A Complimentary Guide

Version 2.0 | Updated: March 2026

Protecting Your Identity & Credit

Safeguard your finances against fraud and identity theft

First Oklahoma Bank

Member F.D.I.C.

WHAT THIS GUIDE COVERS

This guide helps you protect your money, credit, and identity from fraud and theft.

You'll learn how to:

- Freeze your credit to prevent identity theft.
- Respond immediately if fraud occurs.
- Monitor your financial accounts effectively.
- Protect your tax information from criminals.
- Get free credit reports and understand what to look for.

Part of the Smart Security Series

Other guides in this security series:

- Taking Control of Your Online Privacy
- Securing Your Home Wi-Fi & Devices

Each guide in our Smart Security Series stands alone and addresses a specific area of protection.

TABLE OF CONTENTS

If You Suspect Fraud Right Now

STEP 1: Secure Your Documents

- **Contact your bank and credit card companies immediately** using the phone number on the back of your card (not the number a potential scammer provided).
- **Change passwords** on affected accounts.
- **Enable two-factor authentication** if not already active.
    - Two-factor authentication (2FA) adds a second layer of security to your account by requiring a second verification step — such as a code from an authenticator app, SMS text, or hardware key — after entering your password.
    - To enable it, go to your account's Security Settings, find the 2FA or Two-Step Verification option, and follow the prompts to link your preferred verification method.

STEP 2: Place a Credit Freeze

A credit freeze stops criminals from opening new accounts in your name. Contact all four major credit bureaus:

- **TransUnion**: 1-800-916-8800 or www.transunion.com/credit-freeze
- **Experian**: 1-888-397-3742 or www.experian.com/freeze/center.html
- **Equifax**: 1-800-685-1111 or www.equifax.com/personal/credit-report-services/credit-freeze/
- **Innovis**: www.innovis.com/securityFreeze/index

Important: Freezing your credit is free and doesn't hurt your credit score. You can temporarily unlock it whenever needed.

If You Suspect Fraud Right Now *(continued)*

STEP 3: File Official Reports

1. **Report to the FTC**: Visit IdentityTheft.gov to create a personalized recovery plan with step-by-step guidance.
2. **File an FBI Internet Crime Complaint**: Visit IC3.gov if you're a victim of online fraud or cybercrime.
3. **File a police report** if needed for documentation (especially for insurance claims).

STEP 4: Monitor & Document

- **Keep detailed notes**: Document dates, times, names of people you spoke with, and reference numbers.
- **Save copies** of all letters, emails, and correspondence.
- **Monitor your credit reports** closely for the next 12 months.

For complete recovery guidance, visit IdentityTheft.gov - the official FTC recovery site with customized action plans.

Understanding a Credit Freeze

What is a Credit Freeze?

A credit freeze prevents anyone (including you) from opening new credit accounts until you unlock it. It's the single most effective way to prevent identity theft.

Common Questions About Credit Freezes

Will freezing my credit hurt my credit score?
No. A credit freeze has zero impact on your credit score.

Can I still use my existing credit cards?
Yes. A freeze only prevents NEW accounts from being opened. Your existing cards, loans, and accounts work normally.

Can I still check my credit report?
Yes. You can still get your free annual credit reports even with a freeze in place.

What if I need to apply for credit?
You can temporarily unlock your credit freeze online or by phone in minutes. Most bureaus let you unlock for a specific time (like 24 hours) or for a specific company.

Does it cost money?
No. Credit freezes are completely free by federal law.

Understanding a Credit Freeze (*continued*)

When Should I Freeze My Credit?

You should free your credit if:

- You want the strongest protection against identity theft (recommended for everyone).
- You've been notified of a data breach affecting your information.
- You're not planning to apply for credit in the near future.
- You've been a victim of identity theft or fraud.
- You want peace of mind knowing no one can open accounts in your name.

Freezing is preventive - you don't have to wait until fraud happens.

Many security experts recommend that everyone freeze their credit as a standard precaution.

How to Freeze Your Credit (Step-by-Step)

You must freeze your credit at all four major credit bureaus. Each one maintains separate records, so freezing one doesn't freeze the others.

