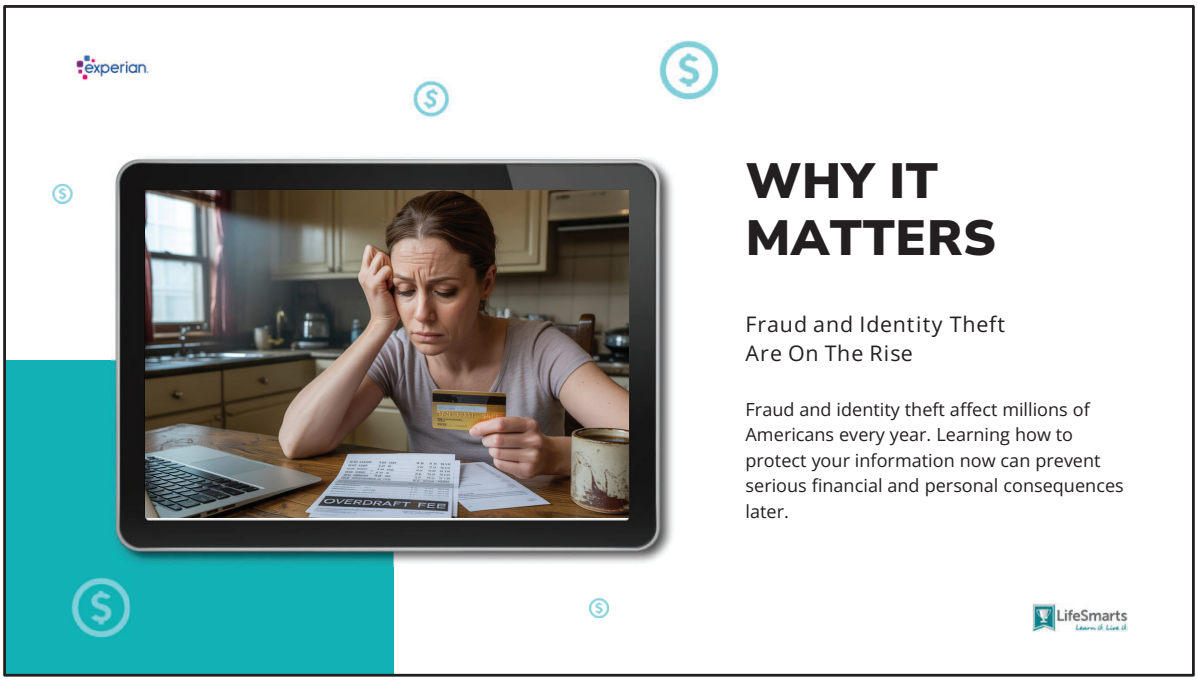
Welcome!

Today we're diving into fraud and identity theft, issues that might sound like they only affect adults, but they're a real risk for teens too.

We'll look at how to protect your personal information online, how fraud alerts work, and what steps you or your family can take if something goes wrong.

This lesson was created by LifeSmarts, the program that helps students learn real-world skills, and it's made possible with support from Experian, leaders in credit and identity protection.



