

Solutions for Victims of Identity Theft: A Guide for Judge Advocates to Assist Servicemembers in Deterring, Detecting, and Defending Against This Growing Epidemic

Major Cindie Blair*

Good name in man and woman, dear my lord, is the immediate jewel of their souls. Who Steals my purse steals trash; 'tis something, nothing; 'Twas mine, 'tis his, and has been slave to thousands; But he that filches from me my good name, Robs me of that which not enriches him. And makes me poor indeed.¹

Introduction

Identity theft is one of the fastest growing crimes in the United States and is rapidly becoming an epidemic that leaves many judge advocates ill prepared to assist victim servicemembers. From 2007 to 2008 identity theft increased by 21% and it costs consumers roughly \$50 billion annually.² Even though identity theft reports declined by 5% in 2009, it still represents the number one complaint to the Federal Trade Commission (FTC), accounting for 21% of complaints received in 2009.³ Specifically, credit card fraud is the most common form of theft.⁴

Recovering from identity theft can be frustrating, time consuming, and expensive.⁵ Police often ignore these complaints, claiming they do not believe the victim or do not have jurisdiction over the crime.⁶ Shockingly, 28% of victims in a survey were unable to restore their identities and fix their credit even after a year of trying.⁷ Additionally, in 2003, the FTC surveyed identity theft victims and found that 9% lost their identity to a member of their own family.⁸ The increases in identity theft crimes led to new legislation, which not only criminalized stealing another's identity, but also defined the crime.⁹

The current federal statute defines identity theft as something that occurs when one "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law."¹⁰ In simpler terms, identity theft is the misuse of another person's information to commit fraud.¹¹ This crime typically consists of three stages: (1) the thief tries to obtain someone's personal information; (2) the thief tries to misuse the information he has obtained; and, (3) the thief completes the crime, leaving the victim to attempt to mitigate the consequences.¹² People must combat identity theft at all three stages to safeguard their good names.¹³

This article serves a dual purpose. First, the article will educate servicemembers on the increased risk of identity theft and how to protect themselves, which will create a greater awareness of the problem and reduce the growing number of victims in the armed forces. Second, it serves as a guide for judge advocates to teach servicemembers and assist victims with the most common problems arising from identity theft. In order to successfully combat these crimes, servicemembers need to be aware of the common scams sweeping across the country and take the proper precautions to safeguard their own identity.

Servicemembers are especially vulnerable to thieves due to overseas deployments, multiple relocations, and the numerous agencies requiring the use of their Social Security Number (SSN) as identification. With proper training and advice from judge advocates, servicemembers can learn to take precautions to safeguard their identities and significantly reduce the risk of becoming victims of identity theft. An article educating judge advocates about the increased risk of identity theft and providing instructions on how servicemembers can protect themselves will create a

* Judge Advocate, U. S. Marine Corps. Presently assigned as Deputy Staff Judge Advocate, Headquarters U. S. Pacific Command, Camp H. M. Smith, Hawaii. This primer was submitted in partial completion of the Master of Laws requirements of the 58th Judge Advocate Officer Graduate Course.

¹ MARTIN T. BIEGELMAN, *IDENTITY THEFT HANDBOOK: DETECTION, PREVENTION, AND SECURITY* 27 (2009) (quoting WILLIAM SHAKESPEARE, *OTHELLO* act 3, sc. 3, at ll. 155-6).

² KRISTIN M. FINKLEA, *CONG. RESEARCH SERV. REPORT, R40599, IDENTITY THEFT: TRENDS AND ISSUES*, at CRS-1 (2009).

³ *FTC ISSUES REPORT OF 2009 TOP CONSUMER COMPLAINTS* (Feb. 24, 2010), available at <http://www.ftc.gov/opa/2010/02/2009fraud.shtm>.

⁴ DIONYSIOS POLITIS, PHAEDON KOZYRIS, & IONNIS IGLEZAKIS, *SOCIOECONOMIC AND LEGAL IMPLICATIONS OF ELECTRONIC INTRUSION* 65 (2009).

⁵ BIEGELMAN, *supra* note 1, at 177.

⁶ *Id.*

⁷ *Id.*

⁸ RACHAEL LININGER & RUSSELL DEAN VINES, *PHISHING: CUTTING THE IDENTITY THEFT LINE* 1 (2005).

⁹ *Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information*, 18 U.S.C. § 1028(a)(7) (2006).

¹⁰ *Id.*

¹¹ THE PRESIDENT'S IDENTITY THEFT TASK FORCE, *COMBATING IDENTITY THEFT: A STRATEGIC PLAN 2-3* (Apr. 2007) [hereinafter *IDENTITY THEFT TASK FORCE*], available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

¹² *Id.*

¹³ *Id.*

greater awareness of the problem and reduce the growing number of servicemember victims.

This article will address identity theft in three parts: “detection, deterrence, and defense.”¹⁴ The first section identifies the problem by informing servicemembers about how thieves steal their information and later use it to commit a crime. It also addresses how victims learn they have been compromised and why servicemembers are so vulnerable. The second section addresses how and when judge advocates should conduct preventative training to servicemembers on this issue. Finally, the third section will serve as a step-by-step guide for legal assistance attorneys responsible for helping victims of identity theft repair their damaged credit, thus restoring “[t]he immediate jewel of their souls.”¹⁵

Detection: Identifying the Problem

How Do Thieves Obtain My Information?

Before anyone can prevent identity theft, he must first identify what to avoid. Thieves obtain personal information from victims in a number of ways, and many involve theft from a careless consumer. This is done through various methods such as stealing someone’s purse or wallet (with credit and bank cards, identification, and checks); taking someone’s mail; stealing personal identifier documents (driver’s licenses, birth certificates, social security cards, and employee badges); rummaging through people’s trash (“dumpster diving”); or by taking personal information from the home (usually by a roommate or family member).¹⁶

Savvy identity thieves will get personal information from businesses or other entities. They can steal records while they are working; trick employees into divulging personal information about themselves or others; bribe a records custodian; copy information from unattended identification; or even hack into a computer records database.¹⁷ Some clever thieves even submit a false change of address to intercept mail or use portable skimming devices that record your credit card information during an authorized transaction for future fraudulent use.¹⁸

The most sophisticated thieves acquire information via computers and the internet. This is accomplished in a

variety of ways and is often referred to as “phishing.”¹⁹ One such method works by offering the unsuspecting victim free software, such as antivirus protection.²⁰ Once the consumer attempts to download the application, he exposes his system to spyware that allows thieves to record keystrokes and to gather sensitive information.²¹ Another common ruse involves sending emails to consumers indicating someone fraudulently used their account and threatening to close the account unless the victim sends their personal information.²² Similarly, the thief may send an email from a business or bank indicating the company lost records or needs to verify information.²³ More experienced computer hackers can even successfully compromise major databases containing personal information.²⁴

How Do Thieves Use My Information?