The 4 Major Credit Bureaus	
TransUnion	www.transunion.com/credit-freeze
Experian	www.experian.com/freeze/center.html
Equifax	www.equifax.com/personal/credit-report-services/credit-freeze/
Innovis	www.innovis.com/securityFreeze/index

What You'll Need

- Your full name
- Social Security Number
- Date of birth
- Current address (and previous addresses from the last 2 years)
- Email address for confirmation

The Process

1. Visit each bureau's credit freeze website (see table above).
2. Create an account or log in if you already have one.
3. Follow the prompts to place the credit freeze.
4. Save your PIN or password (you'll need this to unlock the freeze later).
5. Repeat for all four bureaus (This process takes about 30 minutes total).

Here is a link to a step-by-step guide:
www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/

Additional Financial Protection Freezes

Beyond the four major credit bureaus, these specialized agencies also collect your information for specific types of financial decisions. Freeze them for complete protection.

Specialized Credit Bureaus

LexisNexis (Personal information and insurance risk scores)

- Freeze: consumer.risk.lexisnexis.com/freeze
- Consumer disclosure report request: consumer.risk.lexisnexis.com/request

CoreLogic/Teletrack (Alternative credit for subprime lending)

- consumers.teletrack.com/freeze

Clarity Services (Payday loans and check cashing)

- consumers.clarityservices.com/securityFreeze

Banking Protection

ChexSystems Freeze

This freeze prevents unauthorized checking or savings accounts from being opened in your name. It also stops banks from checking your banking history when you're not opening a new account.

www.chexsystems.com/security-freeze/place-freeze

Note: You can temporarily lift (unlock) any of these freezes when you legitimately want to open a new account, then reactivate them immediately after.

Protecting Your Tax Information

Federal Tax Protection (All States)

IRS Identity Protection PIN (IP PIN)

Criminals file fraudulent tax returns using stolen Social Security Numbers to claim refunds. An IP PIN prevents this.

What is an IP PIN?

This is a unique 6-digit number you receive each year from the IRS. You must include it when filing your federal tax return. Without it, the IRS will reject the return.

How to enroll:

1. Create an IRS Online Account at www.irs.gov.
2. Verify your identity (requires ID, tax return info, and phone or financial account).
3. Enroll in the IP PIN program.
4. Receive your new PIN each January.

Important: Never share your IP PIN with anyone except the IRS or your trusted tax preparer.

More information:

www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

Protecting Your Tax Information (*continued*)

State Tax Protection (Oklahoma Residents)

OkTAP (Oklahoma Taxpayer Access Point)

Create an OkTAP account. This will securely manage your Oklahoma state taxes online.

Through OkTAP, you can file returns, make payments, check refund status, and upload documents securely without mailing sensitive information.

oklahoma.gov/tax.html

Protecting Your Phone Number

Protecting your phone number with SIM locks at both the carrier and device level making it harder for criminals to hijack your accounts through SIMswap attacks.

Why Criminals Target Your SIM:

- Criminals try to take over your phone number so they can receive your text messages and calls, including one-time passcodes for banks, email, crypto, and social media.
- Often thieves will gather your personal details first (from breaches, phishing, or social media), then trick or pressure the carrier into moving your number to a SIM or eSIM they control.
- Once they control your number, they can reset passwords, drain bank or investment accounts, steal crypto, and lock you out of your own services.

How to Protect Yourself at the Carrier Level:

Carrier-level protections reduce the chance that a fraudster can move your number without your approval.

Here are three easy steps to guide you.

1. **Turn on your account or number lock.**
    - Many carriers now offer a “wireless account lock,” “number lock,” or similar setting that blocks SIM swaps, number transfers, and major changes unless you unlock it first in the app or website.
    - Log in to your carrier account (app or web), then go to security or account protection settings, and enable any option that explicitly mentions blocking SIM changes or port outs.

Protecting Your Phone Number (*continued*)

2. **Set strong account credentials with the carrier.**
    - Use a long, unique password for your carrier login and avoid reusing passwords from other sites.
    - If the carrier supports it, add a separate account PIN/passcode and ensure it is not easy to guess (no birthdays, addresses, or simple patterns).
3. **Lock down support interactions.**
    - Ask your carrier what extra verification they can require before changing SIMs or ports (e.g., in-person ID checks, special notes on the account).
    - Be skeptical of calls or texts claiming to be from your carrier asking for one-time codes or account PINs. Contact the carrier back using the number on their official website instead.