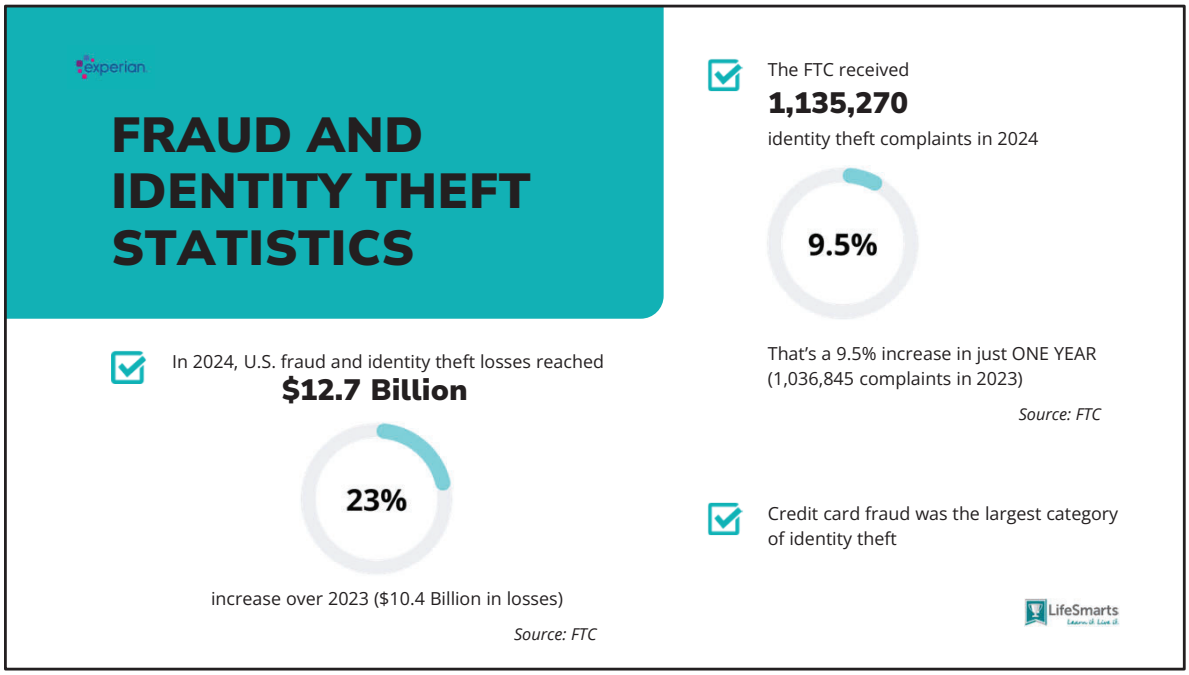
Before we jump into the details, let’s stop and think about why this lesson matters.

Fraud and identity theft aren’t just problems for adults... they affect people of all ages, including teens.

Losing control of your personal information can damage your finances, your credit, and even your sense of security.

That’s why it’s important to understand how these crimes work and what steps you can take to protect yourself.

Now let's look at some real numbers from Experian that show just how big of a problem this has become.

