LEGAL BRIEF
IDENTITY THEFT

February 2018

PREPARED BY
NELLIS LAW CENTER, 4428 England Ave (Bldg 18), Nellis AFB, Nevada 89191-6505
702-652-2479

An identity thief steals some piece of your personal information and uses it without your knowledge to commit fraud or theft. An all-too-common example is when an identity thief uses your personal information to open a credit card account in your name.

While you cannot completely prevent identity theft from occurring, you can minimize your risk by managing your personal information wisely, cautiously, and with heightened sensitivity.

If you've been a victim of identity theft, you can call the Federal Trade Commission's (FTC) Identity Theft Hotline toll free at 1-877-IDTHEFT (438-4338). The FTC puts your information into a secure consumer fraud database and may, in appropriate instances, share it with other law enforcement agencies and private entities, including any companies about which you may complain. Visit www.consumer.gov/idtheft for more information.

In addition, the FTC has developed an ID Theft Recovery Plan - for information visit https://identitytheft.gov.

IF YOU'RE A VICTIM

Sometimes an identity thief can strike even if you've been very careful about keeping your personal information to yourself. If you suspect that your personal information has been stolen and misused to commit fraud or theft, take action immediately, and keep a record of your conversations and correspondence. Exactly which steps you should take to protect yourself depends on your circumstances. However, four actions are appropriate in almost every case.

YOUR FIRST FOUR STEPS

1. Place a fraud alert on your credit reports and review your credit reports.
Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of one of the three consumer reporting companies below to place a fraud alert on your credit report. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.
Equifax: 1-888-766-0008; www.equifax.com
Experian: 1-888-397-3742; www.experian.com
TransUnion: 1-800-680-7289; www.transunion.com

You are entitled to a free credit report every 12 months. Visit www.annualcreditreport.com or call 1-877-322-8228 to obtain your free report. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like your Social Security Number (SSN), address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. See Disputing Errors on Credit Reports at http://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports to learn how. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, use the FTC sample letter (http://www.consumer.ftc.gov/articles/0384-sample-letter-disputing-errors-your-credit-report) to dispute the fraudulent charges or debits. Write to the company at the address given for "billing inquiries," NOT the address for sending your payments.
- For new unauthorized accounts, you can either file a dispute directly with the company or file a report with the police and provide a copy, called an "Identity Theft Report," to the company.
    - If you want to file a dispute directly with the company and do not want to file a report with the police, ask if the company accepts the FTC's ID Theft Affidavit (https://www.ok.gov/osbi/documents/FTC%20Identity%20Theft%20Affidavit.pdf). If it does not, ask the representative to send you the company's fraud dispute forms.
    - However, filing a report with the police and then providing the company with an Identity Theft Report will give you greater protection. For example, if the company has already reported these unauthorized accounts or debts on your credit report, an Identity Theft Report will require them to stop reporting that fraudulent information.

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

3. File a complaint with the Federal Trade Commission.
You can file a complaint with the FTC using the online complaint assistant (https://www.ftccomplaintassistant.gov), or call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261. Be sure to call the Hotline to update your complaint if you have any additional information or problems.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

Additionally, you can provide a printed copy of your online complaint to the police to incorporate into their police report. The printed FTC ID theft complaint, in conjunction with the police report, can constitute an Identity Theft Report and entitle you to certain protections. This Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit report; (3) prevent a company from continuing to collect debts that result from identity theft; and (4) place an extended fraud alert on your credit report.

4. File a report with your local police or the police in the community where the identity theft took place.

Call your local police department and tell them that you want to file a report about your identity theft. Ask them if you can file the report in person. If you cannot, ask if you can file a report over the Internet or telephone. If the police are reluctant to take your report, ask to file a "Miscellaneous Incident" report or try another jurisdiction such as your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft.

When you go to your local police department to file your report, bring a printed copy of your FTC ID theft complaint and your supporting documentation. Ask the officer to attach or incorporate the ID theft complaint into their police report. Tell them that you need a copy of the Identity Theft Report (the police report with your ID theft complaint attached or incorporated) to dispute the fraudulent accounts and debts created by the identity thief. In some jurisdictions the officer will not be able to give you a copy of the official police report but should be able to sign your complaint and write the police report number in the "Law Enforcement Report" section.

YOUR NEXT STEPS

Although there's no question that identity thieves can wreak havoc on your personal finances, there are some things you can do to take control of the situation. For example:

- **Stolen Mail:** If an identity thief has stolen your mail to get new credit cards, bank and credit card statements, pre-screen credit offers or tax information, or if an identity thief has falsified change-of-address forms, that's a crime. Report it to your local postal inspector. Contact your local post office for the phone number for the nearest postal inspection service office or check the Postal Service website at www.usps.gov.

- **Change of address on credit card accounts:** If you discover that an identity thief has change the billing address on an existing credit card account, close the account. When you open a new account, ask that a password be used before any inquiries or changes can be made on the account.