Once a consumer is aware of how thieves access personal information, the next step is to realize how the criminal uses the stolen identity. Depending on the information obtained, thieves can defraud victims in a number of ways. With personal identification, thieves can alter the identification information; produce counterfeit documents; distribute or sell personal information to others; and open credit or bank accounts in the victim’s name.²⁵ Some criminals even use personal information to impersonate the victim or take over their actual identity.²⁶ Illegal immigrants assume the identity of a citizen to get jobs benefits, to obtain mortgages and credit cards, and to be welcomed into society.²⁷ There is also an increase in the use of other people’s SSNs to make false medical claims with insurance companies.²⁸ Additionally, the thief may file fraudulent tax returns in victims’ names or even provide a victim’s information to police if arrested.²⁹

¹⁴ TAKE CHARGE: FIGHTING BACK AGAINST IDENTITY THEFT, at cover (n.d.) [hereinafter TAKE CHARGE], available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.shtm> (last visited Jan. 10, 2010).

¹⁵ WILLIAM SHAKESPEARE, OTHELLO act 3, sc. 3, at ll. 155–6.

¹⁶ BIEGELMAN, *supra* note 1, at 177; *see also* TAKE CHARGE, *supra* note 14, at 2.

¹⁷ TAKE CHARGE, *supra* note 14, at 2.

¹⁸ BIEGELMAN, *supra* note 1, at 36; *see also* ID THEFT: WHAT IT’S ALL ABOUT 11 (June 2005), available at <http://www.ftc.gov/bcp/pubs/consumer/idtheft/idth08.shtm>.

¹⁹ LININGER & VINES, *supra* note 8, at 1 (Phishing is the “act of obtaining personal information directly from the end user through the internet. This information can then be used for fraud, Identity theft, or other purposes.”). *Id.*

²⁰ BIEGELMAN, *supra* note 1, at 30.

²¹ *Id.* (Spyware is a type of malware that is installed on computers and collects little bits information at a time about users without their knowledge.).

²² LININGER & VINES, *supra* note 8, at 9.

²³ *Id.*

²⁴ *Id.* at 22.

²⁵ BIEGELMAN, *supra* note 1, at 28; *see also* IDENTITY THEFT TASK FORCE, *supra* note 11, at 18.

²⁶ BIEGELMAN, *supra* note 1, at 28

²⁷ *Id.*

²⁸ BIEGELMAN, *supra* note 1, at 28; *see also* IDENTITY THEFT TASK FORCE, *supra* note 11, at 20.

²⁹ TAKE CHARGE, *supra* note 14, at 4.

If a criminal obtains a credit card number either by visual inspection, an old receipt, or through “skimming,”³⁰ he can make purchases online while the card is still in the consumer’s possession.³¹ Skimming also allows the thief to encode data from the card and into blank cards for use by multiple people at any company that accepts credit.³² If the thief goes a step further by forwarding or stealing the victim’s mail, the consumer may not get a statement or be alerted when fraudulent transactions occur.³³ There are countless ways a thief can fraudulently use someone’s personal information; the key is for the victim to identify the breach early and act immediately.

How Do I Know I Have Been Victimized?

The more time that passes between the act of identity theft and when the victim discovers the crime, the more it costs the victim.³⁴ Often victims learn about theft only when it negatively affects their lives.³⁵ For instance, if an unsuspecting consumer is not vigilant, he may learn he is a victim only through a denial of credit, receipt of credit cards not applied for, or calls from bill collectors.³⁶

A consumer may also see an unrecognized charge or debit on a bank or credit account statement.³⁷ If diligent, they may learn about fraudulent activity when checking a credit report for unrecognized transactions and credit.³⁸ Victims may even be arrested for crimes they did not commit or receive merchandise in the mail they did not order.³⁹ However the victim discovers the fraud, the issue must be addressed immediately.

What Makes Servicemembers Vulnerable?

Of all the information a thief can use, the SSN most facilitates their crime and is usually necessary to commit identity theft because it provides access to an individual’s entire financial life.⁴⁰ In 1969, the Department of Defense

(DoD) replaced the military service number with the SSN as an identifier for servicemembers.⁴¹ The U.S. Government Accountability Office (GAO) first reported the identity theft risk of using SSNs in public records in 2006.⁴² The report found that eight million DoD identification cards contained the full SSN of the employee or servicemember.⁴³ In April 2008, responding to the growing concern of identity theft, the DoD decided to no longer use the full SSN on identification cards.⁴⁴ However, a servicemember’s full SSN still appears on their identification tags (i.e., “dog tags”).⁴⁵

Additionally, the servicemember’s (and often their family’s) SSN was or is still contained on military records (including medical and dental records), duffel bags, relocation documents, orders, dining facility rosters, and in many databases including those of TriCare and the Veteran’s Administration.⁴⁶ Having an SSN so readily accessible to others puts servicemembers and their families at a higher risk than civilians who are not required to use their SSN as often. Many unmarried servicemembers also live in a shared environment like the barracks, allowing roommates or a visitor’s easy access to identification cards or dog tags.

Because the military uses the SSN as an identifier, many military-related databases contain this sensitive information, leading computer savvy thieves to target the military.⁴⁷ Every year the number of database breaches increases.⁴⁸ Of the five industries with the greatest number of recorded breaches, the military is the third largest at 16.8%.⁴⁹

Gov’t Info. of the Comm. on the Judiciary (May 1998) (Statement of David Medine, Assoc. Dir. for Credit Practices, Bureau of Consumer Prot., Fed. Trade Comm’n); Oscar Gandy, Professor, Comments of the Elec. Privacy Info. Ctr., Consumer Action, Privacy Activism, Commercial Alert, Privacy Journal, World Privacy Forum, Privacy Rights Clearinghouse 3 (June 22, 2005), <http://epic.org/privacy/profiling/dodrecruiting.html>.

⁴¹ Social Security Number Chronology (Nov. 9, 2005), <http://www.socialsecurity.gov/history/ssn/ssnchron.html>.

⁴² Privacy Rights Clearinghouse; My Social Security Number—How Secure Is It? (June 1993), <http://www.privacyrights.org/print/fs/fs10-ssn.htm> [hereinafter Privacy Rights Clearinghouse].

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ Melanie Henson, *Identity Theft and the Military: U.S. Service People Are Prime Targets*, CREDIT IDENTITY SAFE, Nov. 10, 2008, available at <http://creditidentitysafe.com/prevention/identity-theft-and-the-military-us-people-are-prime-targets.htm>.

⁴⁶ Byron Acohido & Jon Swartz, *Military Personnel Prime Targets for ID Theft*, USA TODAY, June 14, 2007, available at http://creditidentitysafe.com/tech/news/computersecurity/infotheft/2007-06-14-military-id-thefts_N.htm?csp=34; see also Henson, *supra* note 45.

⁴⁷ Kelly P. Pate, *Identity Theft: Army Protecting Its Own in New Ways*, ARMY.MIL/NEWS, Oct. 15, 2008, <http://www.army.mil/-news/2008/10/15/13304-identity-theft-army-protecting-its-own-in-new-ways/>.