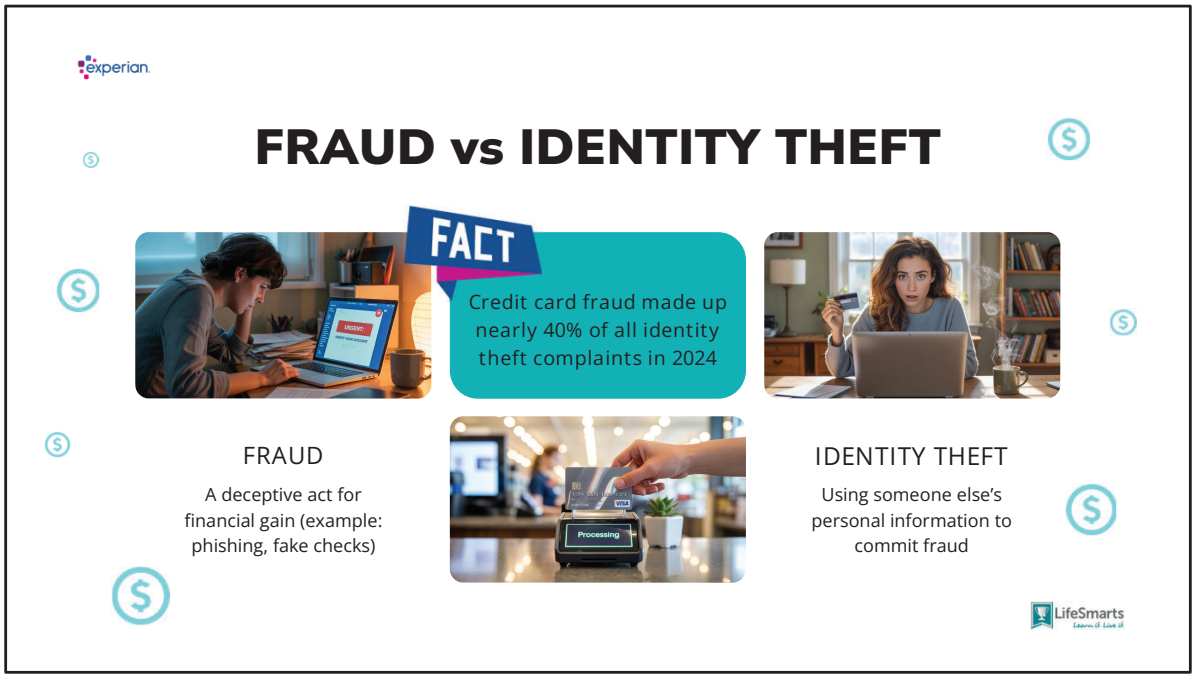


Here's what the numbers tell us. In 2024, fraud and identity theft losses in the U.S. reached $12.7 billion. That's a 23% jump in just one year, up from $10.4 billion in 2023.

The Federal Trade Commission also received more than 1.1 million identity theft complaints in 2024 — a 9.5% increase over the year before. That means more people than ever are reporting that their identities have been misused.

The #1 type of identity theft in 2024 was credit card fraud — thieves opening fake accounts or breaking into real ones.

These numbers make it clear: fraud and identity theft are not rare, isolated issues. They're happening more often, with bigger losses, and affecting millions of people across the country.



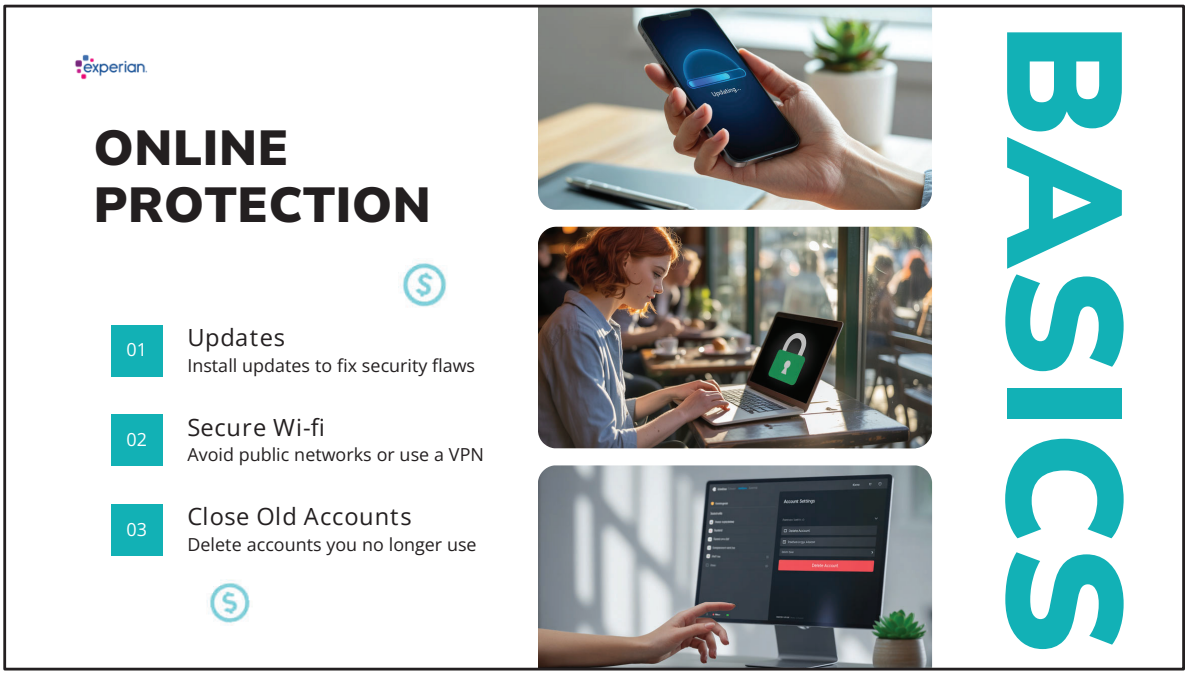
Fraud and identity theft are connected, but not the same thing.