How to Protect Yourself at the Device Level:

Device-level protections stop someone from easily using your SIM or phone if they steal it.

1. **Enable SIM PIN on your phone.**
    - A SIM PIN makes the SIM ask for a code whenever the phone restarts or the SIM is moved to another device, helping prevent someone from using your SIM in a new phone.
    - On most phones you can find this under Settings → Security or Cellular/Mobile Data → SIM lock/SIM PIN. Turn it on, then change the default PIN to a code only you know.

Protecting Your Phone Number (*continued*)

2. **Use a strong screen lock.**
    - Always use at least a 6-digit PIN, strong password, or biometric (fingerprint/face) instead of simple patterns or 4-digit codes.
    - Turn on automatic lock after a short period of inactivity (for example, 30 seconds or 1 minute) to reduce the window where the phone is unlocked in someone else's hands.
3. **Secure the data on the phone itself.**
    - Keep full disk encryption and built-in "Find My"/remote wipe features enabled so you can erase the device if it is lost or stolen.
    - Regularly update your phone's operating system. This process makes sure you have the latest security fixes.

Why this Combination Matters:

- Carrier-level locks help stop remote SIMswap and port-out fraud, where attackers never touch your physical phone but convince the carrier to move your number.
- Device-level SIM PINs and screen locks protect you if the phone or SIM is physically stolen or briefly accessed (for example, at a public place or workplace).
- Using both greatly reduces the chances that criminals can intercept your one-time codes, reset passwords, and empty financial or crypto accounts tied to your number.

Stop Pre-Approved Credit Offers

Opt-Out Prescreen

Pre-approved credit card and insurance offers arrive because credit bureaus sell your information to lenders. These offers create two risks:

1. Mail theft - criminals can steal these offers from your mailbox and use them to open accounts.
2. Privacy - your information is being sold and shared without your direct consent.

How to opt out:

Visit www.optoutprescreen.com and choose:

- **5-year opt-out** (online, takes effect in 5 days).
- **Permanent opt-out** (requires mailing a signed form).

This service is free and legitimate - it's jointly operated by the major credit bureaus as required by law.

Get Your Free Credit Reports

By federal law, you're entitled to one free credit report from each bureau every 12 months.

Official site:

www.annualcreditreport.com

Warning:

Only use AnnualCreditReport.com - other sites may look similar but aren't the official source.

What to Look For:

When you review your credit report, check for:

- **Accounts you didn't open** - credit cards, loans, or lines of credit you don't recognize.
- **Credit inquiries you didn't authorize** – This shows you when companies have checked your credit.
- **Incorrect addresses** - addresses where you've never lived.
- **Wrong personal information** - misspelled names, incorrect Social Security Number.
- **Suspicious activity** - unfamiliar transactions or account changes.

If you find errors or fraud:

1. Dispute them directly with the credit bureau through their website.
2. Contact the company that reported the information.
3. File a report at IdentityTheft.gov if fraud is involved.
4. Keep copies of all correspondence.

Get Your Free Credit Reports (*continued*)

Pro Tip: Spread Out Your Reports

Instead of checking all three bureaus at once, request one report every four months from a different bureau:

- **January**: Request Experian report
- **May**: Request Equifax report
- **September**: Request TransUnion report

This gives you year-round credit monitoring for free.

Free Credit Monitoring

Credit Karma

Credit Karma is a free credit monitoring and score tracking monitoring service.

What you get:

- Credit scores from TransUnion and Equifax (updated weekly).
- Credit monitoring with alerts for new accounts or inquiries.
- Tips for improving your credit score.
- Free credit report information.

Sign up: www.creditkarma.com

How they make money: Credit Karma shows you targeted credit card and loan offers. You're never required to apply for anything.

Monthly Financial Checkup

Set a recurring calendar reminder to check these items each month:

Review Account Statements

- Bank statements
- Credit card statements
- Investment accounts
- Connected payment apps (Venmo, PayPal, Cash App)

What to look for: Charges you don't recognize, even small ones like one or five dollars. Criminals often test stolen cards with small purchases first.

Check Account Logins

Most banks and financial apps show recent login activity. Here’s what to look for:

- Unfamiliar devices
- Logins from strange locations
- Login times when you weren't using the account

Review Connected Apps

In your bank or credit card app, look for "Connected Apps," "Third-Party Access," or "Linked Services."

