

Prevention

Protecting yourself from fraud starts with prevention. Steps you can take:

- Take your outgoing mail to a U.S. Post Office instead of placing in your home mailbox, especially if the letter contains a check, gift cards, or cash. Report any unusual activity to the Postal Inspector through your local post office. If you need to report fraud related to the U.S. Mail or an unauthorize change of address, you can file a report with the U.S. Postal Inspection Service at www.uspis.gov/report/.
- Use online banking and review frequently to detect any potential fraud. Check if your bank offers text/email alerts on transactions.
- Change passwords on bank accounts and email accounts if you have been a victim of ID theft.
 Set up preset spending text alerts from bank.
- Set up an account with IRS.gov to prevent fraud related to your tax returns. Visit www.irs.gov/ payments/your-online-account to set up an ID.ME account. Even if you don't often utilize the account, you can prevent a criminal from fraudulently creating an IRS account in your name.

Additional Information

If you have been a victim of ID Theft, contact the credit bureaus. You can obtain a credit report, place, or manage a credit freeze, add a fraud alert, and file disputes on accounts.

You can get a free copy of your credit report at each nationwide credit bureau once every 12 months from www.annualcreditreport.com.

Equifax.com Experian.com TransUnion.com 800-525-6285 888-397-3742 800-680-7289

If your personal identifying information (PII) was used to open a bank account, you may consider filing a report with **ChexSystems** to dispute any fraudulent transactions. Visit www. chexsystems.com. If a criminal tries to open a new bank account using your name and personal identifiable information (PII), a security freeze with ChexSystems may help prevent the fraudulent account from being established. Learn more at www.chexsystems.com/security-freeze/information.

You should file a report with the **FBI's Internet Crimes Complaint Center** (IC3) at www.ic3.gov. Trained analysts at IC3 review and research the complaints, disseminating information to federal, state, local, or international law enforcement as appropriate. Please read the FAQs tab under "Site Navigation" on the IC3 website.

The **Identity Theft Resource Center** (idtheftcenter.org) is a non-profit organization established to empower and guide consumers, victims, business, and government to minimize risk and mitigate the impact of identity compromise and crime.

How Oregon DMV Can Help

You may be eligible for a new driver license or ID card number if your name and number have been used fraudulently. To apply submit at least one of the following documents:

- A police report or a letter on police letterhead;
- A report or letter from a credit card company, credit reporting bureau or financial institution;
- A report or letter from the Oregon Department of Revenue or the Internal Revenue Service;
- A document issued by a court; or
- A letter from a District Attorney.

You must include:

- A signed statement explaining what happened and why you need a new number; and
- Your contact information, including a daytime phone number.

Mail or fax your request with sufficient proof that both your name and drive license or ID card number has been used by another person to:

Oregon DMV Driver Programs, DL/ID Issuance Policy 1905 Lana Avenue NE Salem, Oregon 97314

Or you may fax the request with proof to 503-945-5497, ATTN: DL/ID Issuance Policy Team.

DMV will review the information you send and send you a letter with the decision (ORS 807.160, ORS 807.400, and OAR 735-062-0130).