Fraud is any kind of trick to steal money or valuables — like sending fake texts or running a scam.

Identity theft is when someone uses your personal information — your Social Security number, bank info, or credit card — to commit that fraud.

And here's a striking number: in 2024, nearly 40% of all identity theft complaints were about credit card fraud.

That means criminals were either opening new cards in someone else's name or taking over existing accounts.



Protecting yourself online doesn't have to be complicated.

First, keep your devices updated. Those software updates often patch security holes that hackers try to exploit.

Second, use secure Wi-Fi. Public networks in coffee shops or airports are risky unless you're using a VPN.

And finally, close old accounts. If you don't use them, they're just sitting out there as extra doors for criminals to try.

These three simple steps can drastically cut down your chances of becoming a victim of online fraud or identity theft.

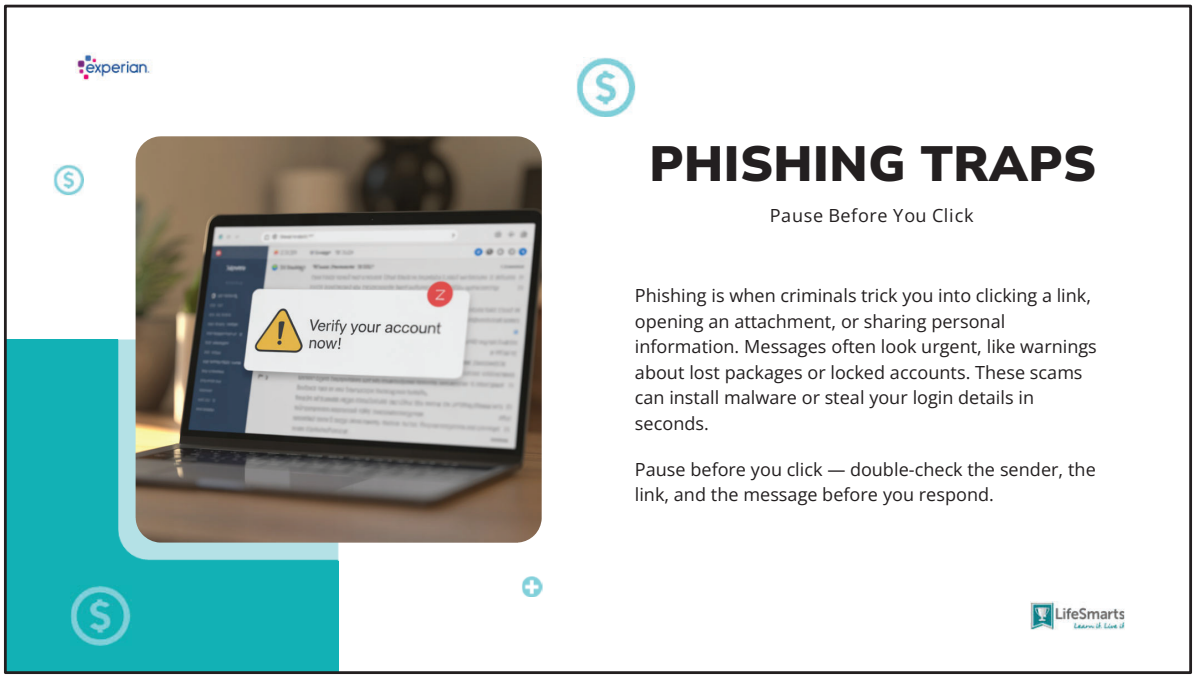
Passwords are the first line of defense, but not all passwords are created equal.

Longer is stronger... at least 15 characters with a mix of letters, numbers, and symbols.

A password manager makes this easier by creating strong, unique passwords and remembering them for you.

