

Chapter 6

Identity Theft



The United States Department of Justice defines identity theft as “a crime in which someone wrongfully obtains or uses another person’s personal data in some way that involves fraud or deception, typically for economic gain.” This crime has been steadily on the rise, especially with the growing popularity of the Internet for buying products and online banking. Although this crime is devastating to everyone, it can be even more so for servicemembers. Beginning in the 1960s, servicemembers’ and their family members’ Social Security numbers were printed on their identity cards, making the numbers especially vulnerable to theft. In 2008, the military recognized that this practice caused servicemembers to be at risk for identity theft and began phasing out printing Social Security numbers on servicemembers’ identity cards. Since 2012, servicemembers have been issued a new ID card without the Social Security number printed on the back. Instead, servicemembers are assigned a DOD number that is unique to them and associated with their Social Security number. Because each military base is different, there may still be some servicemembers who have outdated ID cards. If so, servicemembers may want to work with their administrative officer to obtain an updated card that doesn’t put them at risk for identity theft.

The consequences of identity theft require a great deal of time, money and energy to handle properly. It has potentially more serious implications for servicemembers because credit worthiness is linked to security clearances. If a servicemember’s identity is stolen, he or she may potentially lose their security clearance.

Free Annual Credit Reports

In addition to using their Social Security numbers as part of their daily routines, servicemembers are required to move frequently based on their assignment. This creates open or revolving business accounts that may stretch across state lines or international borders. Open or revolving accounts can make it difficult for a servicemember to keep track of the account information, especially if the servicemember is deployed. It is important to maintain a secure record of all open accounts and to monitor credit reports at least once a year. But make sure to not get duped into paying for credit reports or accidentally signing up for credit monitoring services

unless you have a need for the additional services, like a credit score, that they provide. Truly free credit reports by each of the three major credit reporting agencies can be obtained once per year at www.annualcreditreport.com.

Identity Theft Prevention

Servicemembers on active duty may be less able to respond to fraudulent activity on bank and credit card accounts in a timely manner. An amendment to the Fair Credit Reporting Act (FCRA) allows a servicemember to place an “active duty alert” in his or her credit report to help prevent identity theft. When servicemembers are away from their usual stations, placing an active duty alert on a credit report may help minimize the risk of identity theft while deployed. This active duty alert requires creditors to verify the applicant’s identity before granting credit in the servicemember’s name. Additionally, the servicemember’s name will be removed for two years from the nationwide consumer reporting companies’ marketing list for prescreened offers of credit and insurance, unless that active duty alert is removed by the servicemember. To place an active duty alert on a credit report, servicemembers need only contact one of the three nationwide consumer reporting companies: Equifax, Experian or TransUnion. Each agency is required to notify the other two. It is important to keep the servicemember’s contact information updated for as long as the alert is placed on the account.

The best ways to prevent identity theft are relatively simple. Servicemembers should avoid giving out any personal information like Social Security numbers and bank account numbers to anyone unless the servicemember initiated the contact. Banks and credit card companies will never make contact via email or telephone seeking to verify personal information. When credit card offers arrive in the mail, don’t toss them in the trash without shredding them first. Keep all personally identifiable information like Social Security cards, bank statements, birth certificates, and driver’s license information in a secure location. Avoid clicking on links in emails that come from an unknown sender. Never give out personal information in an email or over the phone unless the contact was initiated by the servicemember.

Any consumer or servicemember should submit a report to the Federal Trade Commission (FTC) if he or she is a victim of identity theft. Consumers should print and keep a copy of the identity theft report, which will be the consumer's Identity Theft Affidavit. Consumers should also file a police report about the identity theft and get a copy of the police report or the report number. When filing the police report, make sure to bring a government-issued photo identification card, proof of address, a copy of the FTC Identity Theft Affidavit, and any other proof of the identity theft. The FTC Identity Theft Affidavit and the police report together make an Identity Theft Report. Creating an Identity Theft Report can help consumers deal with credit reporting companies, debt collectors, and businesses that gave credit to the person who stole the consumer's identity. The FTC can be contacted toll-free at 877-FTC-HELP (877-382-4357) or online at www.ftc.gov.

For a complete guide to dealing with the consequences and aftermath of identity theft, please refer to the FTC's Guide "Taking Charge" which is available for free on the FTC's website at www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf or by calling the FTC. Consumer Affairs Counselors may be able to help servicemembers work through this Guide.

