

Go to IdentityTheft.gov for next steps.

Your next step might be closing accounts opened in your name, or reporting fraudulent charges to your credit card company.

IdentityTheft.gov can help — no matter what your specific identity theft situation is.

Identity Theft

Military Personnel & Families:
What to know, What to do



FEDERAL TRADE COMMISSION
IdentityTheft.gov

August 2023



FEDERAL TRADE COMMISSION
IdentityTheft.gov

Is someone using your personal or financial information to make purchases, get benefits, file taxes, or commit fraud? That's identity theft. It can disrupt your life, hurt your finances, and even put your security clearance at risk.

Visit [IdentityTheft.gov](https://www.identitytheft.gov) to report identity theft and get a personal recovery plan.

Identity Protection Tools for Servicemembers

Active duty military can get a free active duty alert and free credit monitoring. National Guard members also have a right to free credit monitoring.

Active Duty Alert

An active duty alert requires creditors to take steps during your deployment to verify your identity before granting credit in your name. It lasts one year but can be renewed for the length of your deployment.

An active duty alert also requires the three nationwide credit bureaus to take your name off their marketing lists for prescreened credit offers for two years — unless you ask them to add you back on.

To set an active duty alert, contact one of the three credit bureaus. Use the contact information on the next page. That credit bureau will notify the other two.

Free Credit Monitoring

Credit monitoring means you'll be notified of any material additions or changes to your credit file. To sign up, contact **each** of the three credit bureaus. Use the contact information on the next page.

What To Do Right Away

Step 1: Call the companies where you know fraud occurred.

- Call the fraud department. Explain that someone stole your identity. Ask them to close or freeze the accounts so no one can add new charges unless you agree.
- Change logins, passwords, and PINs for your accounts.

Step 2: Place a one-year fraud alert and get your credit reports.

- Place a free alert by contacting one of the three credit bureaus. That credit bureau must tell the other two. A fraud alert will make it harder for someone to open new accounts in your name.
- Get your free credit reports from Equifax, Experian, and TransUnion. Go to **[AnnualCreditReport.com](https://www.annualcreditreport.com)** or call 1-877-322-8228.
- Review your credit reports. Make note of any account or transaction you don't recognize. This will help you report the theft.

Credit Bureau Contacts

- **[Experian.com/help](https://www.experian.com/help)**
888-EXPERIAN
(888-397-3742)
- **[TransUnion.com/credit-help](https://www.transunion.com/credit-help)**
888-909-8872
- **[Equifax.com/personal/credit-report-services](https://www.equifax.com/personal/credit-report-services)**
800-685-1111

Get updates at
[IdentityTheft.gov/CreditBureauContacts](https://www.identitytheft.gov/CreditBureauContacts).

Step 3: Report identity theft to the FTC.

- File a report at **[IdentityTheft.gov](https://www.identitytheft.gov)** and include as many details as possible.

Based on the information you enter, **[IdentityTheft.gov](https://www.identitytheft.gov)** will create your Identity Theft Report and recovery plan.

- Notify your commanding officer. You don't want them caught off guard if they get calls looking for you, trying to collect on debts that aren't yours.