And now, we're starting to see passkeys. Instead of typing a password, you use your phone's fingerprint, face ID, or a PIN to verify it's really you.

Passkeys are harder for criminals to steal and can't be phished the way passwords can.



Phishing is one of the most common fraud tactics today.

The goal is to create a sense of panic so you click without thinking... like telling you a delivery will be lost or that your bank account is frozen.

The second you click, you could be downloading malware or handing over your login credentials.

The key is to pause before you click. Ask yourself:

Do I know the sender?

Does the link look suspicious?

And if in doubt, don’t click... go directly to the company’s official website instead.

Sometimes what feels like harmless sharing can actually give away key details.

Posting your birthdate or personal info online might seem fun, but criminals can use those facts to guess passwords or reset accounts.

Sharing travel plans can also backfire. If you post that you're away, you're telling others when your home is empty.

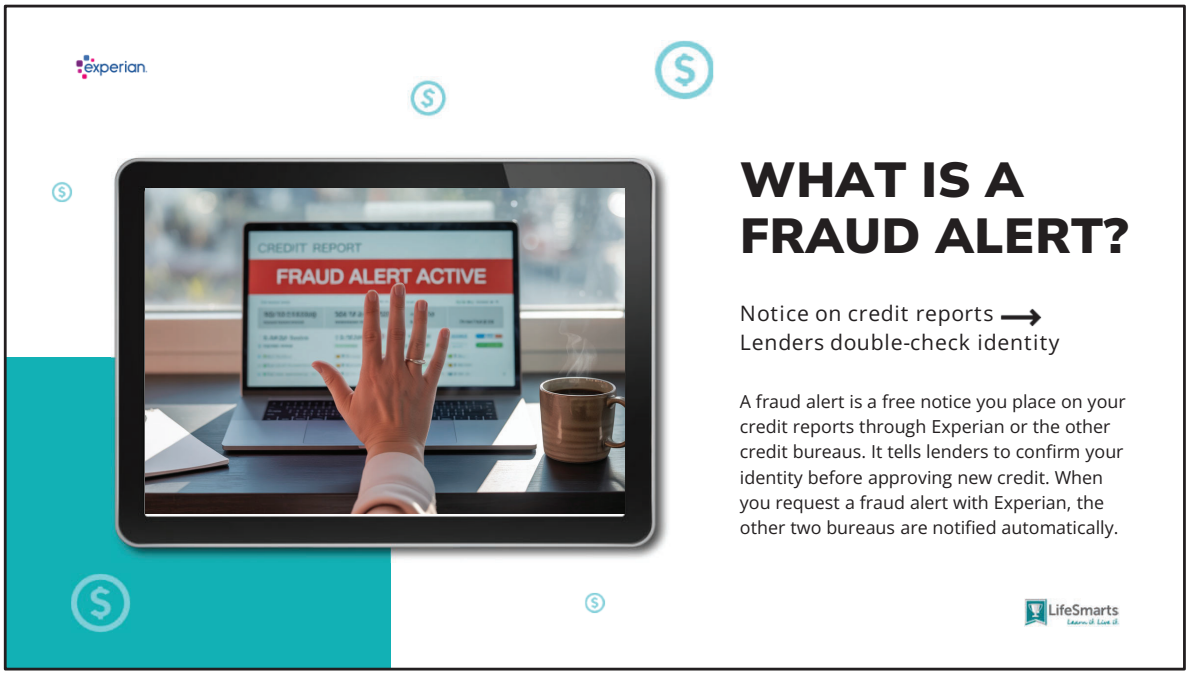
And finally, check your privacy settings. If your profile is wide open, anyone, including scammers, can see what you're posting.

We've talked about prevention, but sometimes things still go wrong... a company you use gets hacked, your wallet goes missing, or your Social Security number gets exposed.

That's when it's time to add an extra layer of protection.

By placing a fraud alert, you're warning banks and credit card companies: 'Double-check this person's identity before approving any new accounts.'

It's free, simple, and one of the fastest ways to stop criminals from causing lasting damage.

