Identity Theft for Military Servicemembers

DETER

- **Skimming**: Unlawful interception of credit card data either through electronic, mechanical or human means.
- **Phishing**: Internet fraudsters send spam or pop-up messages to gain personal and financial information.
- **Smishing**: Text messaging in an attempt to gain personal and financial information.
- **Spam**: Unsolicited amounts of commercial emails.

DETECT

- Routinely monitor your financial accounts and billing statements by looking for charges that you did not make.
- Review financial and medical statements for errors.
- Investigate any suspicious activity immediately!
- Request a free credit report through www.AnnualCreditReport.com.

DEFEND

- Put an “active duty alert” on your credit report while you’re deployed.
- Review your credit report annually.
- Do not give out your Social security number, Military I.D., or other personal information unless you are 100% sure of the creditability of the person or business.
- Notify the post office not to accept any address changes without your personal Postal Service password.
- Periodically request an “account history” from the Social Security Administration.

Protect your information online

- Update virus protection and firewall software.
- Do not open files sent to you by strangers.
- Look for indicators that a website is secure (https: in web address).
- When disposing of an old computer, use a wipe utility program to overwrite the hard drive.

Fight Back

Report any problem as soon as possible. Request a fraud alert or security freeze on our credit report and close the fraudulent account.

For more information or to file a complaint, call the Florida Department of Law Enforcement at (850) 410-7000, the Florida Attorney General at 1-866-966-7226, or the Federal Trade Commission at 1-877-438-4338.