⁴⁸ FINKLEA, *supra* note 2, at CRS-20.

⁴⁹ *Id.*

³⁰ BIEGELMAN, *supra* note 1, at 36 (defining skimming as using a portable credit card reader to capture account data from the magnetic stripe and then placing that information on a counterfeit card for fraudulent use).

³¹ IDENTITY THEFT TASK FORCE, *supra* note 11, at 18.

³² *Id.*

³³ TAKE CHARGE, *supra* note 14, at 3.

³⁴ POLITIS, KOZYRIS, & IGLEZAKIS, *supra* note 4, at 66.

³⁵ *Id.*

³⁶ ID THEFT: WHAT IT’S ALL ABOUT, *supra* note 18, at 11.

³⁷ LININGER & VINES, *supra* note 8, at 21.

³⁸ ID THEFT: WHAT IT’S ALL ABOUT, *supra* note 18, at 11.

³⁹ TAKE CHARGE, *supra* note 14, at 2.

⁴⁰ BIEGELMAN, *supra* note 1, at 236; *Prepared Statement of the Fed. Trade Comm’n on “Identity Theft” Before the S. Comm. on Tech., Terrorism and*

One example of a database breach affecting military personnel involved an incident in 2006 when someone stole a Department of Veterans Affairs laptop from an employee's home.⁵⁰ The computer held personal information on more than 28 million veterans, military personnel, and their spouses.⁵¹ Over 50,000 of the affected individuals was on active duty.⁵² The Department of Veterans Affairs were similarly complacent in August 2006, when it lost computer data for 38,000 patients; on 2 November 2006, when it lost a computer with data for 1,600 patients; and in February 2007, when it compromised data on a hard drive containing information for two million VA patients and doctors.⁵³ In 2002, the theft of computer servers from a military health care contractor in Phoenix, Arizona, compromised SSNs and other personal data for more than 500,000 active duty and retired servicemembers and their families.⁵⁴

While most people fear strangers gaining access to major military databases, studies over the last few years have found the largest identity theft threat is from trusted insiders within organizations.⁵⁵ Unfortunately, this is also true for military units and has resulted in criminal prosecutions of servicemembers for theft and misuse of sensitive personal information. One such case involved Airman First Cass Shepherd, an administrative apprentice for his Air Force squadron.⁵⁶ Airman Shepherd used the names and SSNs of other airmen obtained from unit rosters to open fraudulent cellular telephone accounts.⁵⁷

A similar case involved a Marine staff sergeant (SSgt) working as an administration chief in the finance office.⁵⁸ The SSgt used personal information obtained in the course of his duties to make false identification papers in the name of one of the reservists receiving checks at his office.⁵⁹ He

then opened a bank account and cashed the reservist's checks using the false identification.⁶⁰

One of the most recent prosecutions involved Specialist (SPC) Reynaldo Jimenez, an active duty Finance Technician in the Army who helped military members with payroll issues from 2005 to 2008.⁶¹ Part of SPC Jimenez's job required him to assist servicemembers access their payroll information through "MyPay"⁶² where he would obtain and keep a list of SSNs and MyPay passwords from numerous military personnel.⁶³ In 2008, SPC Jimenez left his Korean duty station without authorization and used some of the stolen SSNs and passwords to change information in their accounts.⁶⁴ He then obtained two false driver's licenses and opened debit card accounts in his fellow Soldiers' names, which he used to route some of the victim's pay to his own account.⁶⁵ SPC Jimenez tried to steal over \$35,000 from more than thirty-five active duty servicemembers but was only successful in stealing about \$6,500.⁶⁶

Besides the use of SSNs and computers, several other factors put servicemembers at a higher risk to become victims of identity theft. Not only does the military provide a regular income paid bi-monthly, but servicemembers are strongly encouraged to pay debts and are subject to criminal prosecution under the Uniform Code of Military Justice for failure to pay their debts.⁶⁷ Also, it is easy for bill collectors to locate the servicemember in case of default due to theft.⁶⁸ As a result, many servicemembers receive an inordinate amount of offers from credit card companies that thieves can

⁵⁰ BIEGELMAN, *supra* note 1, at 241.

⁵¹ *Id.*

⁵² Henson, *supra* note 45.

⁵³ Acohido & Swartz, *supra* note 46.

⁵⁴ Steve Lynch, *Year of Preventing Identity Crime: Prevention Is the Best Protection for the U.S. Coast Guard's Ninth District*, POLICE CHIEF MAGAZINE, June 6, 2008, available at http://policechiefmagazine.org/magazine/magazine/index.cfm?fuseaction=display_arch&article_id=1530&is_sue_id=62008.

⁵⁵ BIEGELMAN, *supra* note 1, at 243.

⁵⁶ *United States v. Shepherd*, ACM 34766, 2002 CCA LEXIS 189 (A.F. Ct. Crim. App. Aug. 20, 2002) (unpublished) (Appellant was found guilty of five drug offenses in addition to the dereliction of duty charge involved with failing to safeguard Privacy Act information and sentenced to a bad conduct discharge, confinement for two years, reduction to E-1, and forfeiture of all pay and allowances.).

⁵⁷ *Id.*

⁵⁸ *United States v. Krauss*, 20 M.J. 741, 742 (N.M.C.M.R. 1985) (Appellant was convicted at a general court-martial for twelve counts of check forgery, twelve counts of treasury check theft, and dereliction of duty and sentenced to a bad conduct discharge, confinement for two years, reduction to E-1, and forfeiture of all pay and allowances.).

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ Press Release, Fed. Bureau of Investigation, Former U.S. Army Finance Technician Sentenced in Manhattan Federal Court to 42 Months in Prison for Theft of Soldiers' Social Security Numbers and Pay (Sept. 30, 2009), available at <http://newyork.fbi.gov/dojpressrel/pressrel09/nyfo093009.htm>.

⁶² *Id.* ("MyPay" is a military website that contains leave and earnings statements and other personal financial information and also directs where a servicemember's pay will be deposited.).

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.* (Jimenez pleaded guilty in April 2009 in the Southern District Court of New York to one count of identity theft, one count of access device fraud, one count of fraud in connection with protected computers, and one count of aggravated identity theft. In addition to forty-two months in prison, the judge also ordered Jimenez to serve three years of supervised release, forfeit \$6,557.47, and pay to the Government \$6,557.47 in restitution.).

⁶⁷ Memorandum from Deputy Assistant Judge Advocate Gen. Legal Assistance (Code 16) on Identity Theft—What It Is and How to Avoid It (n.d.) (last visited Jan. 13, 2010) [hereinafter Identity Theft Memorandum], available at [http://www.ig.navy.mil/Divisions/Intel/Intel_Security%20\(Identity%20Theft\).htm](http://www.ig.navy.mil/Divisions/Intel/Intel_Security%20(Identity%20Theft).htm) (last visited Jan. 13, 2010); see also UCMJ art. 134 (2008).