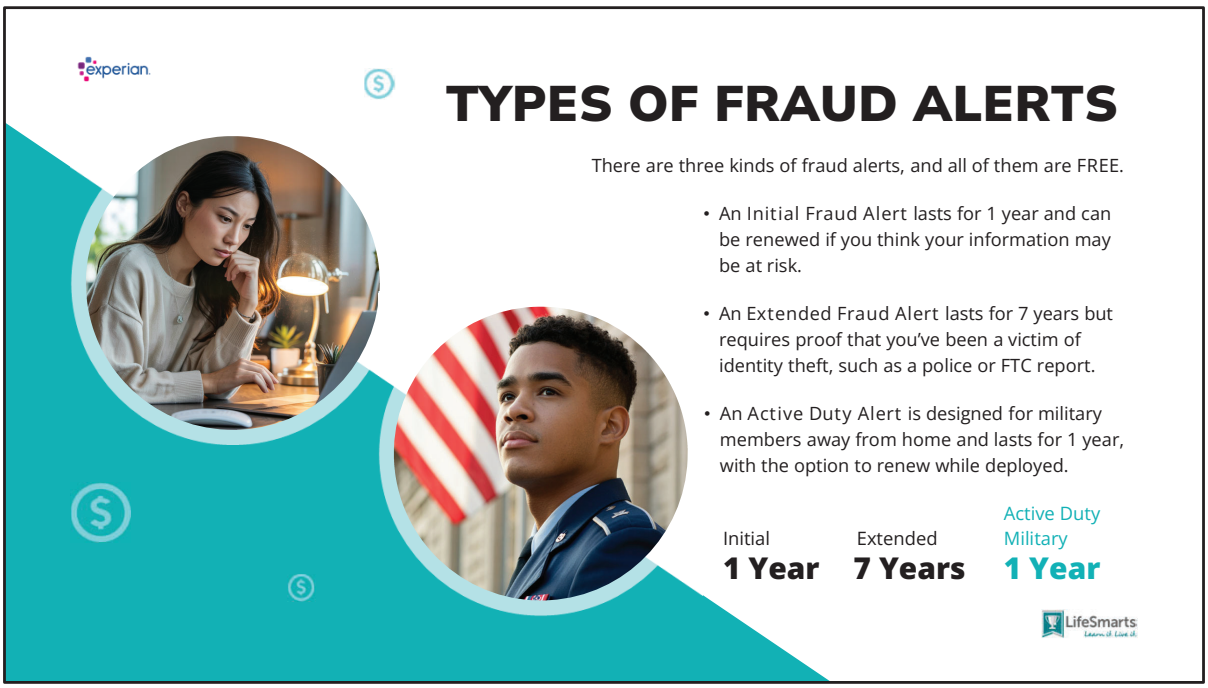


A fraud alert is a safety flag on your credit reports.

You can place one through Experian, and they'll make sure the other two bureaus — Equifax and TransUnion — get the same notice.

That way, any time a lender sees your credit file, they know to double-check that it's really you.

The alert doesn't block you from using credit, but it makes it much harder for criminals to succeed.



Fraud alerts aren't one-size-fits-all.

An Initial Alert is what most people start with. It lasts a year and can be renewed as often as needed.

An Extended Alert is much stronger: it lasts seven years, but you'll need to show proof you've already been a victim, like a police or FTC report.

The third type is for the military: an Active Duty Alert, which lasts a year and can be renewed while you're deployed.

The key takeaway is that there's an option for different situations... whether you're being cautious, recovering from identity theft, or protecting your credit while serving.

