# Nevada Identity Theft Program

The program, designed by the state Legislature, assists identity theft victims in the recovery process by providing a new and effective card to demonstrate that their identity has been stolen. The program can assist Nevadans with restoring credit and avoiding improper criminal charges.

To be eligible for a Nevada Identity Theft Card, a victim must first file a police report with local law enforcement and ask for a brochure and application for the card. To file a police report, you will need proof of your identity and Social Security number.

After completing the application process, a victim may receive a secured, personalized identification card that can be used to alert law enforcement and creditors about fraudulent activity.

For more information or questions about the Nevada Identity Theft Program, please call 1-877-213-5227 or email PIU@ag.nv.gov.



## Filing a Consumer Complaint

Are you a victim of fraud, deception or an unfair business practice?

The Office of the Attorney General wants to hear from you.

Complaint forms are available on our website at <u>ag.nv.gov</u> or in print form at any one of our office locations. Forms are available in both English and Spanish, and can be completed online or in-person. Please include any appropriate documentation to support the complaint. All complaints must be signed by the complainant.

Please note that the Office of the Attorney General cannot provide you with legal advice or represent you in personal legal actions. If you feel you need to hire a private attorney, you may consider contacting your local legal aid office.

### Contact Us

Carson City Office 100 North Carson Street Carson City, Nevada 89701-4717 P: 775-684-1100 / F: 775-684-1108

Las Vegas Office 555 E. Washington Avenue Suite 3900 Las Vegas, Nevada 89101 P: 702-486-3420 / F: 702-486-3768

Preventing Identity Theft Office of the Nevada **Attorney General** AARON D. FORD

Attorney General

What is identity theft? Identity theft is the use of another individual's personal identifying information with the intent to fraudulently obtain credit, property or services. Nevada's identity theft law takes into account computer and Internet technology, and makes it a crime to aid or abet another person in securing this personal identifying information. Identity theft is a crime at both the state and federal levels.

#### Warning Signs

•You see withdrawals from your bank account that you can't explain.

- •You don't receive your bills or other mail.
- •Merchants refuse your checks.
- •Debt collectors call you about debts that aren't yours.
- •You find unfamiliar accounts or charges on your credit report.
- •Medical providers bill you for services you didn't use.
- •Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- •A health plan won't cover you because your medical records show a condition you don't have.
- •The IRS notifies you that more than one tax return was filed in your name.
- •You receive notice that your information was compromised by a data breach at a company where you do business or have an account.

#### What to Do

If you have experienced any of these warning signs, act quickly. Taking these steps will help you limit the damage. Visit <u>IdentityTheft.gov</u> to report identity theft and create a personal recovery plan.

- Call the companies where you believe fraud occurred.
- File a report with your local police department.
- Place a fraud alert on your credit reports and request copies of your report.
- Report identity theft to the Federal Trade Commission.

<u>IdentityTheft.gov</u> can assist with step-by-step instructions specific to your situation.

If your information is lost or stolen, <u>IdentityTheft.gov</u> will also outline the specific steps you can take to help protect yourself from identity theft in the future.

#### Protecting Your Identity

Make protecting your identity a part of your everyday routine by following these steps:

•Read your credit card and bank statements carefully and often.

Know your payment due dates. If a bill doesn't show up when you expect it, look into it.
Read the statements from your health insurance plan. Make sure the claims paid match the care you received.

Shred any documents with personal and financial information. These items should be shredded immediately: sales receipts, ATM receipts, paid credit card statements, paid utility bills, credit offers, cancelled checks that aren't tax-related, and expired warranties.
Review each of your three credit reports at least once a year. Visit <u>annualcreditreport.com</u> to get your free reports.

For more information, visit <u>ftc.gov/idtheft</u>.

What do thieves do with your information? They can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can also file a tax refund in your name and get your refund.

#### Securing Online Info

- Don't give out personal information on the phone, through mail or over the Internet, unless you know who you're dealing with.
  Before disposing of a computer/mobile device, wipe all personal information.
  Use strong passwords with your laptop, credit, bank and other accounts.
- •Don't overshare on social networking sites. A thief can find information about your life and use it to access your accounts.

#### Securing Offline Info

Lock your financial documents in a safe place at home, and keep your wallet safe at work.
Leave your Social Security card at home.
Before sharing personal information, ask why it is needed, how it will be safeguarded, and the consequences of not sharing.

•Promptly remove mail that arrives in your mailbox. If you won't be home for several days, request a vacation hold on your mail. •When ordering new checks have them mailed

•When ordering new checks, have them mailed to a secure location.

#### Securing Your Devices

•Install anti-virus software, anti-spyware software and a firewall. Update them often.

- •Don't open files, click on links or download programs sent by strangers.
- Keep financial information on your laptop only when necessary. Don't use an automatic login feature, and always log off when you're finished.
  Avoid sending personal information over your laptop or smartphone on an unsecured public wireless network.