THINGS YOU SHOULD KNOW ABOUT IDENTITY THEFT

Compliments of:
Fripp Island Security
and
FIPOA Security Committee

November 2013

INTRODUCTION

Identity theft is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name

Our goal is to help you take some simple steps so that it won't happen to you.

SCAMS

Scams are everywhere. Identity theft has become a major problem. Strictly speaking, identity theft occurs when someone literally steals you identity. They set up bank accounts, take out credit cards, file tax returns, and borrow money in your name. Related scams include someone using your credit card number illegally or stealing your PIN and looting your bank account.

Phishing is identity theft's evil twin. It occurs when someone pretends to be a legitimate business or government organization and convinces you to give up personal or financial information. Scam artists often use phone calls or e-mail messages to contact you; they even set up fake web sites modeled after a legitimate business or governmental agency.

How does the scam artist steal your identity? He or she really only needs a few pieces of information. Name, social security number, date of birth, and mother's maiden name are enough to obtain additional credit in your name or open a bank account. If the thief can find your current credit card number, that's a bonus.

- Identity theft complaints registered with the Federal Trade Commission in one year: 255,000.
- Most commonly reported forms of identity theft were credit card fraud, phone or utilities fraud, bank fraud (electronic funds transfers), and employment fraud.
- The national Taxpayer Advocate called identity theft the #1 consumer complaint in the country.

DISGUISES

Clever scam artists have many methods for stealing your identity. Here are a few.

- **Dumpster Diving** – Criminals steal millions of American identities each year by going through the discarded trash of individuals and businesses.
- **Phishing –** Thieves call or e-mail individuals pretending to be from the IRS, your bank, or other institutions and ask for personal financial information.

- **Skimming –** Crooks steal credit/debit card numbers when a card is used to pay for a purchase.
- **Changing addresses –** Thieves divert an individual's bills to another location by filling out a change of address form and then steal the information on the bills.
- **Plain stealing –** Crooks steal wallets, purses, mail, bank statements, credit card statements, pre-approved credit card mailings, personnel records, and anything else they can get their hands on that contains your private information.
- **Be alert to scams if you're job hunting –** Crooks can find your resume online and posing as recruiters, e-mail you asking for personal information to do "a background check."
- **Don't become a victim of identity theft –** do not respond to a fake IRS e-mail that tells you are due a refund and asks for your social security number and bank information. The IRS never sends unsolicited e-mails to taxpayers.
- **Be cautious about solicitation –** Thieves will use look-alike web sites and sound-alike names of charities or political campaigns. Their purpose is to collect credit card numbers and personal information they can use to steal from you.
- **Providing too many details about yourself –** Be careful on a social networking sites. Detailed information can lead to problems. Giving your birth date, family information, and other facts could enable a scam artist to put together enough information to impersonate you.

BE ALERT

Scam artists constantly think of creative new ways to steal your personal data. Scam to watch for are:

- **Bogus tax forms** that appear to come from the IRS requesting personal data
- **Fake letters** from your bank asking for "account update" information.
- **Bogus e-mails** from retailers or Internet service providers asking you to update credit and account details.
- **Phone calls or e-mails** referring to fraud problems on your account and asking you to "confirm" personal data.
- **Bogus applications** for low interest credit cards asking for your credit and personal details.

PROTECT YOURSELF

- **Don't make the mistake** of thinking identity theft is mainly an online problem. There are very real offline ways to fall victim to identity theft. Recent research suggests that you're in greater danger from con artists rummaging through your trash or stealing your mail than from online scams.
- **Shred credit card receipts** and anything else that contains your personal identification information before throwing it in the trash.
- **Check your credit report regularly**. The three major consumer reporting companies are required by law to give you a free copy of your credit report each year if your ask for it. Go to www.annualcreditreport.com or call 1-877-322-9228 to order your free reports. Look for mistakes, accounts you don't recognize, or strange credit inquiries. Report suspicious items immediately.
- **If you suspect you're at risk** of becoming a victim of identity theft, consider putting a "fraud alert" on your credit report. A note in your file to advise lenders to confirm directly with you before opening up any new credit accounts in your name.
- **If any financial information is stolen, file a police report.** Creditors may want proof that you've been a victim of identity theft.
- **Report any identity theft** to the local law enforcement agency, the Federal Trade Commission, and if a tax return is involved, to the IRS as well.

MORE TIPS

- **Keep** passwords secure. Don't use obvious passwords, such as your birth date, middle name, or part of your social security number
- **Never** click links sent in unsolicited e-mails.
- **Don't** preprint your telephone number, driver's license number, or social security number on your checks.
- **Don't** put outgoing mail in your mailbox. Use the post office collection box instead.
- **If** bills or credit card statements include suspicious charges, investigate them immediately.

- **Don't** sign the back of your credit card, and don't leave it blank. Write "Photo ID Required" instead.
- **Don't** carry more in your wallet than necessary. Carrying multiple credit cards, your social security card, PINs, etc. will give thieves all they need if your wallet is stolen or lost.

Identity theft is no longer a novel occurrence, and it's easy to let down your guard. The crooks get more imaginative and seem to find new opportunities to rip you off. Take identity theft seriously, or you could become the next victim. Remember, it's not just the potential financial loss that can occur when your identity is stolen; it's the months (and even years) of your life that may be lost to sorting out the problem and regaining your identity.