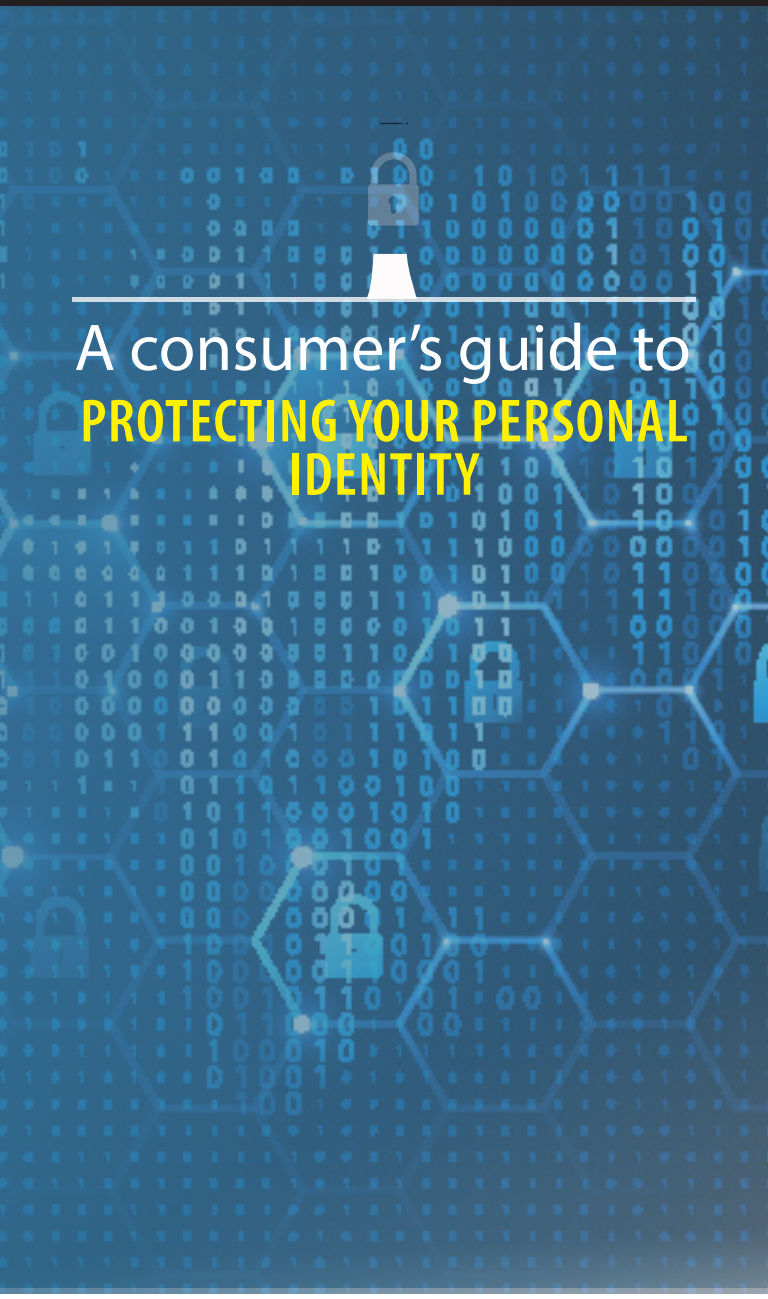


A consumer's guide to
PROTECTING YOUR PERSONAL IDENTITY

DCBS Consumer and Business Services
Division of Financial Regulation

Contents

Oregon Division of Financial Regulation

Protecting Oregonians' access to fair products and services through education, regulation, and consumer assistance.

What is personal information?

In Oregon, personal information includes a person's name, combined with any of the following:

- Social Security number
- Oregon driver license or identification card number issued by the Oregon Department of Transportation
- Passport number or other U.S.-issued identification number
- Financial, credit, or debit card number, along with a security code or password that would allow access to a consumer's financial account
- Physical characteristics data - such as a fingerprint, retina, or iris image - used to authenticate identification during a financial transaction
- Health insurance policy number or health insurance subscriber number, combined with any other unique identifier used by health insurers
- Medical history, mental or physical condition, medical diagnosis, or treatment by a health care professional

Protecting your personal information is important

Identity theft happens when someone steals your personal information and uses it without your permission. Thieves can

use your information to commit fraud, including draining your bank account, making charges on your credit card, taking out new loans, filing taxes, opening new utility accounts, and hurting or ruining your credit.

Prevention tips

- Keep your personal information, including your Social Security card, locked in a secure place in your home. Do not leave these items in your car.
- Shred financial documents, credit card offers, and other paperwork you do not need.
- Regularly check all of your account statements (credit card, bank, etc.) for any unusual charges.
- Clarify the need when you are asked for your Social Security number. Ask if you can use an alternate identification instead.
- Use only secure websites when submitting personal information. A secure website address begins with https.