- **Bank Accounts:** If you have reason to believe that an identity thief has tampered with your bank accounts or check or ATM card, close the accounts immediately. When you open new accounts, insist on password-only access to minimize the chance that an identity thief can violate the accounts.

  In addition, if your checks have been stolen or misused, stop payment. You can contact the following major check verification companies to learn more about the services they provide in helping you tract your stolen or misused checks.

  SCAN: 1-800-262-7771
  Telecheck: 1-800-927-0188
  CrossCheck: 1-800-552-1900

- **Investments:** If you believe that an identity thief has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager and to the Securities and Exchange Commission

  You can file a complaint with the SEC by visiting the Complaint Center at http://www.sec.gov/complaint.shtml. Be sure to include as much detail as possible. If you do not have access to the internet, write to the SEC at: SEC, Office of Investor Education and Advocacy, 100 F Street NE, Washington, D.C. 20549-0213, or call 800-732-0330.

- **Phone Services:** If an identity thief has established new phone service in your name, is making unauthorized calls that seem to come from – and are billed to – your cellular phone, or is using your calling card and PIN, contact your service provider immediately to cancel the account and/or calling card. Open new accounts and chose new PIN's.

  If you are having trouble getting fraudulent phone charges removed from your account, contact your state Public Utility Commission for local service providers or the Federal Communications Commission for long-distance service providers and cellular providers at https://www.fcc.gov/consumers/guides/filing-informal-complaint or 1-888-CALL-FCC.

- **Employment:** If you believe someone is using your SSN to apply for a job or to work, that's a crime. Report it to the SSA's Identity Protection Hotline at 1-800-908-4490. Also call SSA at 1-800-772-1213 or go to http://www.socialsecurity.gov/myaccount/ to verify the accuracy of the earnings reported on your SSN and to request a copy of your *Social Security Statement.*

- **Driver's License:** If you suspect that your name or SSN is being used by an identity thief to get a driver's license or a non-driver's ID card, contact your Department of Motor Vehicles. If your state uses your SSN as your driver's license number, ask to substitute another number.

- **Bankruptcy:** If you believe someone has filed for bankruptcy using your name, write to the U.S. Trustee in the Region where the bankruptcy was filed. A listing of the U.S. Trustee Program's Regions can be found at http://www.justice.gov/ust/eo/ust_org/office_map.htm or you can send the letter to Executive Office for U.S. Trustees, Office of Criminal Enforcement, 441 G Street, NW, Suite 6150, Washington, DC 20530

  Your letter should include:
  - Name and address of the person or business you are reporting.
  - The name and number of the bankruptcy case and the location of where it was filed.
  - Any identifying information you may have regarding the individual or the business.
  - A brief description of the alleged fraud, including how you became aware of the fraud and when the fraud took place. Please include all supporting documentation.
  - Identify the type of asset that was concealed and its estimated dollar value, or the amount of any unreported income, undervalued asset, or other omitted asset or claim.
  - Your name, address, telephone number, and email address.
  - You are not required to identify yourself, though it is often helpful if questions arise.

  The U.S. Trustee, if appropriate, will make a referral to criminal law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the U.S. Attorney and/or the FBI in the city where the bankruptcy was filed.

- **Criminal records/arrests.** In rare instances, an identity thief may create a criminal record under your name. For example, your imposter may give your name when being arrested. If this happens to you, you may need to hire an attorney to help resolve the problem. The procedures for clearing your name vary by jurisdiction.

MINIMIZING RISK

While nothing can guarantee that you won't become a victim of identity theft, you can minimize your risk and minimize the damage if a problem develops by making it more difficult for identity thieves to access your personal information.

Protect your SSN
Don't carry your Social Security card in your wallet or write your SSN on a check. Give your SSN only when absolutely necessary, and ask to use other types of identifiers. If your state uses your SSN as your driver's license number or if your health insurance company uses your SSN as your policy number, ask to substitute another number.

Your employer and financial institutions will need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your SSN for general record keeping. If someone asks for your SSN, ask:

- Why do you need my SSN?
- How will my SSN be used?
- How do you protect my SSN from being stolen?

- What will happen if I don't give you my SSN?

If you don't provide your SSN, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to these questions will help you decide whether you want to share your SSN with the business. The decision to share is yours.

Treat your trash and mail carefully
To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, always shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.

Deposit your outgoing mail containing personally identifying information in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, contact the U.S. Postal Service at 1-800-275-8777 or online at https://holdmail.usps.com/holdmail/, to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it.

Be on guard when using the Internet
The Internet can give you access to information, entertainment, financial offers, and countless other services, but at the same time, it can leave you vulnerable to online scammers, identity thieves and more. For practical tips to help you be on guard against Internet fraud, secure your computer, and protect your personal information, visit www.OnGuardOnline.gov.

Select intricate passwords
Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother’s maiden name, your birth date, the last four digits of your SSN or your phone number, a series of consecutive numbers, or a single word that would appear in a dictionary. Combinations of letters, numbers, and special characters make the strongest passwords. When opening new accounts, you may find that many businesses still ask for your mother’s maiden name. Find out if you can use a password instead.

