Newsletter Vol. 15 Winter 2020

State National Bank
Big Spring | Lamesa | O'Donnell

PO BOX 1271, Big Spring TX 79721-1271
(432) 264-2100
Telephone Banking/Lost and Stolen Cards
(866) 220-9423
www.statenational.bank
Member FDIC

Learning more about scams and how to protect yourself

Guard Against Identity Theft

Legitimate Debt Collector or Scammer?

When an account like a credit card, auto loan, or cell phone bill becomes past due, the original creditor may attempt to collect the amount owed. The creditor may also hire a debt collector or sell the debt to someone who may try to collect the debt. While there are many legitimate debt collectors, there are also scammers who may try to get you to pay on debts that you don't owe or on debts that don't even exist. Get the name of the collector, the collection company, its address, and phone number.

Warning Signs of Debt Collection Scams

- **The debt collector refuses to give you "validation" information about the debt.** If the debt collector does not provide this information during the initial contact with you, they are required within 5 days of first contacting you to "validate" or tell you the amount of the debt, the name of the current creditor, and how to get the name of the original creditor.
- **They pressure you to pay by money transfer or prepaid card.** Scammers like these payment methods because they may be untraceable, and it can be hard for you to get your money back.
- **They falsely threaten you with jail time or pose as a government official.** Be aware that if you do owe criminal fines or restitution, it is possible that failure to pay may result in your arrest.
- **They say they will tell your family, friends, and employer.** They can only ask others about your whereabouts to try and contact you.
- **They ask you for sensitive personal financial information such as your bank account, routing numbers, or Social Security number.**
- **They call you at inconvenient times.** Legitimate debt collectors can't call you before 8 a.m. or after 9 p.m.

Before You Pay

Make sure you have been given information or have received the written notice about the debt before you pay anything.

Check with the original creditor. Is the debt yours? If so, is it their collector? If you think you don't owe some – or all – of the debt, dispute it with the collector by mail or online.

When scammers threaten to arrest you, suspend your driver's license, or call your employer if you don't pay immediately, hang up and report the collector to the FTC at **ftc.gov/complaint**.

What is the "waiting package" phishing scam?

The number of people who shop online has increased during the pandemic and fraudsters are more than happy to use this time to steal your personally identifiable information (PII) and money.

The Federal Trade Commission is warning of another new phishing scam. If you get a text message about a package you don't remember ordering, be careful. It could be a "waiting package" scam.

The FTC says criminals are sending unsolicited text messages that contain some variations of this message: "We came across a parcel from March pending for you. Kindly claim ownership and schedule for deliver here." Just like in phishing emails, they include an embedded link that might install malware on your device or direct you to a site created by the scammers who may trick you into giving personal information — letting scammers steal your passwords, account numbers, or Social Security number.

What should I do if I get a text about a package I don't remember ordering?

The FTC recommends you handle a "waiting package" scam the same way you would any other phishing scam. "If you get an unexpected text message about a package, **don't click on any links**," writes the FTC. "If you think the message could be legit, contact the company using a website or phone number you know is real. But don't use the information in the text message."

Of the more than **3.2-million fraud cases** reported to the Federal Trade Commission (FTC) in 2019, **identity theft accounted for 20.33%** of cases and was the most-common type of fraud.

Scammers Favorite Payment Method

First, there's **money wiring**. Somebody might call you, maybe about a prize you won, a loved one in trouble, or because you supposedly owe taxes or some kind of fee. The story sounds real and maybe even alarming. The person on the phone rushes you to Western Union or MoneyGram to send the money. But wiring money is like sending cash. You almost never get it back, and scammers know that.

Another favorite of scammers are **gift cards** or **cash reload cards**. Here's how it works: those same people call, and, again, there's a prize, a family emergency, or some fee they want you to pay. They tell you to go to the store and put money on a gift card, like an iTunes card or a cash reload card, like MoneyPak, Vanilla Reload, or Reloadit. Sometimes they'll even stay on the phone with you while you go to the store. Once your money is loaded onto the card, they'll ask for the card's registration numbers. That lets them get the money right away, and you're left with nothing.

Making Donations Through Social Media or Crowdfunding

Research any charity before you give. Also, if tax deductions are important to you, remember that donations to individuals are not tax deductible.

The safest way to give on social media or through crowdfunding is to donate to people you know who contact you about a specific project. Don't assume solicitations on social media or crowdfunding sites are legitimate, or that hyperlinks are accurate — even in posts that are shared or liked by your friends. Do your own research. Call your friends or contact them offline to ask them about the post they shared.

If you are concerned, the best starting point is to check to see if the charity is rated by Charity Navigator and then contact the organization directly to learn more.

Federal law allows you to get a **free** copy of your credit report, at your request, every 12 months from each credit reporting company.

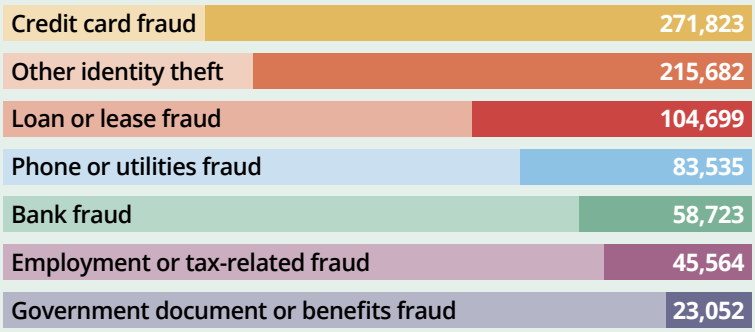
www.AnnualCreditReport.com
877.322.8228

"Overpayment" Scammers Target Small Business Owners

Keep an eye out for "overpayment" scams. A new supplier sends you a check payment for more than you charged. Scammers will ask for the difference back. By the time your bank realizes the check is fake, the scammer has your money. Make sure the name and business address check out.

Scammers are very creative so there are many variations of an overpayment scam. Another example is – a scam artist may tell a wedding photographer that the cashier's check was supposed to be for the travel agent and that unless they wire the difference, the newlyweds won't be able to go on their honeymoon. These requests will often be accompanied by stories designed to evoke sympathy. Don't fall victim to their con!

Most Reported Types of Identity Theft



Data source: *Federal Trade Commission (2020)*

Get a Recovery Plan

Did someone use your personal information to open up a new mobile account or credit card? Or maybe buy stuff with one of your existing accounts? Or did they file for unemployment or taxes in your name? That's identity theft. And you are not alone. According to the FTC's "Consumer Sentinel Network Data Book," the most common categories for fraud complaints last year were identity theft, imposter scams, and telephone & mobile services. Credit card fraud was most prevalent in identity theft cases where people reported that a fraudulent credit card account was opened with their information.

If any of this happened to you, the FTC wants to help you stop the damage and start recovering. First, call your credit card company right away. Then go to identitytheft.gov to find out what you need to do next. First you'll be asked questions about what happened and give information about the crime, along with your name and address. Based on your information, you will get a recovery plan to help you fix the problems caused by your identity theft. Go to **www.identitytheft.gov** to report your identity theft and get a recovery plan.