⁶⁸ Identity Theft Memorandum, *supra* note 67.

easily intercepted.⁶⁹ Many servicemembers are further vulnerable because they tend to be young and lack financial expertise.⁷⁰ These young enlisted servicemembers are generally commercially unsophisticated, trusting, inexperienced, and away from home for the first time.⁷¹

Deployed personnel are probably the most targeted group of servicemembers for identity crimes.⁷² One reason is that deployed members have limited access to on-line services or even regular mail delivery, and therefore may not look at a credit report for a year or more.⁷³ Additionally, most mail forwarded to deployed servicemembers is delayed, which prevents swift discovery of fraudulent transactions.⁷⁴ Even if servicemembers detect fraud, deployments interfere with immediate reporting since most police departments do not accept reports over the phone.⁷⁵ One Marine corporal returned from Iraq in 2006 only to learn someone in San Diego had opened credit card accounts, bought a house, and fraudulently started a business using his identification.⁷⁶ While the corporal eventually cleared his good name, his efforts still took a year, even with the help of a commercial fraud protection company.⁷⁷

Families of deployed personnel are also frequently targeted for identity theft.⁷⁸ Identity thieves obtain information about when a servicemember is deployed and his family's contact information from a variety of sources, including official military websites, other family members, military insiders, or even websites maintained by the servicemembers themselves—such as an account on Facebook or another social networking site.⁷⁹ Once thieves have this information, they use it to accomplish a variety of scams.

One of the most reprehensible scams perpetrated using only a deployment schedule and a phone number, is accomplished by the thief calling a deployed servicemember's family posing as someone from the DoD.⁸⁰ The thief asks a family member for the SSN of the relative

who was allegedly killed in combat in order to confirm the identity of the deceased member.⁸¹ A similar scam involves the caller posing as a Red Cross representative stating the servicemember was hurt while deployed.⁸² The caller advises the family that treatment cannot start until paperwork requiring verification of the member's SSN and date of birth are completed.⁸³

Deterrence: Preventing the Problem

What Do We Teach Servicemembers?

In order to stop thieves from taking advantage of servicemembers, it is essential to teach prevention and to incorporate preventative measures into standard processes for handling and storing personal information. There are numerous steps all servicemembers and their families should take to protect themselves from becoming victims of fraud.

Take Precautions to Safeguard Social Security Numbers

Because SSNs are the key to identity theft, servicemembers should avoid providing their SSNs whenever possible.⁸⁴ The servicemember can avoid this by not printing the full number on checks or dog tags.⁸⁵ Additionally, the member should strongly challenge all businesses or other entities requesting a SSN, and provide it only if required by law.⁸⁶ Servicemembers and their families should not carry a Social Security, insurance, or any other card with a visible SSN and should keep wallets on their person or locked up at all times.⁸⁷

Many people are unaware that some states use the SSN as a driver's license number; however, new federal legislation has been introduced prohibiting states from displaying the SSN on a license.⁸⁸ Most states will issue a license with an alternative number for a minor fee.⁸⁹ Servicemembers with a SSN as driver's license number are encouraged to contact

⁶⁹ Henson, *supra* note 45.

⁷⁰ Identity Theft Memorandum, *supra* note 67.

⁷¹ Lynch, *supra* note 54.

⁷² Henson, *supra* note 45; *see also* Acohido & Swartz, *supra* note 46.

⁷³ Pate, *supra* note 47.

⁷⁴ Lynch, *supra* note 54.

⁷⁵ *Id.*

⁷⁶ Acohido & Swartz, *supra* note 46.

⁷⁷ *Id.*

⁷⁸ Paul McNamara, *Cruel ID Thieves Target Military Families*, NETWORKWORLD.COM COMMUNITY, Oct. 11, 2006, <http://www.networkworld.com/community/node/8842>; *see also* Henson, *supra* note 45.

⁷⁹ McNamara, *supra* note 78.

⁸⁰ *Id.*

⁸¹ *Id.*

⁸² New Scam Targeting Military Spouses, May 29, 2007, http://protectour.org/public_advisories.

⁸³ *Id.*

⁸⁴ BIEGELMAN, *supra* note 1, at 296.

⁸⁵ Social Security Number and Date of Birth Issues, Concerns, and Policy, http://www.dogtagsrus.com/catalog/information.php?info_id=5 (last visited 14 Jan. 2010); *see also* BIEGELMAN, *supra* note 1, at 295.

⁸⁶ Privacy Rights Clearinghouse, *supra* note 42.

⁸⁷ BIEGELMAN, *supra* note 1, at 296.

⁸⁸ U.S. GEN. ACCOUNTING OFFICE, REPORT TO THE CONGRESSIONAL COMMITTEES, GAO-05-1016T: FEDERAL AND STATE LAWS RESTRICT THE USE OF SOCIAL SECURITY NUMBERS YET GAPS REMAIN (2005), *available at* <http://www.gao.gov/new.items/d051016t.pdf>.

⁸⁹ Privacy Rights Clearinghouse, *supra* note 42; *see also* TAKE CHARGE, *supra* note 14, at 32.

their state's department of motor vehicles and request a replacement as soon as possible.⁹⁰

Safeguard Other Important Information

While it is crucial servicemembers protect their SSN, it is just as important to safeguard access to all personal and financial information, such as date of birth, bank accounts, credit cards, insurance, and other information.⁹¹ One simple way to minimize theft is to limit the number of credit cards owned or used and carry only the minimum number of cards and information that are absolutely necessary.⁹² Servicemembers should never carry ATM PINs or other passwords in their wallet or store them on cell phones or computers.⁹³

Servicemembers should also never give confidential information, such as a mother's maiden name or birth date, over the telephone, through the mail, or on the internet unless familiar with the requestor, and should always inquire why someone needs this information.⁹⁴ Additionally, servicemembers should use a confetti-cut shredder to shred any written documentation with personal information such as credit card or bank statements, copies of applications, or credit card receipts and offers before discarding them in the trash.⁹⁵

Review Credit Reports

Everyone is entitled to a free credit report from all three bureaus (TransUnion, Equifax, and Experian) every twelve months or anytime a creditor takes adverse action against a person, so long as he requests a report within 60 days of receiving notice of the adverse action.⁹⁶ The only way to order a free report from all three reporting companies simultaneously is by visiting www.annualcreditreport.com, calling 1-877-322-8228, or mailing an Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.⁹⁷

A better way to ensure credit and identity remain safe is to order a report separately from one of the three credit

bureaus every four months.⁹⁸ For example, a person can write Equifax in October for a free annual report, TransUnion in February and Experian in June. This enables a person to receive a free credit report three times a year instead of annually for a more thorough inspection of financial information.

