

# IF IT HAPPENS TO YOU

If you become a victim, your best defense is to recognize it quickly and take immediate action to mitigate its effects.

1. Notify your financial institution immediately if there are unauthorized entries or transactions on your account.

Close existing accounts that have been used fraudulently. Ask if the company accepts the Federal Trade Commission's Identity Theft Affidavit, available at [ftc.gov](https://www.ftc.gov). If not, ask them to send you a copy of their fraud dispute form. Complete it and return it for processing.

When opening replacement accounts, use new PINs and passwords.

Ask the company to put "fraud alerts" on accounts that have not been compromised.

Advise them not to change your address without your written notification and verification. If you do have a change of address or phone number, be sure to notify them, otherwise it may be difficult to obtain credit in the future.

2. Contact the three consumer reporting agencies and place a fraud alert on your credit report. You can place a 90-day initial fraud alert on your credit report, which can be renewed in 90-day intervals indefinitely. You can also place an extended fraud alert on your credit report for seven years if you provide a police report or official record showing you have been the victim of identity theft. For a small fee, you can also freeze your report, preventing lenders from seeing your report, unless you grant them access.
3. Cancel your ATM/Debit card if it has been stolen or compromised. You may be liable for unauthorized charges if fraud is not reported immediately (refer to your ATM/Debit card contract). Obtain a new card, account number and PIN.

4. Notify check verification companies if your checks have been stolen. Ask them to notify their retail partners. Cancel your existing account and request a new account.
5. Notify your employer if you suspect that your payroll and retirement records have been compromised.
6. Contact the Social Security Administration (SSA) if your Social Security card is lost or your Social Security number (SSN) has been misused or stolen.
7. Contact your state's department of motor vehicles (DMV) office if your driver's license has been stolen or to see if another license has been issued in your name.
8. Call police and report all crimes committed. Obtain a copy of the report or the number of the report to submit to creditors.
9. Call the Federal Trade Commission (FTC) to report the theft and file a complaint. Your information will be included in a secure online database of identity theft cases that aids civil and criminal authorities worldwide.
10. Seek appropriate professional advice immediately if legal issues should arise.

As a service member, you face unique challenges related to identity theft. Unusual work schedules, frequent relocation and deployment affect your access to normal consumer protection channels.