FIRST BANK

Fraud Spotter Checklist

Safety starts with smarts. Don't fall for the wolf in sheep's clothing.

- ☐ Y ☐ N Is the call, email, or text unexpected?
- ☐ Y ☐ N Is it from an unfamiliar number, person, email, or company?
- ☐ Y ☐ N Are they claiming you owe them money or are being fined?
- ☐ Y ☐ N Are you being asked for your PIN, password, credit card number, or other sensitive info?
- ☐ Y ☐ N Are you being pressured to act quickly or threatened if you do not?
- ☐ Y ☐ N Is it an offer or prize that seems almost too good to be true?
- ☐ Y ☐ N Do they tell you not to contact your bank, your family members, or anyone else?
- ☐ Y ☐ N Does the message have misspelled words or strange-looking links?
- ☐ Y ☐ N Have you only met this person, and now they need money to help a family member or friend with an emergency?
- ☐ Y ☐ N Are they asking you to send payment through money, in the form of gift cards, or with cryptocurrency?
- ☐ Y ☐ N Is this an unexpected invoice, IT request, wire, or payroll change? (This is especially for business owners.)

If you answered yes to any of the above, **it may be a scam**. Reach out to your local First Bank branch or email **fraud@localfirstbank.com** before you continue the conversation or provide any information.

Can you spot the scam?

Here are just 3 scenarios, but it pays to stop, think, and keep your information secure.

Scenario 1 Does the Fraud Wolf have your number?

Your phone rings and the caller claims to be with First Bank customer support. He warns there may be fraud on your account and asks for a one-time passcode to confirm your identity.

Solution:
Never share important data with an unknown caller. Scammers may use your information or passcode to access your bank account, local you out, or add your card to their digital wallet. Scammers may use your information or passcode to access your bank account, lock you out, or add your card to their digital wallet.

Scenario 2 Is your business safe from fraud?

A vendor you often work with reaches out from an unfamiliar phone number. They mention that they need to update your payment info in their system to process the invoice for your last order.

Solution:
When in doubt, don't risk it — hang up and call your vendor directly! Even if the call seems legitimate, indicators like Caller ID are easy to spoof. Taking an extra moment to stop a potential scam is worth it. Your First Bank team is always here to help.

Scenario 3 A faster way to pay — or a fraudulent one?

While browsing online for new clothes, you find a store with products you love. The catch? They only accept payment through a cryptocurrency app.

Solution:
Slow down and trust your instincts. Scammers love crypto and instant payment apps that make it difficult to get your money back. Remember, First Bank debit and credit cards offer built-in fraud protection while shopping online.