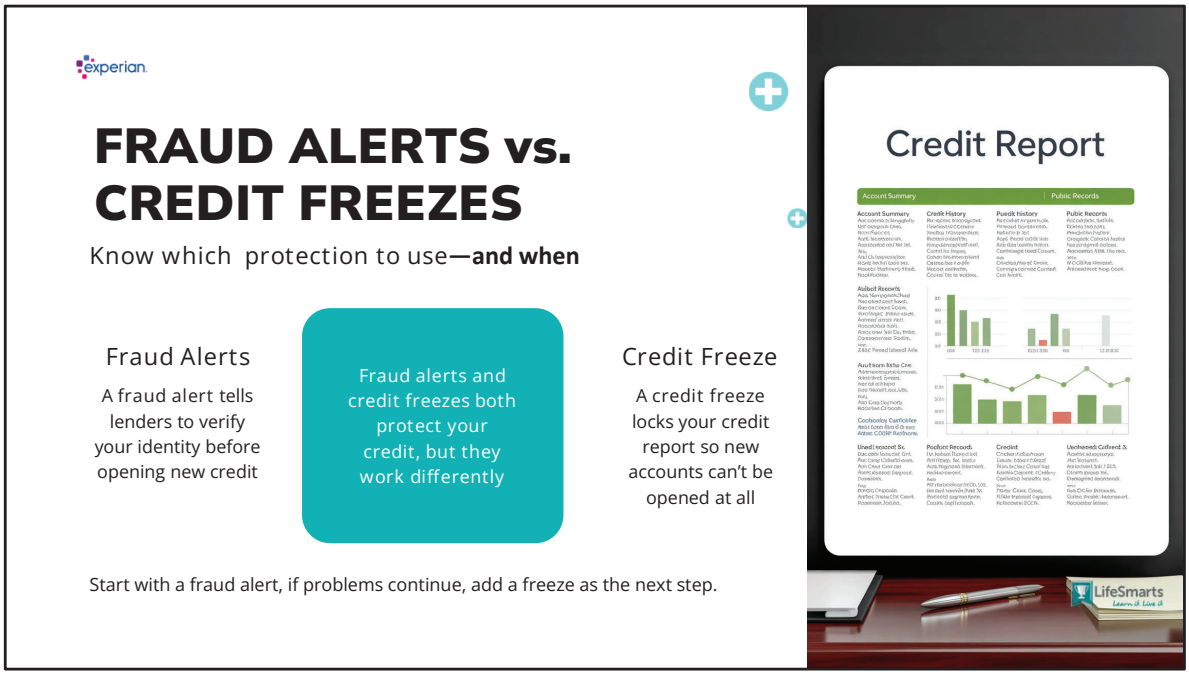
Here's the good news: anyone can place a fraud alert. You don't have to wait until fraud happens. Many people add one as a precaution if their information might have been exposed, like in a data breach.

Setting up a fraud alert is straightforward. The fastest way is online through Experian's Fraud Alert Center, but you can also do it by phone or by mail. All you need is basic information: your name, Social Security number, and address. Once you place the request, Experian shares it with the other two credit bureaus so the alert shows up on all three reports.

An initial fraud alert lasts for 1 year, and during that time lenders will be required to take extra steps to confirm it's really you before opening any new accounts.

In most cases, a fraud alert provides the protection you need. But if fraud continues, a credit freeze can be your next step. Let's look at how those two compare.

Fraud alerts are always free, and you can renew or remove them at any time. It's a simple step that adds a powerful layer of protection.



Fraud alerts and credit freezes are both helpful, but they're used in different ways.

A **fraud alert** is usually the first step. It tells lenders to double-check your identity before approving new credit — and it doesn't stop you from using your existing credit cards or accounts.

A **credit freeze**, on the other hand, completely locks your credit report. That means no new accounts can be opened until you lift it. It's powerful, but if you activate it too soon, it can slow down other recovery steps, since no one can access your report — even those helping you resolve fraud.

Think of it as a two-step system: start with a fraud alert, and use a freeze later only if needed.

The best protection is a combination of good habits and smart tools.

Your daily actions... keeping devices updated, using strong passwords, and avoiding oversharing... reduce your risk.

But if something does go wrong, a fraud alert is a simple, free way to stop criminals in their tracks. And if issues continue or you need a stronger lock, a credit freeze can be your final step.

Together, these steps give you real protection and peace of mind.

Thank you for learning with us today... and thank you to Experian and LifeSmarts for making this lesson possible.