

Your Security is our Priority

Understanding Identity Theft



Astoria Bank is Looking Out for You

Nothing is more important to us than your financial security, which is why we take steps to protect the sensitive/personal information you may provide to us. We follow strict guidelines to guard against unauthorized access to your sensitive information.

If you have questions about identity theft or think that you may have received a fraudulent email or phone call, please visit your neighborhood Astoria Bank branch.

It's also important that you learn what you can do to protect yourself against identity theft, both online and offline.

Steps You May Take to Protect Yourself Against Identity Theft

- ❑ Never give your personal information over the phone, through the mail or over the Internet unless you have initiated the contact or are confident you know who you're dealing with.
- ❑ If you are not sure that a contact is legitimate, contact the company yourself, either by phone, in person, or by visiting the company's Web site by typing in the site's address or using a page you have previously bookmarked.
- ❑ Don't carry your Personal Identification Numbers (PINs) with you--memorize them and keep them in a safe, secure location.
- ❑ Review account statements regularly to ensure that all charges are correct. If your statement is late in arriving, call your financial institution to find out why. Take advantage of Online Banking to periodically review activity online and catch suspicious activity.
- ❑ Shred personal financial documents such as charge receipts, credit applications, insurance forms, or any other important material.
- ❑ Keep your Social Security Card in a safe place and only give out the number when absolutely necessary.
- ❑ Cover the ATM Key Pad with your hand when entering your PIN number.

Steps You May Take to Protect Yourself Online

- ❑ Update your anti-virus software regularly to guard against new viruses.
- ❑ Keep your browser and operating system up-to-date. New versions and updates often include important security enhancements.
- ❑ Don't download files or click on hyperlinks in emails from people you don't know. They may contain a virus that can infect your computer.
- ❑ Do not be intimidated by an email or caller who suggests serious consequences if you do not immediately provide or verify financial information. Astoria Bank will never send you an email asking you to log in to a link or provide your personal information.

- ❑ Use a personal firewall to limit uninvited access to your computer, especially if you have high-speed or an "always on" connection to the Internet.
- ❑ If you store financial information on your computer, use a password consisting of numbers, symbols and letters, both upper and lower case.
- ❑ Avoid using an automatic login feature that saves your user name and password and always log off when you're finished.
- ❑ Be sure to read Web site privacy policies to know your information will be secure, how it will be used, and if it will be shared with third parties.

Steps You Should Take If You Believe Your Identity Has Been Stolen

If you suspect your identity has been stolen, there are four steps you should take immediately.

1. Place a fraud alert on your credit reports.

Call any one of the three major credit bureaus to help prevent an identity thief from opening additional accounts in your name.

Equifax	1 (800) 525-6285
Experian	1 (888) EXPERIAN (397-3742)
TransUnion	1 (800) 680-7289

As soon as the credit bureau confirms your fraud alert, an alert will automatically be placed by all credit bureaus, and all three reports will be sent to you free of charge. Once you receive these reports, review them carefully for any incorrect information, particularly accounts you didn't open or unexplained debts.

2. Close any accounts that have been tampered with or opened fraudulently.

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

Keep a copy of the report.

4. Contact the authorities that specialize in Identity Theft.

Federal Trade Commission Identity Theft Hot Line:
1 (877) IDTHEFT (438-4338)

Social Security Fraud Hot Line:
1 (800) 269-0271

US Postal Inspectors:
1 (800) 372-8347