Servicemembers should also review their children's credit reports to ensure thieves have not confiscated the minor's identity.⁹⁹ When reviewing the report, look for unauthorized credit inquiries or approved credit and any other mistakes regardless of whether it is fraud related.¹⁰⁰ If the servicemember finds any issues, he should immediately report the problem to the credit bureaus and seek legal assistance if necessary.¹⁰¹

Review Credit Card and Bank Statements

Due to the risk of mail theft and the frequency with which military personnel relocate, it is imperative servicemembers know the billing cycle of credit card and bank statements and review the paperwork every month.¹⁰² Thieves often submit change-of-address notices of potential victims or steal mail from unlocked boxes in order to obtain another's personal information.¹⁰³ When reviewing statements, the servicemember should look for unauthorized charges or debits and other mistakes such as excess or double charging by the creditor.¹⁰⁴ It is also important to review cancelled checks on bank statements and reconcile the account to make sure a thief has not changed the amount on the check or accessed the account.¹⁰⁵

Computer and Internet Awareness and Safety

If the servicemember must disclose personal information over the internet, he should take precautions to ensure he has the latest spyware and anti-virus software installed.¹⁰⁶ Military personnel are provided free anti-spyware software at <https://iase.disa.mil/sdep> and anti-virus software or at

⁹⁰ *Id.*

⁹¹ BIEGELMAN, *supra* note 1, at 296.

⁹² *Id.*; *see also* TAKE CHARGE, *supra* note 14, at 32.

⁹³ BIEGELMAN, *supra* note 1, at 296.

⁹⁴ *Id.*

⁹⁵ *Id.* at 298; *see also* TAKE CHARGE, *supra* note 14, at 32.

⁹⁶ TAKE CHARGE, *supra* note 14, at 28.

⁹⁷ *Id.*

⁹⁸ BIEGELMAN, *supra* note 1, at 297 (These reporting companies may be contacted separately for a credit report at: Equifax: 1-800-525-6285; www.equifax.com; Experian: 1-888-EXPERIAN (397-3742); www.experian.com; and TransUnion: 1-800-680-7289; www.transunion.com).

⁹⁹ *Id.*

¹⁰⁰ *Id.*

¹⁰¹ *Id.* at 296.

¹⁰² *Id.* at 305.

¹⁰³ *Id.* at 296.

¹⁰⁴ *Id.* at 304.

¹⁰⁵ *Id.*

¹⁰⁶ Privacy Rights Clearinghouse, *supra* note 42.

<https://infosec.navy.mil> for use on their home computers.¹⁰⁷ The military also has strict rules mandating periodic changes to computer passwords utilizing a mix of alpha and numeric characters in combination for better security.

Servicemembers should practice the same diligence on their home computers to protect against unauthorized access to computers, accounts, and wireless networks.¹⁰⁸ People should not record the passwords or make them easily identifiable.¹⁰⁹ Additionally, the passwords should be at least eight characters in length, but fourteen or more is best.¹¹⁰ Stronger passwords will contain random letters, numbers, punctuation, and symbols that are not repeated or written down, and the user should change the password on a regular basis.¹¹¹ It is also best to enable password protection on a home computer and ensure encryption of any home wireless networks so thieves cannot access it and steal personal information.¹¹² Servicemembers should also avoid using public computers, which are often infected with malware or viruses that allow thieves access to the websites and files a person uses.¹¹³

Additionally, servicemembers should only do business with well-known, reputable online companies and ensure the connection is secure by looking for the closed padlock symbol on the bottom of the page.¹¹⁴ Another indication of a secure site for passing personal information is when the Uniform Resource Locator (URL) address at the top of the page changes from “http” to “https.”¹¹⁵ Computers should also have sufficient firewall protection to help block thieves from remotely loading virus programs that can record and transmit keystrokes and other files.¹¹⁶

Servicemembers must be aware of phishing and other email schemes.¹¹⁷ Do not open messages or files from

¹⁰⁷ Computer Resources for Military Service Members, <http://freecomputerzone.com/downloads/military.html> (last visited Jan. 15, 2010) (At the INFOSEC site, click on the COMPUSEC tools tab and scroll down to the anti-spyware link, second from the top. The servicemember can then save the software to a local hard drive to write on a CD-ROM or other portable media for home use. Users must be on a “.mil” workstation to download the software.).

¹⁰⁸ BIEGELMAN, *supra* note 1, at 300 (For example, Microsoft offers additional guidance for improving computer and network security at www.microsoft.com/security; additionally, Microsoft has a password checker to gauge the level of security for chosen passwords at www.microsoft.com/protect/yourself/password/checker.aspx.).

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² *Id.*

¹¹³ *Id.*

¹¹⁴ Privacy Rights Clearinghouse, *supra* note 42.

¹¹⁵ BIEGELMAN, *supra* note 1, at 301.

¹¹⁶ *Id.* at 300.

¹¹⁷ *Id.*

strangers and be sure to use the junk mail filter provided by most email services to eliminate mail from an unknown contact.¹¹⁸ In addition, banking and other financial institutions do not generally request personal information online.¹¹⁹ If a financial or other institution claims to require an update to personal information, the servicemember should contact the institution directly to check its legitimacy instead of responding.¹²⁰ Another common scam is to offer free software, vacations, electronics, or other prizes to obtain personal information for fraudulent uses.¹²¹ A good rule of thumb for dealing with this type of fraud is to remember that if it sounds too good to be true, it probably is.¹²²

Finally, when disposing of old computers, ensure servicemembers remove the hard drive and either smash or drill holes in it prior to reselling, donating, or discarding an old computer.¹²³ This is the best way to ensure thieves do not recover confidential information.¹²⁴ At a minimum, the servicemember should use a “wipe” utility program to overwrite the hard drive since reformatting or deleting may not completely erase personal information.¹²⁵

Place Fraud Alerts on Credit Reports and Consider Alternative Protections

Credit reports contain personal information, such as past and current addresses, whether someone has been sued or filed for bankruptcy, and how and when bills are paid.¹²⁶ The three credit reporting bureaus also sell personal information to creditors, employers, and other businesses that use the data to (among other things) evaluate credit, rental, and employment applications.¹²⁷ A fraud alert is a notification on a person’s credit report that requires creditors to contact the registrant and verify applications prior to approval.¹²⁸ When someone places a fraud alert on his credit report, consumer reporting companies also remove the person’s name from the marketing lists for prescreened offers of credit and insurance.¹²⁹

¹¹⁸ *Id.*; see also TAKE CHARGE, *supra* note 14, at 33.

¹¹⁹ BIEGELMAN, *supra* note 1, at 300.

¹²⁰ *Id.*

¹²¹ *Id.* at 300, 307.

¹²² *Id.* at 307.

¹²³ *Id.* at 300.

¹²⁴ *Id.*

¹²⁵ TAKE CHARGE, *supra* note 14, at 34.

¹²⁶ ‘ACTIVE DUTY’ ALERTS HELP PROTECT MILITARY PERSONNEL FROM IDENTITY THEFT 1 (July 2005) [hereinafter ‘ACTIVE DUTY’], available at <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt147.shtm>.

¹²⁷ *Id.*

¹²⁸ BIEGELMAN, *supra* note 1, at 308.

