Question:

What should I do if my identity has been stolen?

Answer:

Take the following four steps right away:

- Place a fraud alert on your credit reports and review your credit reports
- Close any accounts that have been tampered with or opened fraudulently
- Checks – close the account and ask bank to notify appropriate check verification service
- File a complaint with the FTC

FTC Identity Theft Hotline 1-877-IDTHEFT

Safety Insurance
AUTO • HOME • BUSINESS

Create your account online at SafetyInsurance.com and take advantage of these benefits:

- *Pay your bill*
- *View your policy*
- *Report a claim*

Safety Insurance
AUTO • HOME • BUSINESS

For more details on Homeowners Insurance from Safety, contact your Agent today.

20 Custom House St. I Boston, MA 02110 I 617.951.0600

www.SafetyInsurance.com

Question:

Does my Homeowner company offer coverage for identity theft?

Answer:

Yes, Safety Insurance offers the Identity Fraud Expense Coverage. This endorsement covers expenses incurred as the result of an act of identity fraud committed against you, our insured. The limit of liability is $15,000; the deductible is $100; and the premium cost is $25.

Question:

How will I know if I am a victim of Identity theft?

Answer:

Some indications of Identity theft include:

- Unexplained charges or withdrawals from your financial accounts.
- Failing to receive bills or other mail.
- Receiving credit cards for which you did not apply.
- Denial of credit for no apparent reason.
- Receiving calls from debt collectors about merchandise or services you did not buy.

Question:

What can I do NOW to avoid Identity theft?

Answer:

Minimize your risk for identity theft:

- Order a free credit report every year at ***www.annualcreditreport.com***, review it carefully and notify the credit bureau of any errors.
- Password protect your mobile device and voicemail with a PIN.
- Buy and use a shredder.
- Never use a PIN or password with the last four digits of your Social Security number. Use strong PINs that are difficult to guess. Memorize your PIN and change it periodically.
- Secure your personal information in your home, e.g., your social security card.
- Avoid giving personal information on the phone, through mail and the Internet unless you initiate the contact.
- Call back customer service to confirm the legitimacy of any incoming calls.
- Outgoing mail should be brought to post office collection boxes.
- Notify post office to hold mail while on vacation.

Make your computer safe from Identity thieves:

- Arranging mobile device settings so the screen locks after a short period of inactivity.
- Downloading anti-virus software and enable firewall protection for your computer and mobile devices.
- Deleting voice and text messages with financial or personal information.
- Avoid downloading files from strangers or clicking on unknown hyperlinks.
- Use a secure browser.
- Do not store financial information on your laptop.
- Avoid using an automatic log-in feature.
- Delete personal information stored before you dispose of a computer or mobile device.
- Read website privacy policies.
- Avoid "phishing" a high tech scam that uses Spam or pop-up messages deceiving you into disclosing your personal information.
- Make sure your phone is safe for mobile banking by:
  - Educating yourself on the security features and how to recognize malicious attacks.
  - Ensuring your phone has an application to encrypt all stored data.
  - Disabling automatic sign ins to your online banking account.

Question:

How do I defend my data when it's in the Cloud?

(simply defined as social networks that store and share our data)

Answer:

In the cloud take these steps to protect your data:

- Read the Terms of Service and receive advance notice of any changes in service before placing any information in the cloud.
- Enter information that you do not want others to see.
- Pay attention to the cloud provider's reserve rights to use, disclose or make public your information.
- Know exactly what happens to your data when removed from the cloud provider.