

PROTECT YOURSELF FROM IDENTITY THEFT

The following are useful tips when accessing an SEI internet site:

- › Always look for your site authentication image whenever you sign on. If you do not see your image, you should not provide your password.
- › Always sign out of your session.
- › Never register your computer with an Internet café or other publicly used computer.

Where can you find additional information regarding identity theft?

- › The Federal Trade Commission (FTC) has a website dedicated to educating consumers about identity theft: ftc.gov/idtheft
- › The FTC has prepared a brochure, Your Access to Free Credit Reports, explaining your rights and how to order a free annual credit report which can be found at: ftc.gov/bcp/conline/edcams/credit
- › In addition, tips for guarding against Internet fraud and securing your computer can be found at: OnGuardOnline.gov
- › You can learn more about keeping your money safe at: mymoney.gov/scams.shtml

What is identity theft?

Identity theft occurs when a person uses your personal information, such as your name, Social Security number, date of birth, or credit card number, without your knowledge or permission, in order to commit fraud or other crimes.

How does it happen?

Identity thieves may use a variety of methods to steal your personal information. Common methods are:

- › **Dumpster Diving** – rummaging through trash in order to find bills or other paper containing your personal information.
- › **Skimming** – using a special storage device to capture information when processing your debit/credit card.
- › **Phishing** – sending unsolicited emails or pop-up messages purportedly from financial institutions or companies in an attempt to get you to reveal your personal information.
- › **Spyware** – malicious software designed to intercept or take partial control of a computer's operation.
- › **Changing Your Address** – completing a change of address form to divert your billing statements to another location.
- › **Stealing** – taking your purse, wallet or mail without your consent.

seic.com

What can you do to protect yourself from identity theft?

Be aware of how your personal information can be stolen and know how to protect yourself against identity theft.

Safeguard your information to deter identity thieves.

- › Shred documents containing personal information before discarding them.
- › Protect your Social Security number, providing it only if absolutely necessary. Don't carry the number in your wallet or write it on a check.
- › Provide personal information via phone, Internet, or mail only when you have initiated the contact with the person and/or company that you are dealing with. Do not be intimidated by an email or caller who suggests dire consequences if you don't immediately provide or verify financial information.
- › Select passwords that are not obvious. Refrain from using your date of birth or the last four digits of your Social Security number.
- › Never click on links sent in unsolicited emails; instead, type in a Web address you know. Use firewalls, anti-spyware protection that detects and removes spyware and an anti-virus program to protect your home computer.

Routinely monitor your financial and billing statements to detect suspicious activity.

- › Pay attention to missing or untimely bills, denials of credit for no apparent reason, calls or letters about purchases that you didn't make, and unexpected credit cards or account statements.
- › Inspect your credit report. Call **1-877-322-8228** or visit **AnnualCreditReport.com**, a service created by the three major consumer reporting companies (Equifax, Experian, and TransUnion) to request your annual free credit reports. You can also request your credit reports by writing to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

What steps should you take if you have experienced identity theft?

- › File a police report.
- › Notify the Federal Trade Commission at ftc.gov/bcp/edu/microsites/idtheft/ or by calling **1-877-IDTHEFT (1-877-438-4338)**
- › Notify your financial advisor and/or financial institution and your creditors.
- › Close accounts.
- › Place a "**fraud alert**" on your credit reports by contacting one of the three consumer reporting companies:
 - Equifax: **1-800-525-6285** or equifax.com
 - Experian: **1-888-EXPERIAN (397-3742)** or experian.com
 - TransUnion: **1-800-680-7289** or transunion.com

What steps will SEI take once we have been notified that you have experienced identity theft?

1. If requested, SEI will provide a new account number for you.
2. If you maintain the original account number, SEI will indicate within their system that identity theft occurred and will add "**restricted**" to the account title.
3. High-risk transactions, such as disbursements, will be verified with your financial advisor prior to processing.
4. "**Restricted**" will continue to appear in the account title until the financial advisor and/or you notify SEI otherwise.
5. If you have a Consolidated Cash Account, you will be advised to notify PNC of the identity theft. If you have a Cash Access Account, you will be advised to notify Bancorp of the identity theft.