March 3 - March 9, 2024

National Consumer Protection Week (NCPW) is a time to help people understand their consumer rights and avoid frauds and scams.

Fidelity State Bank offers a free brochure on the Top 20 Scams

Stop in at one of our locations to pick up a copy or visit the website under the additional services menu. To view the website page now you can copy and paste this URL into your browser.

https://www.fidelitytopeka.com/additional-services/avoiding-fraud-common-scams/

5 Ways to Help Protect Your Identity

1. Read your credit card statements carefully and often.
2. Know your payment due dates. If a bill doesn't show up when you expect it, look into it.
3. Read the statements from your health insurance plan. Make sure the payments match the care you received.
4. Shred any documents with personal and financial information on them.
5. Review each of your credit reports as least once a year. It's free at annualcreditreport.com

View the video on 5 ways to help protect your identity.

Or copy and paste this URL to view the video
https://vimeo.com/352067376

What To Know About Credit Freezes and Fraud Alerts

Credit freezes and fraud alerts can protect you from identity theft or prevent further misuse of your personal information if it was stolen. Learn what they do and how to place them.

Credit Freezes

Who can place one: Anyone can freeze their credit report, even if their identity has not been stolen.

What it does: A credit freeze restricts access to your credit report, which means you — or others — won't be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you're applying for new credit. When the freeze is in place, you will still be able to do things like apply for a job, rent an apartment, or buy insurance without lifting or removing it.

Duration: A credit freeze lasts until you remove it.

Cost: Free

How to place: Contact each of the three credit bureaus — Equifax, Experian, and TransUnion.

Fraud Alerts

Fraud alerts are available in different situations and have different benefits.

Who can place one: Anyone who suspects fraud can place a fraud alert on their credit report.

What it does: A fraud alert will make it harder for someone to open a new credit account in your name. A business must verify your identity before it issues new credit in your name.

When you place a fraud alert on your credit report, you can get a free copy of your credit report from each of the three credit bureaus.
Duration: A fraud alert lasts one year. After a year, you can renew it.

Cost: Free

How to place: Contact any one of the three credit bureaus — Equifax, Experian, and TransUnion. You don't have to contact all three. The credit bureau you contact must tell the other two to place a fraud alert on your credit report.

Extended fraud alert

Who can place one: An extended fraud alert is only available to people who have had their identity stolen and completed an FTC identity theft report at IdentityTheft.gov or filed a police report.

What it does: Like a fraud alert, an extended fraud alert will make it harder for someone to open a new credit account in your name. A business must contact you before it issues new credit in your name.
When you place an extended fraud alert on your credit report, you can get a free copy of your credit report from each of the three credit bureaus twice within one year from when you place the alert, which means you could review your credit report six times in a year.
In addition, the credit bureaus will take you off their marketing lists for **unsolicited credit and insurance offers** for five years, unless you ask them not to.

Duration: An extended fraud alert lasts seven years.

Cost: Free

How to place: Contact any one of the **three credit bureaus** — Equifax, Experian, and TransUnion. You don't have to contact all three. The credit bureau you contact must tell the other two to place an extended fraud alert on your credit report.

Warning Signs of Identity Theft

What Do Thieves Do With Your Information?

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

Clues That Someone Has Stolen Your Information

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.

If your wallet, Social Security number, or other personal information is lost or stolen, there are steps you can take to help protect yourself from identity theft.

Recovering from Identity Theft

IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

IdentityTheft.gov

Review your bank statements and your accounts for any unrecognized charges.

Services available to help safeguard your account.

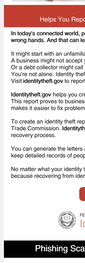
Utilize **e-statements*** to avoid having paper bank statements stolen from your mailbox.

Monitor your account with Online Banking -24 hour access to monitor transactions coming in and going out of your account.

If you have questions about e-Statements or how to sign up forOnline Banking give us a call. 785-295-2100

With **online banking** you can also access your account from your cell phone using our secure mobile app anytime and anywhere there is cell coverage.

*e-Statements require the use of online banking.



IdentityTheft.gov
Helps You Report and Recover from Identity Theft

In today's connected world, personal information sometimes falls into the wrong hands. And that can lead to identity theft.

It might start with an unfamiliar charge on your credit card.
A business might not accept your check.
Or a debt collector might call you about a bill that isn't yours.
You're not alone. Identity theft can happen to anyone. Stay calm.
Visit **identitytheft.gov** to report it and get a personal recovery plan.

Identitytheft.gov helps you create an identity theft report.
This report proves to businesses that someone stole your identity and it makes it easier to fix problems caused by identity theft.

To create an identity theft report, you file a complaint with the Federal Trade Commission. **Identitytheft.gov** guides you through each step of the recovery process.

You can generate the letters and forms you need. Track your progress. And keep detailed records of people you've talked to.

No matter what your identity theft situation is, **identitytheft.gov** can help because recovering from identity theft is easier with a plan.

watch the video

FEDERAL TRADE COMMISSION
IdentityTheft.gov

Phishing Scams and How to Spot Them

E-Mail Scams:

Phishing is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source – an internet service provider, a bank, or a mortgage company, for example. *It asks the consumer to provide personal identifying information.*

Then a scammer uses the information to open new account or invade the consumer's existing accounts.

There are several tips that consumers can follow to avoid phishing scams, such as *not responding* to e-mails or pop-up messages that ask for personal or financial information.

Fidelity State Bank also recommends not clicking on links and not opening attachments from someone you do not know.

Text Scams:

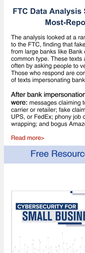
FTC Data Analysis Shows Bank Impersonation is the Most-Reported Text Message Scam

The analysis looked at a random sample of 1,000 text messages reported to the FTC, finding that fake bank security messages, often supposedly from large banks like Bank of America and Wells Fargo, were the most common type. These texts are designed to create a sense of urgency, often by asking people to verify a large transaction they did not make. Those who respond are connected to a fake bank representative. Reports of texts impersonating banks have increased nearly twentyfold since 2019.

After bank impersonation, the most frequently reported text scams were: messages claiming to offer a free gift, often from a cell phone carrier or retailer; fake claims of package delivery issues from the USPS, UPS, or FedEx; phony job offers for things like mystery shopping and car wrapping; and bogus Amazon security alerts.

Read more>

Free Resources for Your Small Business

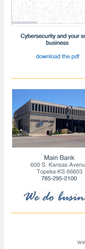


Cybersecurity and your small business

download the pdf

Scams and your small business

download the pdf
or ask a loan officer for the booklet



Main Bank
600 S. Kansas Avenue
Topeka KS 66603
785-295-2100

Westridge Location
5926 SW 21st Street
Topeka KS 66604
785-228-8440

We do business Right here at home

www.fidelitytopeka.com

FDIC