Verify a source before sharing information
Don’t give out personal information on the phone, through the mail, or on the Internet unless you’ve initiated the contact and are sure you know who you’re dealing with. Identity thieves are clever and may pose as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their SSN, mother’s maiden name, account numbers, and other identifying information.

Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization’s website by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or call customer service using the number listed on your account statement or in the telephone book.

Safeguard your purse and wallet
Protect your purse and wallet at all times. Don't carry your SSN or card; leave it in a secure place. Carry only the identification information and the credit and debit cards that you'll actually need when you go out.

Store information in secure locations
Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house. Share your personal information only with those family members who have a legitimate need for it. Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.
Ask about information security procedures in your workplace or at businesses, doctor's offices, or other institutions that collect your personally identifying information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.

About identity theft insurance
Although identity theft insurance won't deter identity thieves, it can, in certain circumstances, minimize losses if an identity theft occurs. As with any product or service, as you consider whether to buy, be sure you understand what you'd be getting. Things to consider include: (1) the amount of coverage the policy provides; (2) whether it covers any lost wages (and, if so, whether there's a cap on the wages you can claim, or a separate deductible); (3) the amount of the deductible; (4) what might be excluded (for example, if the thief is a family member or if the thief made electronic withdrawals and transfers); (5) whether the policy provides a personal counselor to help you resolve the problems of identity theft; and (6) whether your existing homeowner's policy already contains some coverage. Be aware that one of the major "costs" of identity theft is the time you will spend to clear your name. Also be aware that many companies and law enforcement officers will only deal with you (as opposed to an insurance company representative). So, even if your policy provides you with a personal counselor, that counselor can often only guide you, as opposed to doing the work to clear your name. And, as you evaluate insurance products and services, you may also consider checking out the insurer with your local Better Business Bureau, consumer protection agency and state Attorney General.

CHOOSING TO SHARE YOUR PERSONAL INFORMATION – OR NOT
What happens to the personal information you provide to companies, marketers, and government agencies? They may use your information just to process your order. They may use it to create a profile about you and then let you know about products, services, and promotions, or they may share your information with others. More organizations are offering consumers choices about how their personal information used. For example, many let you "opt out" of having your information shared with others for promotional purposes.

Pre-Screened Credit Offers
If you receive pre-screen credit card offers in the mail (namely those based upon your credit data), don't tear them up after you decide you don't want to accept the offer, identity thieves may retrieve the offers for their own use without your knowledge.

To opt out of receiving pre-screened credit card offers, visit www.optoutprescreen.com or call: 1-888-5-OPT-OUT (1-888-567-8688). The three major credit bureaus use the same toll-free number to let consumers choose not to receive pre-screened credit offers. Note: You will be asked to provide your SSN which the consumer reporting companies need to match you with your file.

Departments of Motor Vehicles
Take a look at your driver's license. All the personal information on it – and more – is on file with your state Department of Motor Vehicles (DMV). A state DMV may distribute your personal information for law enforcement, court proceedings and insurance underwriting purposes but may not distribute it for direct marketing without your express consent. Contact your state DMV for more information.

Not every DMV distributes personal information for direct marketing or other purposes. You may be able to opt out if your state DMV distributes personal information for these purposes. Contact your state DMV for more information.

Federal Laws
The federal government and numerous states have passed laws that address identity theft.

The Identity Theft and Assumption Deterrence Act, enacted by Congress in October 1998 (and codified, in part, at 18 U.S.C. Section 1028) is the federal law direct at identity theft. Violations of the Act are investigated by the federal enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and SSA's Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

In most instances, a conviction for identity theft carries a maximum penalty of 15 years imprisonment, a fine, and forfeiture of any personal property used or intended to be used to commit the crime. Schemes to commit identity theft or fraud also may involve violations of other statutes, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud, or Social Security fraud. Each of these federal offenses is a felony and carries substantial penalties – in some cases, as high as 30 years in prison, fines, and criminal forfeiture.

State Laws
Many states have passed law related to identity theft; others may be considering such legislation. Where specific identity theft laws do not exist, the practices may be prohibited under other laws. Contact your State Attorney General's office or local consumer protection agency to find out whether your state has laws related to identity theft.

THE INFORMATION CONTAINED IN THIS PAMPHLET IS OF A GENERAL NATURE AND IS PROVIDED FOR YOUR ASSISTANCE AND CONVENIENCE. IT IS NOT INTENDED AS LEGAL ADVICE AND IS NOT A SUBSTITUTE FOR LEGAL COUNSEL. IF YOU HAVE ANY QUESTIONS AS TO HOW THE LAW IN THIS AREA AFFECTS YOU OR YOUR LEGAL RIGHTS, CONTACT A CIVILIAN ATTORNEY OR THE NELLIS AIR FORCE BASE LEGAL OFFICE FOR AN APPOINTMENT WITH A LICENSED ATTORNEY.