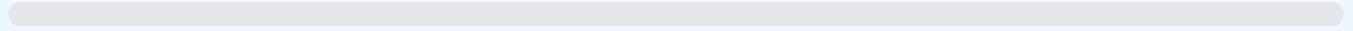


# Identity Protection Planner

Interactive tool for protecting your personal information and planning identity theft recovery

Protection Progress: 0%



## Personal Information Protection Checklist

- Store Social Security card securely** HIGH

Keep your Social Security card in a locked safe or safety deposit box, not in your wallet.

- Shred sensitive documents** HIGH

Use a cross-cut shredder for bank statements, medical bills, and pre-approved credit offers.

- Use strong, unique passwords** HIGH

Create different passwords for each account using a password manager.

- Enable two-factor authentication** HIGH

Add 2FA to all financial accounts, email, and social media.

- Review credit reports regularly** MEDIUM

Check all three credit bureaus at AnnualCreditReport.com at least once per year.

- Monitor bank and credit card statements** MEDIUM

Review statements monthly for unauthorized charges or suspicious activity.

- Secure home Wi-Fi network** MEDIUM

Use WPA3 encryption, change default router password, and hide network name.

- Opt out of pre-screened credit offers** LOW

Call 1-888-5-OPT-OUT to reduce mail theft risk and junk mail.

- Use informed delivery from USPS** LOW

Get email previews of incoming mail to detect missing items.

- Limit social media information sharing** MEDIUM

Avoid posting birth date, address, phone number, or vacation plans publicly.

## Credit Freeze / Fraud Alert Setup Guide

A credit freeze prevents new accounts from being opened in your name. It's free to place and lift.

### Equifax

1-800-685-1111

[equifax.com/freeze](http://equifax.com/freeze)

Pending

Mark Complete

### Experian

1-888-397-3742

[experian.com/freeze](http://experian.com/freeze)

Pending

Mark Complete

### TransUnion

1-888-909-8872

[transunion.com/freeze](http://transunion.com/freeze)

Pending

Mark Complete

# Identity Theft Recovery Action Plan

If you become a victim of identity theft, follow these steps in order:

● **Immediately**

## **1. Place fraud alerts on credit reports**

Contact one bureau; they'll notify the others. Initial alert lasts 1 year.

● **Within 24 hours**

## **2. Report to FTC at IdentityTheft.gov**

Create an official Identity Theft Report and get a personalized recovery plan.

● **Within 24 hours**

## **3. File a police report**

Some creditors require this. Bring your FTC report and any evidence.

● **Within 48 hours**

## **4. Contact affected companies**

Call fraud departments of banks, credit card companies, and other affected accounts.

● **Within 1 week**

## **5. Review credit reports thoroughly**

Request free reports from all three bureaus and dispute fraudulent accounts.

● **Ongoing**

## **6. Monitor accounts and credit**

Continue checking statements and credit reports for several months.

## Build Your Personal Protection Action Plan

### Action Item

e.g., Set up credit monitoring service

### Deadline

mm/dd/yyyy



**Add to Plan**

## Ongoing Monitoring Recommendations

### Weekly

Check bank and credit card transactions online

### Monthly

Review all financial statements for unauthorized activity

### Quarterly

Check one credit bureau report (rotate through all three)

### Annually

Review all three credit reports and update passwords