

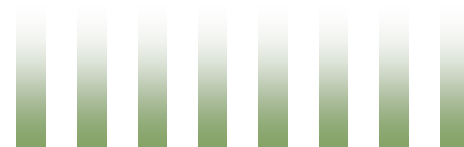


Nigerian Advance Fee Fraud

This scheme involves people pretending to be a Nigerian official or business person asking individuals and companies to help transfer millions of dollars out of Nigeria in exchange for high, no strings attached profits. Individuals and companies are being contacted through mass mailings, faxes, phone calls and emails.

The U.S. Secret Service has established a task force addressing this particular type of fraud. If you have been contacted in anyway regarding this type of scheme, please email any information you have regarding the incident to 419.fcd@uss.s.treas.gov or fax (202) 406-6930. If you have been a victim of this type of scheme and have had a financial loss, please contact your local U.S. Secret Service Field Office. You can find the office nearest you on the Secret Service website, www.secretservice.gov. If you would like to read more information about the Nigerian Advance Fee Fraud scheme, you may find it on the same website.

We have provided the following information as an educational tool for our customers. We hope the information will help you better understand the types of schemes that are prevalent in the world we live in and how to guard and protect yourself from becoming a victim of identity theft and fraudulent activity.



Bank of New Madrid
A Real Community Bank

MAILING ADDRESS & TELEPHONE NUMBERS

PO Box 10, New Madrid, MO 63869
573-748-5551

PO Box 607, Lilbourn, MO 63862
573-688-2111

PO Box 325, Portageville, MO 63873
573-379-5551

Banking Hours

Monday-Thursday

8:30-4:00

Friday

8:30-5:00

Saturday (drive-in only)

8:30-12:00

“www.bankofnewmadrid.com”

MEMBER FDIC



**SKIMMING AND
NIGERIAN ADVANCE FEE
FRAUD**



CREDIT CARD FRAUD is an unfortunate vulnerability we all face when we use our credit card(s) or debit card(s). It can happen whether we are conducting a transaction on-line, over the phone, or in a well-known department store. Because card security is so important, we recommend you practice the following rules when using your card(s).

- Memorize your PIN number, do not write it down.
- Never give your PIN number to anyone.
- If selecting your own PIN number, do not use personal information that can be easily obtained, such as your initials, birth date, or phone number.
- Sign your card as soon as you receive it.
- Maintain a list of card account numbers and phone numbers for reporting stolen or lost cards. Keep this list separate from your cards.
- Never give out card account information over the phone or over the Internet, unless you know the source to be a reliable one.
- Always verify the amount of the sale before signing the receipt.
- Be sure to retrieve your card from the merchant.
- Always know where your cards are, and never leave them in an area easily accessible to someone else.
- Report lost or stolen cards to the issuing bank immediately.
- Report any suspicious card activity to the issuing bank immediately.
- Keep receipts and compare to monthly card statements.
- Never reply to an email request for personal or account information.

If you happen to have a Visa credit card, a Bank of New Madrid Visa Debit card or any other Visa bank debit card, you can add safety to your online buying, with participating online stores, using Verified by Visa password protection. "Take the Visa card you already use, add a password to confirm your identity, and you've got verified by Visa-the new service exclusively for Visa cardholders. The password is linked to your card, not to your computer, helping prevent unauthorized purchases before they even happen. Create your own password today at www.visa.com/verified, and begin shopping with added security and peace of mind."

SKIMMING is a criminal act enabling criminals to obtain your credit card information in order to produce counterfeit cards. There are two types of skimming. The first is when someone takes an extra swipe of your card when you have handed it to the person for payment of some sort. The criminal takes a second swipe of your card into a small, hand-held device, known as a skimmer. This device extracts your card information and stores it and allows the criminal to create a counterfeit card. Once this is done, the information can be downloaded into a computer and emailed anywhere in the world.

The second type of skimming is collecting ATM/Debit card numbers and Pins for the purpose of stealing money from your account. Shoulder surfing is one way to accomplish this. Someone watches you while you use an ATM and steals your information that way. Criminals can also skim information by installing skimmers and small cameras on ATM machines. The skimmer reads the magnetic stripe on the back of the card and the camera is used to record the pin number being entered during the transaction. Once the criminal has the stolen information, they can then create counterfeit ATM/Debit cards that can be used to withdraw money or even make purchases.

Here are some simple steps to follow when using your ATM/Debit card:

- Always be aware of your surroundings when using an ATM.
- If using a drive-through ATM, lock car doors and roll up all car windows not being used.
- Have your card ready to use when you pull up to the ATM.
- Try to conduct transactions during daylight hours if possible, as most ATM-related crimes occur after dark.
- Look at the ATM closely. Be wary of any odd-looking devices or wires attached to the machine. If something doesn't look right to you, do not use the machine.
- Always protect your pin number. Do not give it to anyone else, or write it on the back of your card, and try to keep the keypad covered while entering your pin number during a transaction.
- Once the transaction is completed, remember to retrieve your card and take your receipt. You will want to check it against your monthly statement.
- You should always check your accounts regularly for any unusual activity or any unauthorized transactions. If you have not already enrolled in our E-Banking service, we recommend you do so as a means of monitoring your account activity. This service is a great way to help guard against identity theft, as well as keep track of your finances. If you happen to note anything suspicious on your account with us, call 573-748-5551 and report the incident immediately.

If you become a victim of credit card fraud, please follow the steps below to minimize the damage.

- Call the issuing financial institution or company of the card(s) in question. Report the incident to their fraud department and ask for the account(s) to be closed.
- Change passwords on all or your online accounts and any websites you have made payments or purchases using your card(s).
- Contact all three credit bureaus and place a fraud alert on your credit reports.

Equifax	(800) 525-6285
Experian	(888) 397-3742
TransUnion	(800) 680-7289

- Once you have reported the fraud, ask for a report from each bureau and request no new credit be granted without your authorization.
- When you receive your reports, be sure to check they are flagged with a "fraud alert" tag and a "victim's statement". You should insist the alert remain on your report for a maximum of seven years.
- Check the reports for any discrepancies in credit lines, debt owed on existing cards, and unexplained debts or unexplained accounts.

- You should contact the Federal Trade Commission and report the fraud incident. You can reach the FTC hotline at 877-438-4338, and they will advise you how to handle the situation.

- Fill out an FTC Identity Theft affidavit. You can then send it to the credit card companies of the cards in question to minimize your responsibility for the debt incurred by the fraud. The FTC will also enter your information in a nationwide "Consumer Sentinel" database for identity theft cases. This database is utilized by law enforcement agencies to find the people behind the credit card fraud.

- File a report with local police and request a copy so you may give it to your financial institution, your credit card companies, and all your other creditors.
- Document any conversations and follow up with correspondence when deemed necessary. Be sure to retain copies of all documents.