

## FRAUD ALERT: HOW TO AVOID ACCOUNT TAKEOVER FRAUD

### What is an “account takeover”?

An account takeover happens when a fraudster poses as a financial institution to get your personal or account information. Once the fraudster has access to your account, they can make unauthorized transactions.

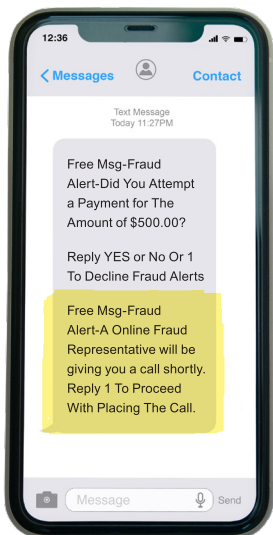


### How Does It Work?

An account takeover begins with a fraudster sending a text message to your mobile phone. They usually claim they're from Frontier State Bank's fraud department. They ask you to confirm a suspicious payment that was sent from your account — this may not be true and could be part of the fraud.




If this is a fraud attack, the fraudster typically follows up with a phone call and asks for your personal information to “cancel the payment.” NOTE: Frontier State Bank will NEVER ask for your personal information over the phone.

The account takeover fraud usually begins on a Friday, after business hours, and runs through the weekend.



The phone (above) shows an example of a fraudulent “account takeover” text message.

### How Can You Prevent Account Takeover Fraud?

-  If someone posing as Frontier State Bank contacts you by phone, email, or text message and wants you to share your personal information, consider it fraud.
-  If you receive a text (or email) like the one shown here, stating a representative will call you or to press a button to place a call, DO NOT reply to the sender. Ignore the message and do not call any phone numbers listed in the text.
-  If you receive a phone call that seems to be a phishing attempt, end the call immediately. And be aware that area codes can be misleading: a local area code does not always guarantee that the caller is local.

**If you feel you have been the victim of fraud, please contact Frontier State Bank immediately at 405-672-7831.**

**AVOID FRAUD: Do not share your personal information with anyone posing as our institution.**

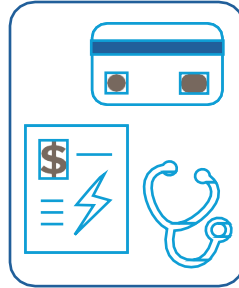
# How to Spot, Avoid, and Report Identity Theft

## What is identity theft?

Identity theft happens when someone uses your personal or financial information without your permission.

They might steal your

- Name and address,
- Credit card or bank account numbers,
- Social Security number,
- Medical insurance account numbers.



They might use them to

- Buy things with your credit cards,
- Get new credit cards in your name,
- Open utilities in your name,
- Steal your tax refund,
- Use your health insurance to get medical care,
- Pretend to be you if they're arrested.

## How will I know if someone steals my identity?



- **Read your bills.** Do you see charges for things you didn't buy?
- **Watch your bank account statement.** Are there withdrawals you didn't make? Are there changes you didn't expect?
- **Check your mail.** Did you stop getting a bill? Did you get a bill for an account you never opened? Or did you get a letter about an employer you don't recognize?
- **Get your credit report.** Are there accounts or other information you don't recognize? To get your report, call Annual Credit Report at **877-322-8228**, or go to **AnnualCreditReport.com**. Federal law gives you the right to get a free copy of your credit report every 12 months from each of the three nationwide credit bureaus. (The three bureaus also now let you check your credit report once a week for free at **AnnualCreditReport.com**).

## How do I protect myself from identity theft?



- **Protect documents that have personal information.** Keep official documents like your birth certificate, Social Security card, and account statements in a safe place. Shred any documents that reveal your personal information before you throw them away. Report lost or stolen checks immediately.
- **Don't share your Social Security number with someone who contacts you unexpectedly.** Even if they say they're from the Social Security Administration, the IRS, your bank, or another organization you know. They're not. It's a scam.
- **Protect your information online and on your phone.** Use passwords that are hard to guess. And add multi-factor authentication, like a code you get by text message, for accounts that offer it. Never share your online banking credentials.
- **Protect your ATM PIN.** Closely guard your ATM Personal Identification Number (PIN).
- **Review your bills.** Look for charges for things you didn't buy, or an unexpected bill.

The unauthorized use of someone's identity is a serious matter to **FRONTIER STATE BANK**.  
If you suspect you may be a victim of identity theft or account fraud, please contact our  
Customer Service department immediately at 405-672-7831.