Remove apps you:

- Haven't used in 6+ months.
- Don't recognize.
- No longer need.

Monthly Financial Checkup (*continued*)

Take Immediate Action on Suspicious Activity

If you see something suspicious:

1. Report to your bank or credit card company immediately.
2. Change passwords on affected accounts.
3. Enable two-factor authentication if not already active.
4. File a complaint with the FTC at reportfraud.ftc.gov if fraud occurred.

Shred Sensitive Documents

Before disposing of any documents containing your personal information, shred them with a cross-cut shredder or tear them into small pieces.

What to Shred:

- Documents with your name and address listed together.
- Bank statements and canceled checks.
- Credit card statements and pre-approved offers.
- Documents with account numbers.
- Social Security Number or tax documents.
- Medical information.
- Any financial statements.
- Old bills with account information.

📌 **Tip**: A cross-cut shredder (which cuts paper into confetti) is more secure than a strip-cut shredder (which cuts into long strips).

Paid Identity Protection Services (Optional)

If you prefer comprehensive protection with minimal effort, these services handle monitoring, alerts, and data removal automatically.

Aura

Comprehensive identity, credit, and digital protection for individuals and families. Which averages around ten dollars a month.

What's included:

- Credit monitoring from all three major bureaus.
- Data broker removal (removes your info from people-finder sites).
- Home title monitoring (alerts if someone tries to sell your property).
- $1 million identity theft insurance.
- VPN for secure browsing.
- Password manager.
- Real-time fraud alerts.
- U.S.-based customer support.

Special rates: aurainc.sjv.io/Qj0AJM

DeleteMe

Automatically and continuously removes your personal information from data brokers and people-finder sites. Which averages around nine dollars a month.

What's included:

- Removal from 30+ major data broker sites.
- Quarterly removal reports.
- Ongoing monitoring and re-removal.
- Privacy dashboard.

joindeleteme.com

Key Resources & Phone Numbers

Emergency Identity Theft Help

- IdentityTheft.gov: www.identitytheft.gov
- FTC Report Fraud: reportfraud.ftc.gov
- FBI Internet Crime Complaint Center: www.ic3.gov

Credit Bureau Fraud Departments

- TransUnion: 1-800-916-8800
- Experian: 1-888-397-3742
- Equifax: 1-800-685-1111

Government Resources

- Federal Trade Commission (FTC): consumer.ftc.gov
- Consumer Financial Protection Bureau: www.consumerfinance.gov
- Social Security Fraud Hotline: 1-800-269-0271

Key Action Items to Get You Started

Start With These 3 Actions Today:

1. Freeze your credit at the four major credit bureaus (takes 30 minutes).
2. Check your bank and credit card statements for anything suspicious.
3. Sign up for free credit monitoring with Credit Karma.

This Week:

- Set up IRS Identity Protection PIN.
- Opt out of pre-approved credit offers.
- Place a ChexSystems freeze.
- Place SIM lock on your account or phone.
- Request one of your free annual credit reports.

This Month:

- Freeze the specialized credit bureaus (LexisNexis, CoreLogic, Clarity Services).
- Set up monthly account review reminders.
- Purchase a cross-cut shredder if you don't have one.

Takeaways

💡**Freezing your credit is the single most effective step you can take to prevent identity theft.** It's free, doesn't hurt your credit score, and you can unlock it anytime you need to apply for credit.

💡**You don't have to do everything at once.** Start with credit freezes and work through the other steps over the next few weeks.

💡**If fraud happens, act fast.** The sooner you report it and freeze your credit, the less damage criminals can do.

Other Guides in this Series

Taking Control of Your Online Privacy
Learn how to reduce your digital footprint by removing your information from data broker sites, adjusting privacy settings on Google, Facebook, Apple, and Amazon, and stopping unwanted marketing calls and emails.

Securing Your Home Wi-Fi & Devices
Protect your home network, smart devices, and personal technology with practical steps like securing your router, using strong passwords, enabling two-factor authentication, and recognizing phishing attempts.

Visit our Customer Security & Privacy page for all guides:
https://firstoklahomabank.com/fraud-prevention/

Questions?

Contact First Oklahoma Bank at 918-392-2500.