions you'll receive for agreeing to transfer money in a foreign country to your bank account for safekeeping.

Credit Card Scams

Credit card scams generally occur when:

- A thief goes through trash to find discarded receipts or carbons, and then uses your account numbers illegally.
- A dishonest clerk makes an extra imprint from your credit or charge card and uses it to make personal charges.
- You respond to a mailing asking you to call a long distance number for a free trip or bargain-priced travel package. You're told you must join a travel club first and you're asked for your account number so you can be billed. The charges you didn't make are added to your bill, and you never get your trip.
- Account information has been breeched or your lost credit card ends up in the wrong hands. For more information, visit the Federal Trade Commission at www.ftc.gov

Identity Theft

Identity Theft occurs when a criminal uses your name, address, Social Security number (SSN), bank account, or credit card account number without your knowledge to open accounts or make purchases.

You are most likely to become a victim of Identity Theft if:

- Your purse or wallet has been stolen containing identification, credit, and bank cards.
- You are scammed by someone who claims to be a legitimate business person.
- Your credit report or personal information was obtained by a dishonest employee abusing access to company records.
- Your information was obtained by someone hacking into business computers.

ATM/Debit Card Fraud

A thief would need both your PIN and the magnetic strip information on the back of your card to commit ATM or Debit Fraud. The PIN is not stored on the card's magnetic strip. So, if your card is stolen or duplicated, the thief has to find some way to get your PIN.

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.