

IDENTITY THEFT, It Could Happen to You

The following are meeting notes taken from the November 2004 Puget Sound Chapter meeting and published in the chapter newsletter, Soundings. They are republished here because of the interest of the public in this topic. This program is an excellent example of the kind of programs available to members of the Puget Sound Chapter of ARMA International, the Association for Information Management Professionals. For more information about membership in the Puget Sound Chapter, contact Debbie Jones, Membership Chair, (206) 878-0166 or filetdxj@aol.com.

Detective Dave Paul of the Tacoma Police Department gave a compelling presentation at a recent Puget Sound Chapter of ARMA meeting about the importance of protecting your private information. Detective Paul explained that thieves are no longer breaking into cars to steal stereos, but are looking for financial information such as checks, Social Security numbers, and credit cards. He claimed that recent data indicates that 80% of mail theft, stolen cars, and other white collar crimes are driven by the addiction to methamphetamines. Identity theft is the fastest and easiest way for the addict to make money. Identity theft, said Detective Paul is "the fastest growing crime in America." Detective Paul began his presentation with a ten minute video produced by the Postal Service. Some of the advice the Postal Service suggests:

- Outgoing mail should be put in the blue Postal Service boxes only.
- Shred or burn credit card applications and old credit cards.
- Order your personal credit report once each year and check for unauthorized activity. Close unused accounts.
- Limit the personal information you put out on the internet.

After the video, Detective Paul presented a wealth of information on Identity (ID) Theft prevention and survival. *How does ID Theft happen?* The bad guys gets your social security number and/or drivers' license number. Then all they need is your date of birth, address, full name and then they can steal your financial future. *How do the bad guys get this info?* They steal wallets, purses, *"shoulder surf"*, access credit reports, steal mail from mailboxes and *"dumpster dive."* **(Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand (from searchsecurity.com). How we can detect ID Theft: Detective Paul claimed that it may not be immediately obvious when ID Theft occurs. However, he said, those who use on-line banking will discover the theft quicker than those who wait for their monthly paper statements from their financial institutions. How we can prevent ID Theft: Detective Paul was able to give quite the "laundry list" of ID theft prevention tips:*

- Don't carry more than your driver's license and one credit card in order to reduce the amount of information that is "out there".
- Close old accounts and check your credit report.
- Do not carry your Social Security card, passport, or birth certificate.

- Install a locked mailbox at your home and consider using a PO Box to avoid mail theft.
- Have your check order sent to you bank, not your home postal box.
- Don't toss pre-approved credit card offers in the trash. Shred them!
- Keep a list or photocopy of your credit card and bank account information in a secure place.
- Never give credit card information over the phone unless you initiate the call (and trust them!)
- Always take credit card receipts with you.
- Memorize your passwords. Don't record them on anything in your wallet or purse.
- Shield your hand when using bank ATMs or phone cards. Beware of "shoulder surfers" - possibly using binoculars.
- Review credit card statements and phone bills. ("You would be surprised at how many people don't do this," he said.)
- Protect your Social Security number! "One of the basic prevention tools", Detective Paul said:
- Don't give it out unless it's absolutely necessary.
- Don't put it on your checks
- Order the Social Security Earnings and Benefits Statement yearly.

What ID Theft victims need to do:

- Report the theft to your local law enforcement as soon as possible. Get a copy of the report, the officer's name and report number. Make a note of the dates and time in a log.
- Notify your credit card companies and banks.
- Get replacement cards with new account numbers.
- When closing your accounts, make sure it is noted "at consumer's request."
- Call the fraud units of the three large credit reporting companies and ask that your accounts be "flagged". (The names of these companies are: Equifax, Experian and TransUnion. For further info each company has a website. The address of each is the company's name followed by .com)
- If checks are stolen, close the account immediately and report it to the police.
- Notify the Postal Inspector if the theft involves your mail.
- Keep a log of all conversations, include date, time, and names.
- Send correspondence by certified mail.
- Keep copies of all letters and documents.

Detective Paul said it is often very, very difficult to repair the damage done by ID theft. As a last resort, some people need to have their Washington State drivers' license numbers changed. While it should be a "last resort", a victim may even need to change their Social Security number. Sadly, at this point, he said, the victim will probably need to seek legal counsel. Clearly the costs—effort, time, and money—can be daunting for the victim of ID theft.

The Puget Sound Chapter thanks Detective Dave Paul for his time and expertise in presenting this informative program