¹²⁹ ‘ACTIVE DUTY’, *supra* note 126; see also Identity Theft Memorandum, *supra* note 67 (servicemembers should also remove their name, phone

An initial fraud alert lasts for ninety days and is used when a person believes he is at risk for identity theft due to a lost wallet or other compromise.¹³⁰ Requesting a fraud alert entitles the consumer to additional free copies of credit reports, and if a compromise actually occurs, the initial fraud alert may be extended and remain in effect for seven years.¹³¹ If a servicemember is deployed he may also place an “active duty alert” on his credit report.¹³² An active duty alert is much like the initial alert except that it lasts for one year, unless early removal is requested.¹³³ A personal representative is also allowed to remove or place an active duty alert and it can be extended if the deployment exceeds one year.¹³⁴ Additionally, the servicemember may consider alternative protections such as using a credit freeze or paying for a credit account monitoring service.

Credit freezes are relatively new and expected to become a significant weapon used in the battle against identity theft.¹³⁵ Placing a credit freeze with the credit bureaus blocks a potential creditor from issuing new credit without obtaining express permission from that person.¹³⁶ The credit freeze also prevents the bureaus from issuing the servicemember’s credit score, which is essential information necessary before a business will extend new credit.¹³⁷ A credit freeze blocks the issuance of instant credit and is often seen by stores who offer big discounts on purchases when opening a new line of credit at the same time.¹³⁸

Monitoring services are companies the servicemember subscribes to that will notify clients via email, text, or telephone of any changes to the credit report such as credit inquiries or the opening of new accounts.¹³⁹ These companies will monitor the report for fraudulent activity and will even take action on the servicemembers behalf if

necessary.¹⁴⁰ Most of the services monitoring companies provide for a fee people can do themselves for free, but it requires servicemembers take time and be diligent in monitoring their own credit reports at least annually.¹⁴¹

How Do We Teach Servicemembers?

A key component to properly educating servicemembers rests with a good preventative law program. Individual legal problems negatively affect the unit’s combat readiness and cause low morale and disciplinary problems.¹⁴² Additionally, servicemembers may have security clearances suspended, possibly resulting in a suspension of duties, if they have negative credit issues resulting from being victimized.¹⁴³ Legal assistance attorneys responsible for implementing the preventative law program must act aggressively and think creatively when educating service members and their families on identifying potential legal issues like identity theft.¹⁴⁴ Identifying such issues early may prevent theft from occurring and will reduce the time and resources necessary to correct problems if they do occur.¹⁴⁵

Briefings concerning identity theft should concentrate mostly on prevention; however, the attorney should also cover the basics of repairing a problem. If time allows, the attorney should prepare and give a one-hour annual briefing on preventing identity theft and consider including the brief at training installations as part of in-processing. At a minimum, the attorney should include identity theft as a portion of an annual preventative law brief.

Additionally, since deployed servicemembers face a higher risk of being victims, the attorney should include information about identity theft in pre-deployment briefs.¹⁴⁶ Attorneys should also prepare and distribute a one-page handout providing information about identity theft and include the family members in briefings. These handouts should be available not only in legal service offices but also in other community offices such as the housing office, family services, or other high-traffic areas for families looking for assistance and information. Servicemembers and their families should be aware of the support and assistance they can receive from the legal office if

number, and home address from marketing lists by notifying the Direct Marketing Association: (1) DMA Mail Preference Service, P.O. Box 9008, Farmingdale, NY 11735-9008, <http://www.the-dma.org>; (2) DMA Telephone Preference Service, P.O. Box 9014, Farmingdale, NY 11735-9014, <http://www.the-dma.org> and call 1-888-5OPTOUT to stop delivery of pre-approved credit offers.).

¹³⁰ TAKE CHARGE, *supra* note 14, at 5.

¹³¹ BIEGELMAN, *supra* note 1, at 308; *see also* TAKE CHARGE, *supra* note 14, at 6.

¹³² MILITARY PERSONNEL AND FAMILIES FIGHTING BACK AGAINST IDENTITY THEFT 1 (n.d.), available at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth02.pdf> (last visited Jan. 13 2010).

¹³³ *Id.*

¹³⁴ *Id.*

¹³⁵ BIEGELMAN, *supra* note 1, at 308; *see also* TAKE CHARGE, *supra* note 14, at 309.

¹³⁶ *Id.*

¹³⁷ *Id.*

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² RICHARD A. GITTINS, *THE MILITARY COMMANDER & THE LAW* 347 (4th ed. 1996).

¹⁴³ Lynch, *supra* note 54.

¹⁴⁴ U.S. DEP’T OF HOMELAND SECURITY, COMDTINST 5801.4E, LEGAL ASSISTANCE PROGRAM 11 (26 Oct. 2005).

¹⁴⁵ GITTINS, *supra* note 142, at 339.

¹⁴⁶ Henson, *supra* note 45.

victimized, and attorneys should be trained and prepared to assist them in repairing the aftermath of identity theft.

Defense: Fixing the Problem

Even with an effective preventative law program, identity theft still occurs. Therefore, it is equally important to know what steps to take once a victim is identified. Sadly, in identity-theft cases, the victim often has to prove his or her innocence and the criminal is rarely prosecuted.¹⁴⁷ Victims of identity theft often face lingering repercussions that negatively affect their credit rating for years.¹⁴⁸ There are many different types of identity theft and related fraud that result in a variety of consequences and often require differing courses of action. This section outlines the most common types faced by military members.

Unauthorized Charges or Lines of Credit

The Fair Credit Billing Act (FCBA) limits liability to \$50 for fraudulent charges on a credit card if the servicemember properly handles the transaction.¹⁴⁹ If a servicemember finds an unauthorized charge on a credit card bill or an unrecognized line of credit in his name, the first step is to contact the creditor to report the incident and cancel the credit card.¹⁵⁰ A written log should be kept of all contact made with any agency that includes the name of the agency and person contacted, the agency phone number, date and time of contact, and synopsis of the conversation.¹⁵¹

The next step is to contact one of the credit reporting services and place a fraud alert on the servicemember's credit report.¹⁵² Only one call is necessary because the agency contacted is required to pass the information to the other two bureaus.¹⁵³ This will ensure that for at least ninety days, creditors will contact the servicemember prior to issuing credit to a possible thief or releasing credit information to requesting entities.¹⁵⁴ The servicemember should also obtain a police report documenting the theft as well as file a complaint with the FTC.¹⁵⁵ While the police

will generally not aggressively pursue the crime, the report will lend credibility to the claim and the credit card company may require it before removing the fraudulent charge or account.¹⁵⁶

After completing the initial steps, the servicemember should send a dispute letter to the creditor mailed to the address for "billing inquiries," not the address for mailing payments.¹⁵⁷ The letter must reach the company within 60 days after the creditor mailed the erroneous bill, so it is essential to send the dispute by certified mail with a return receipt as proof.¹⁵⁸

The servicemember also has the right to prevent the company from reporting the fraudulent information to the reporting agencies by sending a request,¹⁵⁹ along with an identity theft affidavit, to the proper address.¹⁶⁰ Be sure to maintain copies of all correspondence and follow up with the creditor if they have not responded in the required 30 days.¹⁶¹ While most credit card companies will accept notice via telephone and resolve the issue immediately for a fraudulent charge, it is always recommended to follow the above FBCA guidelines to ensure the servicemember's rights are protected.¹⁶²

Correcting Fraudulent Information on Credit Reports

The Fair Credit Reporting Act (FCRA) places the burden of correcting fraudulent credit report information on the credit bureaus and the reporting creditor.¹⁶³ As soon as a servicemember spots fraudulent information on a credit report, he should immediately contact the creditor and reporting agency to deny the transaction and place a fraud alert on his credit report.¹⁶⁴ The victim must complete an

complaints the FTC handles at <http://ftc.gov/multimedia/video/scam-watch/file-a-complaint.shtm>).

