Tips To Protect Information

PRINCIPAL FINANCIAL GROUP®

Are You Security Savvy?

Identity Theft

Identity theft occurs when someone unlawfully obtains personal information with the intent to commit fraud.

Victims of identity theft report situations where bank accounts have been drained, credit cards have been used, loans have been obtained fraudulently and medical care has been received using their name and personal information.

Protect personally identifiable information to avoid having your identity stolen.

Identity theft in the United States rose to a three-year high in 2012, with more than 5 percent of the adult population, or 12.6 million people, falling victim to such crimes.

Personally Identifiable Information	
Name	Social Security number
Physical address	Birthdate
Phone number	Mother's maiden name
Email address	Account information

Credit Report

Request a copy of your credit report periodically. Review it to find out if accounts have been opened without your consent. Obtain a free credit report online at www.annualcreditreport.com or by calling 1.877.322.8228.

Strong Passwords

Strong passwords are one of the best ways to protect information. Create unique passwords that are easy to remember; difficult to guess.

Create a password in five easy steps:

1	Create an eight word sentence.	Bob and I go to Europe every July.
2	Use the first letter of each word.	b a i g t e e j
3	Use upper and lower case letters as you would in a sentence.	B a I g t E e J
4	Replace at least one letter with a number. J for July is replaced with 7. (July is the seventh	B a I g 2 E e 7
5	Replace at least one letter with a special character.	B & I g 2 E e 7

Additional tips

- ☐ Avoid using easily available information such as your Mother's maiden name, date of birth or last four digits of your Social Security number.
- ☐ Set passwords on your credit card, bank and phone accounts.
- ☐ Use a passcode to secure your phone.
- ☐ Use different passwords on each website you use.
- ☐ Consider purchasing software to securely store multiple passwords and PINS. Search online for "password managers".

Handheld Devices

Whether traveling for business or stopping by a local coffee shop, you will see many handheld devices being used. Laptops, tablets and smartphones are everywhere. Protecting yourself in a mobile world is crucial.

Keep handheld devices with you. Don't leave them out in the open or unattended.

Be careful about what information is stored on them. When possible, use a passcode/password on the device and encrypt information.

Additional tips

- ☐ Reduce your data 'footprint'. Think about emails, texts, documents, notes and apps saved on your device. Delete the information and apps no longer used. The data on your device can paint a complete picture of your life.
- ☐ When using public Wi-Fi networks, avoid conducting online transactions involving use of your account credentials or sharing information that may be useful for insider trading, identity theft, and more. Hackers can easily "eavesdrop" on what you are doing.
- ☐ Have a plan for what to do, who to contact and what passwords to reset in the event your device is lost, stolen or misplaced. Consider carrying a mini card in your wallet listing your device serial number, carrier's phone number and top list of accounts. Do not list passwords!

Checklist

Use this checklist as a guide to protecting information

Social Security Numbers

- ☐ Remove Social Security numbers from driver's license, health insurance/medical card, student ID cards and personal checkbook.
- ☐ When asked to provide your Social Security number, ask how it will be used and protected.

Personal Information

- ☐ Shred personal documents.
- ☐ Wait until morning to set out trash to avoid dumpster divers.
- ☐ Do not give out personal information by phone, mail or over the Internet unless you initiated the call/transaction or confirm you are giving it to a legitimate person.
- ☐ Use software to overwrite information on a computer hard drive before throwing or giving it away.
- ☐ Teach your children not to give information on the phone or the Internet.
- ☐ Recognize the signs of phishing scams. Hover over hyperlinks (but not for too long) to review the link address. If you know the sender, cautiously open attachments. If you do not know the sender and aren't expecting an email/attachment, avoid opening it.

Mail

- ☐ Use secure postal service collection boxes for outgoing mail.

Principal® Financial Group

WE'LL GIVE YOU AN EDGE®

EE11470A / 10/2014