- Examine all emails and do not respond or click on an embedded web link if you do not know the sender. Suspicious links often carry malware.
- Check your three credit reports once a year, without charge, at 877-322-8228 (toll-free) or **www.annualcreditreport.com**. Stagger when you check each credit bureau report in order to check three times a year for free.
- Check your checking or savings account records once a year, free, by visiting **www.chexsystems.com** or calling 800-428-9623 (toll-free).
- Do not give any personal information over the phone, Internet, or mail unless you started the contact.
- Limit your use of debit cards to locations you trust. Use the chip feature on a card machine instead of swiping.

Two free tools for reducing the effect of ID theft

You can reduce your exposure to the effect of ID theft by placing a **security freeze** on your credit file maintained by the consumer credit reporting agencies. The three major reporting agencies are TransUnion, Equifax, and Experian. An alternative option is to request a **fraud alert**. Active duty members of the military can request an active duty fraud alert. While credit agencies may offer more consumer ID theft prevention tools, **placing a security freeze or a fraud alert and unfreezing or lifting fraud alerts are free**. Credit agencies are required to inform you of your rights (Page 10 of this guide).

Difference between a security freeze and a fraud alert

A security freeze prohibits a reporting agency from disclosing or sharing information in your credit records. There are exceptions, including an affiliate or subsidiary of a company you owe money to, employment screening, tenant screening, background screening, underwriting of insurance, or as a result of a legal recourse against you. You can request the freeze and unfreeze for the length of time you deem necessary based on the options provided by the reporting agency.

An initial fraud alert placed on a credit file lasts for one year. Upon seeing a fraud alert display on your credit file, a business must verify your identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which lasts seven years.

Placing a security freeze

If you request to place a security freeze by mail, the agency must meet the request within **three business days** after receiving your request. If your request was made by phone or a secure electronic process, the placement of a freeze must be made within **one business day**. Place a freeze at all three credit bureaus; they do not share the freeze notice between themselves.

Lifting a security freeze

If you request to lift a security freeze by mail, the agency must meet the request within **three business days** after receiving your request. If your request was made by phone or a secure electronic process, the removal of a freeze must be made within **one hour after the request**.

Placing a fraud alert

If you request to place a fraud alert by mail, the agency must meet the request within **three business days** after receiving your request. If your request was made by phone or a secure electronic process, the placement of an alert must be made within **one business day**. For a fraud alert, you need to tell only **one** of the three agencies, which will inform the other agencies.

Renewing or stopping a fraud alert

An initial fraud alert stays in place for one year. An extended fraud alert stays in place for seven years. You can remove or renew for free at any time.

Reducing the risk of artificial credit reports

Scammers use Social Security numbers and personal identifying information of minors, elderly, and financially vulnerable people to create artificial credit records. Creating and using artificial credit reports is called synthetic identity theft. Children and elderly are particularly vulnerable to this type of identity fraud because the new profile or fake identity can go undetected for several years. To prevent the misuse of personal information, it is important to secure such information. If authorized accounts were established for your dependents, consider opting out. This will help prevent sharing or selling your personal information with companies that do not have a financial relationship with you. You can also opt out by calling 888-5OPTOUT (567-8688) (toll-free) or going online at **www.optoutprescreen.com**.

Credit reporting agency information

TransUnion

Online: transunion.com/credit-freeze

By phone: 800-680-7289

By mail:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000

Equifax

Online: equifax.com/personal/credit-report-services/credit freeze

By phone: 888-298-0045

By mail:
Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian

Online:

To request a freeze: experian.com/freeze/center.html

For credit alerts and information:

experian.com/fraud/center.html

By phone: 888-397-3742

By mail:
Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Other resources:
To opt out from receiving credit offers:

Online: www.optoutprescreen.com

By phone: 888-5OPTOUT (567-8688) (toll-free)

To verify the accuracy of your records related to your checking or savings accounts: ChexSystems

Online: www.chexsystems.com

National protection for records of protected consumers

Minors younger than 16 years old and incapacitated people can be protected if you, as a parent, legal guardian, or conservator, follow the reporting agencies' steps to place a freeze or fraud alert on their records. This will help prevent the misuse of their personal information.

Notice of rights - federal law

You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving an extension of credit. As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a one-year alert placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business must verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which lasts for seven years.

A security freeze does not apply to a person or entity (or its affiliates), or collection agencies acting on behalf of the person or entity, with

which you have an existing account that requests information in your credit report to review or collect the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

Immediate actions

If you believe you are a victim of identity theft:

- Report the theft to the Federal Trade Commission: **www.identitytheft.gov/**
- Follow the personal recovery plan the FTC designs for you
- Contact all your creditors, such as your bank or credit union, credit card company, cell phone provider, and other utilities and lenders
- Change your login IDs, passwords, and PINs
- You may file a police report

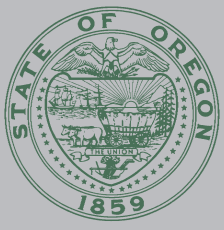
The following free booklet includes steps to recover from identity theft, including sample dispute letters: **www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf**

Oregon Department of Consumer and Business Services

Division of Financial Regulation

888-877-4894 (toll-free)

www.dfr.oregon.gov



440-4115e (2/20/COM)