Fast Facts 24
Identity Theft

STATE OF CALIFORNIA
DMV
Department of Motor Vehicles

Identity theft and identity fraud are two of the fastest growing crimes in the United States (U.S.).

Driver's license (DL) and identification (ID) cards are the primary means of identification in California, making them targets for identity fraud. The Department of Motor Vehicles (DMV) is doing everything possible to protect your identity.

This brochure provides identity theft victims with important information to protect their identity.

What Is Identity Theft?

Identity theft is taking someone else's personal information (such as the DL/ID card number, social security number [SSN], bank or credit card account numbers, etc.). An imposter can use your identity to open fraudulent credit accounts, secure loans for cars and housing, or steal money from your bank accounts. It is a serious crime with serious consequences.

How Do Thieves Get Your Information?

Thieves can get your information by:

- Looking through your trash for bills or other documents with your personal information.
- Stealing your mail or wallet.
- Stealing your credit or debit card number by using "false fronts" attached to the front of ATM devices.
- Listening to conversations you have in public.
- Tricking you into giving them information by phone or email.
- Obtaining your information on the Internet or from someone who stole it.
- Stealing your information from a loan or credit application, customer file, hospital, bank, school, or business dumpster.
- Hacking into your personal computer or phone equipment.
- Accessing your personal information (such as a friend, relative, roommate, coworker, or employee).

Prevention Tips:

- Double-check your name and address on all DMV documents and tell a DMV representative if you have moved or if your address is incorrect.
- If you recently applied for a DL/ID card and did **not** receive it within 60 days, call 1-800-777-0133 to find out why. Sometimes, these are stolen from mailboxes.
- Avoid putting additional personal information, such as your DL/ID number, middle name, or telephone number, on your checks. Store checks in a safe place.
- Store your personal information in a secure place at home (especially if you have roommates) before you employ outside help or have work done on your house.
- Before placing credit card or ATM receipts, bank account or credit card statements, and unsolicited credit card offers in the trash, shred them (a crosscut shredder works best).
- Do **not** use public trash cans to discard forms or papers that contain personal identifying information (PII).
- Reduce the number of preapproved credit offers you receive by calling 1-888-5OPT OUT (567-8688).
- Put passwords on your accounts instead of using your mother's maiden name.
- Do not carry your SSN in your wallet. If you have cards that use your SSN, such as health plans or bank accounts, ask for another number. Never give your SSN unless there is a legitimate reason to do so.
- Carry only the minimum amount of identifying information and only one credit card in case your wallet is lost or stolen.
- Always take your receipts for credit card and ATM transactions.
- Never give out personal information on the phone unless you initiated the call.
- Use a locked mailbox to send and receive mail.
- Never click on links sent in unsolicited emails. Protect your personal information on your computer with strong passwords. Use a firewall and virus/spyware protection software that is updated regularly.
- Before you discard your old computer, use secure deletion software to permanently erase your hard drive data or physically destroy your hard drive. Utilize an e-waste facility to recycle your computer and cell phones.
- Pay attention to your billing cycles and statements. If you do **not** receive a statement, call the bank or issuing company. Report unauthorized charges or withdrawals immediately.
- Monitor and review your credit report. You may request a free credit report once every 12 months from each of the three major consumer credit reporting companies: Equifax, Experian, and TransUnion. Visit **annualcreditreport.com** or call 1-877-322-8228 for more information.

Disclaimer: *This brochure is for informational purposes only and should not be construed as legal advice or as the policy for the California Department of Motor Vehicles. If you want advice on a particular case, contact an attorney or other expert.*

What Is DMV Doing to Secure My Identity?

DMV takes the following measures to ensure your identity is secure:

- DMV employees are continuously trained on fraudulent document detection.
- Customers applying for a California DL/ID card for the first time must provide a birth verification/legal presence document, SSN, and residency document(s). At the application and payment window, your fingerprint is captured electronically and stored. The fingerprint provided when your photo is taken is compared to the first fingerprint taken to make sure you are the same person who started the application. This ensures that anyone attempting to access your record will **not** be able to do so.
- When you renew a DL/ID card in a DMV field office, your fingerprint is captured when your application and payment are processed and compared with the fingerprint stored on your record. The DMV technician also verifies your personal information and photo on the DMV database. If a new photo is taken, your fingerprint taken at the photo station is compared with the fingerprint captured at the time of application and payment. These precautions assist DMV in ensuring fraud does not occur on your record.
- Registered owner(s) requesting a replacement title (ownership certificate) or license plates for a vehicle must provide a California DL/ID card to prove their identity.
- Companies licensed by DMV, such as auto dealerships or driving schools, are audited regularly to ensure their compliance with the law.
- DMV verifies legal presence documents issued by the U.S. Citizenship and Immigration Service (USCIS), a Bureau of the Department of Homeland Security.
- DMV electronically verifies the SSN with the Social Security Administration.
- A DL/ID card will **not** be issued until the information provided is verified.

Important: DMV uses your SSN for identification purposes. It is not released to anyone unless required by law (*Vehicle Code* §1653.5).

What if I Become a Victim of Identity Fraud?

If you discover you have become a victim of identity fraud or theft of your DL/ID card, immediately contact DMV for an appointment. At the time of your appointment, be prepared to:

- Complete a statement describing the facts of the fraud.
- Submit a copy of the police report or a written explanation of why a police report was **not** filed.
- Submit copies of canceled checks, bills, or letters from companies or banks indicating the fraud.

In addition, you need to prove your identity. Except for an expired California DL/ID card, only valid, unexpired documents are acceptable to prove your identity. The following is a partial list of acceptable documents:

- California DL/ID card
- U.S. Birth Certificate or U.S. Passport
- U.S. Certificate of Birth Abroad or Report of Birth Abroad of U.S. Citizen
- Certification of Citizenship
- Certification of Naturalization
- Permanent Resident Card
- U.S. Military ID

California DL/ID Card Theft/Fraud

To report a complaint, go to Filing a Complaint for Unlawful Activities at dmv.ca.gov/invcf.

Additional Contacts

The following are additional bureaus or agencies you may contact if you are a victim of identity theft:

Equifax
equifax.com
PO Box 740241
Atlanta, GA 30374
1-800-525-6285

Experian
experian.com
1-888-397-3742

Trans Union
transunion.com
Fraud Victim Assistance Division
PO Box 6790
Fullerton, CA 92834
1-800-680-7289

U.S. Federal Trade Commission
ftc.gov/idtheft
1-877-ID-THEFT (438-4338);
TTY 1-866-653-4261, or write to:

Identity Theft Clearing House
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580

Social Security Administration
ssa.gov
1-800-772-1213 or TTY 1-800-325-0778

Privacy Enforcement and Protection Unit
oag.ca.gov/privacy

Your local law enforcement