FRAUD RESPONSE CHECKLIST

Simple steps to protect your money and your accounts!

Fraud attempts are increasing, and they are getting more convincing. Knowing what to watch for and how to respond quickly can help limit losses.

Step 1: Use Bank First Fraud Protection Tools

Bank First offers:

- ☐ Secure Online and Mobile Banking access, allowing you to check your accounts frequently
- ☐ Real-time debit card alerts
- ☐ Card controls within Digital Banking
- ☐ Business customers should utilize fraud prevention tools, such as Positive Pay and dual controls

Step 2: Recognize the Warning Signs

Be alert if you receive:

- ☐ Calls, texts, or emails asking for account numbers, login credentials, or one-time passcodes
- ☐ Messages that create urgency or fear ("This is the fraud department," "Your account will be locked," "Suspicious activity detected")
- ☐ Requests to click a link, scan a QR code, or download an attachment
- ☐ Random or unexpected messages that appear to be from Bank First that you have not initiated

Step 3: Stop and Do Not Engage

If something feels off, STOP, and:

- ☐ Do not reply to the message or caller
- ☐ Do not click links, open attachments, or scan QR codes
- ☐ Do not share account information, passwords, or codes
- ☐ End the call immediately if pressured

Fraudsters rely on speed. Do not respond.

Important: Bank First will never call, text, or email you unexpectedly to ask for your digital banking credentials or verification code. Additionally, if you receive a call from someone claiming to represent the Fraud Department, hang up and contact your local branch.

Step 4: Contact Bank First Immediately

If you're suspicious:

- ☐ Contact your local Bank First office immediately
- ☐ Log in to Online or Mobile Banking to review recent transactions
- ☐ Freeze your debit or credit card, if needed, by calling the number on the back of your card or:
  - To report a lost or stolen **Debit/ATM Card, call 1-800-554-8969.**
  - To report a lost or stolen **Credit Card, call 1-855-325-0905.**

The sooner we know, the faster we can help limit potential losses.

Step 5: Secure Your Accounts

After reporting suspicious activity:

- ☐ Change passwords for affected accounts
- ☐ Enable alerts and transaction notifications
- ☐ Monitor your accounts closely for additional activity
- ☐ Review linked services such as payment apps or subscriptions

If you are ever unsure, contact Bank First directly. Acting quickly can make a significant difference.

BankFirst

www.bankfirst.com

MEMBER FDIC | EQUAL HOUSING LENDER