1ST FIRST NATIONAL BANK

What Banking Should Be.

FRAUD AWARENESS

Financial fraud is one of the most devastating things that can happen to you. Financial fraud is simply the theft or embezzlement of money or any other property from a person. We recognize that you have worked hard for your money and some basic steps can be taken to protect your money and prevent you from becoming a victim of financial fraud.

If you believe you have been a victim of fraud:

- File a police report with your local police station
- Report to Federal Trade Commission: **www.ftc.gov/complaint** or **877-382-4357**
- Report to Iowa Attorney General's Office at **888-777-4590 or 515-281-5926 in Des Moines**
- Report fraudulent activity on your FNB Bank account by calling 515-232-5561
- File a complaint with the Internet Crime Complaint Center (IC3) at https://www.ic3.gov/

COMMON FRAUD SCAMS

Fake Check Scams

With this scam, someone sends you a check and tells you to deposit it. Then they tell you to wire some or all of the money back to them — or to another person. The money appears in your bank account, so you do it. But the check is fake. It can take weeks for the bank to figure it out, but when it does, the bank will want you to repay the money you withdrew. Scammers make up lots of stories like...

- You've won a prize and need return part of the funds to pay taxes and fees.
- You've participated in a mystery shopping assignment to evaluate a bank's wire service.
- You've been overpaid for something you sold online and now you need to return the extra funds.
- You were offered a job and were sent a check for supplies, then you'll need to wire a portion back.

Romance Scam

Romance scammers create fake profiles on dating sites and apps. They strike up a relationship with you and work to build your trust, sometimes talking or chatting several times a day. Then, they make up a story — like saying they have an emergency — and ask for money. A romance scammer might also contact you through social media sites like Instagram, Facebook, or Google Hangouts.

Family Emergency Scam

You get an unexpected call from someone who pretends to be a friend or relative. They say they need cash for an emergency and beg you to wire money right away. They might say they need your help to get out of jail, pay a hospital bill, or leave a foreign country. They often ask you not to tell anyone in your family. Their goal is to trick you into sending money before you realize it's a scam.

FRAUD SAFETY TIPS

- **Verify the caller.** Call them back at a number you know to be genuine, not one they have given you.
- **Consult a trusted family member** before acting on any request.
- **Never give personal information,** including social security number, account number or other financial information, to anyone over the phone unless you initiated the call and the other party is trusted.
- **Trust your instincts.** Don't be fooled. If something doesn't feel right, it may not be right. If it sounds too good to be true, it probably is.
- **Never pay or send money** to anyone who claims you have won a prize.
- **Never act quickly.** Fraudsters are very demanding and request that funds be sent urgently.
- **Never send cash in the mail.**

Apartment Rental Scam

You respond to an ad for an apartment with surprisingly low rent. Before you've even seen the apartment, you apply and are told to wire money — maybe for an application fee, security deposit, or the first month's rent. After you wire the money, you find out that there is no apartment for rent, or that the scammer put their contact information on someone else's photo or rental ad. Scammers run a similar scam with vacation rentals.

1ST FIRST NATIONAL BANK

What Banking Should Be.

FRAUD: WIRE TRANSFERS & CASH WITHDRAWALS

A wire transfer is a way of moving money electronically between two banks. Wire fraud is a scheme that attempts to defraud or obtain money based on false representation or promises. It can occur in many different forms these days —from a phone call or an email to a text or social media messaging. Scammers may also ask you to withdrawal cash to purchase other monetary instruments.

First National Bank's staff is trained to ask multiple questions before sending funds by wire. You can help **even more** by educating yourself on the tactics used by con artists. This will add yet another layer of protection to your funds.

BEFORE WIRING FUNDS OR TAKING CASH ASK YOURSELF THE FOLLOWING...

- ☐ Is someone on the phone with me **right now**?
- ☐ Has **someone** remotely accessed my computer?
- ☐ **Am I being instructed** to take out cash to purchase Bitcoin, crypotocurrency or gift cards?
- ☐ Have I **met** the person to whom I am sending the funds?
- ☐ Did I receive this request **per an email**? If yes, did I verify the request over the phone by a *known phone number?*
- ☐ Is someone **pressuring or threatening me** to send funds immediately?
- ☐ Is this wire transfer to **benefit a government agency**?

WIRE TRANSFER PROCESS

- Wire transfers can only be initiated in-person by current First National Bank customers. We do not accept wire transfers by phone, fax or email.
- Only collected funds will be used to send a wire transfer.
- The customer's signature is required at the time of transfer.
- Wire transfers are sent Monday-Friday, until 2:30 p.m.
- The fee for outgoing domestic wire transfer is $35.00 plus tax ($37.45).
- The following information is required to initiate a wire transfer: amount; ABA/routing number of receiving bank; and the name, physical address (no PO Boxes); and account number of the receiving party.

SAFETY TIPS: AVOID BEING SCAMMED

- **Don't wire money, send cash, or use gift cards or cryptocurrency to pay someone who says they're with the government.** Scammers ask you to pay these ways because it's hard to track that money, and almost impossible to get it back.
- **Don't give your financial or other personal information to someone who calls, texts, or emails and says they're with the government.** Hang up the phone and call the government agency directly at a number you know is correct.
- **Don't trust your caller ID.** Caller ID can be faked; it could be anyone calling from anywhere in the world.
- **Don't click on links in unexpected emails or texts.**
- **Don't click on the link in a pop up or call the phone number.** Scammers will pretend to be from a real company —like Microsoft or Apple. Never let anyone remotely access your computer unless you're 100 percent sure you're working with the correct company.

STOP | THINK | CONNECT

- **STOP.** Before taking any final action, which may not be reversible, give yourself 24 hours to consider the risks and spot any problems.
- **THINK.** The red flags are often all around you and designed to confuse you. Allow yourself the time and physical space to clear your head and take an honest assessment of the situation.
- **CONNECT.** Pick up your phone and call a trusted friend or family member to get a second opinion.