COMMON WAYS ID THEFT HAPPENS:

Skilled identity thieves use a variety of methods to steal your personal information, including:

1. **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
2. **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
3. **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. **Changing Your Address.** They divert your billing statements to another location by completing a "change of address" form.
5. **"Old-Fashioned" Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records from their employers, or bribe employees who have access.

Identity theft is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name.

The rigors of military life can compound the problems that identity theft creates.

Active Duty Alerts:

If you are deployed away from your usual duty station and do not expect to seek new credit while you are deployed, consider placing an "active duty alert" on your credit report. An active duty alert requires creditors to take steps to verify your identity before granting credit in your name.

An active duty alert is effective for one year, unless you ask for it to be removed sooner. If your deployment lasts longer than a year, you may place another alert on your report.

To place an active duty alert, or to have it removed, call the toll-free fraud number of one of the three nationwide consumer reporting companies. (Check under "Defend" in this brochure.) The company you call is required to contact the other two.

The law allows you to use a personal representative to place or remove an alert.

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

To learn more about ID theft and how to deter, detect, and defend against it, visit **ftc.gov/idtheft**. Or request copies of ID theft resources by writing to:

Consumer Response Center
Federal Trade Commission
600 Pennsylvania Ave., NW, H-130
Washington, DC 20580

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

MILITARY PERSONNEL & FAMILIES

FIGHTING BACK AGAINST IDENTITY THEFT

FEDERAL TRADE COMMISSION

DETER

Deter identity thieves by safeguarding your information.

- **Shred financial documents** and paperwork with personal information before you discard them.
- **Protect your Social Security number.** Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- **Don't give out personal information** on the phone, through the mail, or over the Internet unless you know who you are dealing with.
- **Safeguard your military ID.** Keep it with you or locked up at all times.
- **Never lend your credit cards** or account information to anyone else.
- **Never click on links in unsolicited emails;** instead, type in a web address you know. Use security software to protect your computer; keep it up-to-date. If you use Peer-to-Peer file sharing, check the settings to make sure you are not sharing your sensitive private files with other users. Visit **OnGuardOnline.gov** for more information.
- **Don't use an obvious password** like your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- **Keep your personal information in a secure place,** especially if you live in barracks or with roommates.
- **Don't let mail pile up** if you can't collect it. Use a mail stop or P.O. Box, or have someone you trust hold your mail while you are away.

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

DETECT

Detect suspicious activity by routinely monitoring your financial accounts and billing statements. If you are unable to take these steps while you are deployed, consider placing an "active duty alert" on your credit report.

Inspect:

- **Your credit report.** Credit reports contain information about you, including what accounts you have and your bill-paying history.
  - The law requires each of the major nationwide consumer reporting companies—Equifax, Experian, and TransUnion—to give you a free copy of your credit report every year if you ask for it.
  - Visit **www.AnnualCreditReport.com** or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- **Your financial statements.** Review your financial accounts and read your billing statements regularly, looking for charges you did not make. If you review financial accounts online from a public computer, be sure to log off of financial sites before you end your session.

Be alert to signs that require immediate attention:

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make

DEFEND

Defend against ID theft as soon as you suspect it.

- **Place a "Fraud Alert" on your credit reports, and review the reports carefully.** The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:
  - Equifax: 1-800-525-6285
  - Experian: 1-888-EXPERIAN (397-3742)
  - TransUnion: 1-800-680-7289

  Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.
- **Close accounts.** Close any accounts that have been tampered with or established fraudulently.
  - Call the security or fraud departments of each company where an account was opened or changed without your okay. Follow up in writing, with copies of supporting documents.
  - Use the ID Theft Affidavit at **ftc.gov/idtheft** to support your written statement.
  - Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
  - Keep copies of documents and records of your conversations about the theft.
- **Explain the situation to your commanding officer.** You don't want your C.O. taken by surprise if contacted by creditors looking to collect on charges made by the identity thief. You also may want a referral to a legal assistance office.
- **File a police report.** File a report with military law enforcement and the local police (if you are in the United States). Their reports will help you with creditors who may want proof of the crime.
- **Report the theft to the Federal Trade Commission.** Your report helps law enforcement officials across the United States in their investigations.
  - Online: **ftc.gov/idtheft**
  - By phone: **1-877-ID-THEFT** (438-4338) or TTY, 1-866-653-4261
  - By mail: **Identity Theft Clearinghouse**, Federal Trade Commission, Washington, DC 20580

To learn more about ID theft and how to deter, detect, and defend against it, visit **ftc.gov/idtheft.**