



Identity Theft Preventative Steps

What To Do After Experiencing Unemployment Fraud

If your personal information has been compromised to file an unemployment claim, consider our simplified steps below to prevent further fraud. Protecting your identity is now easier than you think.

Report to Your State's Unemployment Office. You may also file a report online at dol.gov/general/maps/fraud.

File a Police Report. Filing a report with your local police office helps with recordkeeping and the legitimacy of the claim.

Review Your Credit Reports (For Free). Accounts or activity that you don't recognize could indicate identity theft. Visit annualcreditreport.com to review now.

Create a Social Security Administration Account (SSA). Setting-up an account with the SSA allows you to monitor the validity of listed annual earnings. Starting now restricts a fraudster from creating an account or claiming/adding information in your name. Note: If you have a security freeze on Equifax's credit report, you must temporarily lift it to register with the SSA.

Place a Security Freeze on Your Credit Files. Placing a security freeze with the credit bureaus locks your credit, making it inaccessible to creditors (and fraudsters). To manage a security freeze, the specific credit bureau may offer pin verification, or may offer manual online changes. If you need to apply for credit, lift your freeze temporarily to apply.

Place Authentication Features on Financial Accounts. Ask your bank to put account passwords or pins for transaction verification purposes.

File an IRS Affidavit. Alert the IRS if you believe your information has been compromised. You don't have to wait until you're a victim. Access the form at irs.gov to get started.

Use ChexSystems Alerts. Place a security alert with chexsystems.com to alert financial institutions of your compromised information. This restricts fraudsters from opening bank accounts in your name.

Beware of Phishing Emails, Calls and Texts. If an unfamiliar source prompts you to complete an action, it may install malware or viruses on your electronic devices. We recommend to never click on any links and never respond to unknown senders of text messages.

Change Passwords Regularly. Smart account management should include complex passwords that are changed regularly. Consider intentionally making financial account passwords different.

Security Freeze Links

Click a logo to start



Protection for your
credit reputation.