¹⁵⁶ *Id.*

¹⁵⁷ *Id.* at 19; *see also* Appendix D.

¹⁵⁸ TAKE CHARGE, *supra* note 14, at 19.

¹⁵⁹ *See* Appendix D (providing a sample dispute letter to a creditor to stop the company from reporting fraudulent, negative information to credit reporting agency).

¹⁶⁰ REMEDY THE EFFECTS OF IDENTITY THEFT 2 (n.d.), *available at* <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth09.pdf> (last visited Jan. 10, 2010); *see also* Appendix B (providing a sample of an identity theft affidavit, which is a form that details information about a specific fraud).

¹⁶¹ TAKE CHARGE, *supra* note 14, at 19.

¹⁶² *Id.* at 13.

¹⁶³ *Id.* at 17.

¹⁶⁴ *Id.*

¹⁴⁷ BIEGELMAN, *supra* note 1, at 177.

¹⁴⁸ *Id.*

¹⁴⁹ Truth in Lending Act, 15 U.S.C. § 1601(161)(e) (2006).

¹⁵⁰ BIEGELMAN, *supra* note 1, at 310.

¹⁵¹ TAKE CHARGE, *supra* note 14, at 11.

¹⁵² BIEGELMAN, *supra* note 1, at 310.

¹⁵³ TAKE CHARGE, *supra* note 14, at 5 (The credit reporting companies can be contacted at the following telephone numbers: Equifax 1-800-525-6285; Experian 1-888-Experian; and TransUnion 1-800-680-7289.).

¹⁵⁴ *Id.* at 6.

¹⁵⁵ *Id.* at 8 (Reports can be filed on the FTC website at www.ftc.gov/idtheft or by calling 1-877-IDTheft. The FTC is also releasing a new video showing how people can file a complaint, and offers examples of what

identity theft affidavit and a blocking letter¹⁶⁵ informing the reporting agency of the fraud.¹⁶⁶

Next, the victim should report the theft to local police and the FTC and include a copy of the police report with the affidavit and blocking letter.¹⁶⁷ Once the reporting agency receives the necessary paperwork, the servicemember can extend the 90-day fraud alert for up to seven years as necessary.¹⁶⁸ It is important to keep a file with any documentation and request all transaction paperwork from the reporting company and the debt collector if applicable.¹⁶⁹ As with any fraud issue, the servicemember should keep a detailed log of all contact made with agencies and send any correspondence by certified mail with a return receipt.¹⁷⁰ It is also important to follow-up with the reporting agency to ensure it removes the negative report and always maintain a file to show as proof if the agencies re-report the transaction.¹⁷¹

Fraudulent Electronic Bank Withdrawals

Unauthorized electronic transactions dealing with credit or banking is governed by the Electronic Fund Transfer Act.¹⁷² If a servicemember loses an ATM card, he must report the loss within two business days of discovery to limit his losses to \$50.¹⁷³ The liability to the consumer increases to \$500 if the loss is reported between two and sixty days of discovery and no limit exists if the missing card is reported after sixty days.¹⁷⁴ Most banks do not adhere to these strict rules and will generally cover the loss.¹⁷⁵ If the card is stolen, immediately report it to the police and keep a copy of the report.¹⁷⁶ The servicemember should also diligently check his bank records to spot any fraudulent transactions.¹⁷⁷

If the servicemember does find an unauthorized transaction, he should call the bank to report the fraud and send a dispute letter (as with the fraudulent credit card

transactions).¹⁷⁸ The institution will then investigate the erroneous transaction within 10 days but may take up to 45 days if necessary.¹⁷⁹ The bank must respond three days after completion of the investigation and remove the error one day later.¹⁸⁰

Fraudulent Checks or Bank Paper Transactions

Unlike electronic transactions, there is no federal law limiting a consumer's liability for fraudulent paper transactions, although state law may apply.¹⁸¹ If a thief fraudulently uses or counterfeits the servicemember's checks, the victim should immediately stop payment, close the account, and notify the check verification system used in these cases.¹⁸² The check verification system keeps retailers from honoring the checks, and will verify if other bank accounts were fraudulently opened in the servicemember's name.¹⁸³

Check verification systems can also provides a consumer report when requested, showing information about checking accounts.¹⁸⁴ The same procedures for correcting credit reports should be followed to correct the consumer report if errors exist.¹⁸⁵ If the bank is not assisting the servicemember with the fraud, he should contact the overseeing federal or state agency that regulates banking operations.¹⁸⁶ The consumer should also contact the business where the thief passed the bad check to ensure they do not send the bill to collections or submit a negative report to the credit reporting agencies.¹⁸⁷

Correcting a Criminal Record

While correction procedures may vary according to state, there are general guidelines to follow if wrongful, criminal

¹⁶⁵ See Appendix C (providing a sample blocking letter to a credit reporting agency).

¹⁶⁶ TAKE CHARGE, *supra* note 14, at 17.

¹⁶⁷ *Id.* at 8.

¹⁶⁸ *Id.* at 6.

¹⁶⁹ *Id.* at 10.

¹⁷⁰ *Id.*

¹⁷¹ *Id.*

¹⁷² Electronic Funds Transfer, 15 U.S.C. § 1693 (901) (b) (2006).

¹⁷³ TAKE CHARGE, *supra* note 14, at 13.

¹⁷⁴ *Id.*

¹⁷⁵ *Id.*

¹⁷⁶ *Id.* at 8.

¹⁷⁷ *Id.* at 27.

¹⁷⁸ *Id.* at 13; see also Appendix D (providing a sample dispute letter).

¹⁷⁹ TAKE CHARGE, *supra* note 14, at 13.

¹⁸⁰ *Id.*

¹⁸¹ *Id.* at 14.

¹⁸² *Id.* at 14–15 (Chex Systems, Inc. is a company used to report fraud to retailers to prevent them from honoring stolen checks and may be contacted at 1-800-428-9623; other such reporting agencies include TeleCheck at 1-800-710-9898; and Certegy at 1-800-437-5120. A company called SCAN will assist in finding out if a thief is passing bad checks in your name and may be contacted at 1-800-262-7771.).

¹⁸³ *Id.*

¹⁸⁴ *Id.* at 15.

¹⁸⁵ *Id.*

¹⁸⁶ *Id.* (To contact the FDIC call 877-ASKFDIC (877-275-3342). The FDIC Call Center will direct your call.).

¹⁸⁷ *Id.*

violations are recorded using the servicemember's name.¹⁸⁸ First, the victim should contact the police department or court agency where the arrest occurred or warrant was issued.¹⁸⁹ The servicemember should confirm his identity and immediately file an impersonation report with the department or court.¹⁹⁰ This is usually done by having the law enforcement agency take fingerprints and a current photograph, and by providing copies of all identifying documents for comparison with the imposter.¹⁹¹ If the arrest warrant or incident occurred far from home, solicit assistance from the local police department in filing the impersonation report and identification.¹⁹²

Once the department is satisfied with the proof provided, it should issue a clearance letter or certificate of release that should remain in the servicemember's possession at all times.¹⁹³ The next step is to request the police department file the appropriate paperwork proving the servicemember's innocence with the district attorney's office or court, resulting in an amended complaint.¹⁹⁴ The victim may also request the name of the perpetrator be changed to the actual criminal or to John or Jane Doe if unknown, with their own name as an alias.¹⁹⁵ Finally, the servicemember will need to contact the district attorney's office for the correct paperwork necessary to regain his good name.¹⁹⁶ Experts also recommend checking with the Department of Motor Vehicles (DMV) for fraudulent use of a servicemember's driver's license and request the DMV flag the file for possible fraud.¹⁹⁷

Conclusion

Servicemembers need and deserve special consideration and assistance with respect to identifying and combating identity theft. As judge advocates, it is our responsibility to educate military members and ensure commanders know that we can equip their unit to detect, deter, and defend against identity theft, thereby improving combat readiness. To do so, we need to conduct initial, annual, and pre-deployment training for all servicemembers on the dangers of complacency; how to stay vigilant; what thieves are looking for; how to keep criminals from obtaining their personal information; and, what steps to take if servicemembers or their families become victims. Servicemembers sacrifice many things in support of their country and the mission, but their good names should not be one of them.

¹⁸⁸ *Id.* at 20.

¹⁸⁹ *Id.*

¹⁹⁰ *Id.* (An impersonation report is a specific police report confirming the wrongful use of another's identity.).

¹⁹¹ *Id.* at 21.

¹⁹² *Id.*

¹⁹³ *Id.*

¹⁹⁴ *Id.*

¹⁹⁵ *Id.* at 17.

¹⁹⁶ *Id.* at 20.

¹⁹⁷ *Id.* at 21.

Appendix B

ID Theft Affidavit

Name _____ Phone number _____ Page 1

Victim Information

(1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as:

(First) (Middle) (Last) (Jr., Sr., III)

(3) My date of birth is _____
(day/month/year)

(4) My Social Security number is _____

(5) My driver's license or identification card state and number is _____

(6) My current address is _____

City _____ State _____ Zip Code _____

(7) I have lived at this address since _____
(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was _____

City _____ State _____ Zip Code _____

(9) I lived at the address in Item 8 from _____ until _____

(10) My daytime telephone number is (_____) _____

My evening telephone number is (_____) _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

How the Fraud Occurred

Check all that apply for items 11 - 17:

(11) I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

(12) I did not receive any benefit, money, goods, or services as a result of the events described in this report.

(13) My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were stolen lost on or about _____ (day/month/year).

(14) To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

Name (if known)

Name (if known)

Address (if known)

Address (if known)

Phone number(s) (if known)

Phone number(s) (if known)

Additional information (if known)

Additional information (if known)

(15) I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.) _____

(Attach additional pages as necessary.)

Victim's Law Enforcement Actions

(17) (check one) I am am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18) (check one) I am am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (check all that apply) I have have not reported the events described in this affidavit to the police or other law enforcement agency. The police did did not write a report. In the event you have contacted the police or other law enforcement agency, please complete the following:

(Agency #1) (Officer/Agency personnel taking report)

 (Date of report) (Report number, if any)

 (Phone number) (email address, if any)

(Agency #2) (Officer/Agency personnel taking report)

 (Date of report) (Report number, if any)

 (Phone number) (email address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

(21) Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

(22) A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith. I also understand that this affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. §1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

Signature

Date Signed

_____ (Notary) [Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

(signature)

(printed name)

(date)

(telephone number)

Fraudulent Account Statement

Completing This Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below.**
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original). **Completing this Statement**

I declare (check all that apply):

As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor/Name and address (the company that opened the account or provided the goods and services)	Account number	Types of unauthorized credit/goods/services provided by creditor (if known)	Date issued or opened (if known)	Amount/ Value provided (the amount charged or the cost of the goods/ services)

During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address _____

Account number _____

Appendix C

Sample Blocking Letter to Reporting Company

Date
Your Name
Your Address
Your City, State, Zip Code

Complaint Department
Name of Consumer Reporting Company
Address
City, State, Zip Code

Dear Sir or Madam:

I am a victim of identity theft. I am writing to request that you block the following fraudulent information in my file. This information does not relate to any transaction that I have made. The items are also circled on the attached copy of the report I received. (Identify item(s) to be blocked by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)

Enclosed is a copy of the law enforcement report regarding my identity theft. Please let me know if you need any other information from me to block this information on my credit report.

Sincerely,

Your name

Enclosures: (List what you are enclosing.)

Appendix D

Sample Dispute Letter to Creditor

Date
Your Name
Your Address
Your City, State, Zip Code

Complaint Department
Name of Consumer Reporting Company
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute a fraudulent (charge or debit) on my account in the amount of \$_____. I am a victim of identity theft, and I did not make this (charge or debit). I am requesting that the (charge be removed or the debit reinstated), that any finance and other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as a police report) supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.

Sincerely,

Your name

Enclosures: (List what you are enclosing.)

Appendix E

Sample Chart of Course of Action

CHART YOUR COURSE OF ACTION

Use this form to record the steps you've taken to report the fraudulent use of your identity. Keep this list in a safe place for reference.

NATIONWIDE CONSUMER REPORTING COMPANIES — REPORT FRAUD

BANKS, CREDIT CARD ISSUERS, AND OTHER CREDITORS (Contact each creditor promptly to protect your legal rights.)

LAW ENFORCEMENT AUTHORITIES — REPORT IDENTITY THEFT

Creditor	Address/Phone Number	Date Contacted	Contact Person	Comments

Agency/department	Phone Number	Date Contacted	Contact Person	Report Number	Comments

Consumer Reporting Company	Phone Number	Date Contacted	Contact Person	Comments
Equifax	1.800.525.6285			
Experian	1.888.EXPERIAN (397.3742)			
TransUnion	1.800.680.7289			