NEIGHBORHOOD CRIME WATCH
IF I DON'T CALL THE POLICE MY NEIGHBOR WILL

COMMUNITY POLICING in Snohomish County

July/August 2005 Volume 9 Issue 4

Inside This Issue

Identity Theft– *Still a Major Problem*

Identity Theft remains a major problem in the US and the state of Washington. According to the Attorney General's Office 5,654 complaints were filed in 2004 for ID Theft. Nationally, the state of Washington ranked 8th in the number of ID Thefts per capita.

In recent months ID Theft has captured the headlines with revelations of the hacking, theft and loss of personal data from major financial and data handling institutions such as LexisNexis and ChoicePoint.

The 2005 session of the Washington State legislature has attempted to help the public to protect itself from ID Theft with three new laws that have been signed by the governor. All three bills take effect on July 24, 2005.

1. Security Freeze- Senate Bill 5418. This law allows ID Theft victims to have a security freeze placed on their credit files after submitting a valid police report to the credit-reporting agencies. When a freeze is in place, the credit-reporting agencies cannot release the consumer's credit report or any information from it without authorization from the consumer. Placing or lifting the freeze is free.

2. Security Breach- Senate Bill 6043. This law requires credit-reporting and consumer data agencies to notify consumers if there is a breach of security compromising their private information. This law is similar to a California notification law that required ChoicePoint to notify consumers when it discovered a theft of its data. The idea is to notify you when there is a compromise of data so that you can take appropriate measures to protect yourself.

3. Police Reports- Senate Bill 5939. Finally, this law requires police departments to provide ID Theft victims with a police or incident report. Then the victim can provide credit-reporting agencies, banks, and other financial institutions with documentation that they are victims of ID Theft. In addition, the law requires credit-reporting agencies to permanently block reporting any information that the consumer identifies as a result of ID Theft (in violation of RCW 9.35.020) within 30 days of receipt of proof of the consumer's identification and a copy of a police report filed by the consumer documenting the consumer's claim of ID Theft.

Identity Theft– *How Thieves Get Your Information*

There are several ways that thieves can steal you personal information:

- **Mail theft.** Thieves will steal credit card payments and statements, pre-approved credit offers and convenience checks.
- **Computer hacking.** Much publicized of late, thieves hack into computers of major financial institutions or data handling companies to take personal financial information.
- **"Dumpster diving"**. Thieves can find personal information in dumpsters at businesses or in garbage cans at your home.
- **"Insider access"**. An employee of a business may wrongfully retrieve personal identification information that the business has collected for legitimate reasons.
- **Purse or wallet loss or snatching.**
- **Computerized information services.** A business that sells personal identification information in electronic form may not safeguard the information appropriately.
- **Internet**. Personal information can be accessed by a thief on the Internet by installing "spyware" on your computer without your knowledge or through "phising" (posing as a legitimate business, asking you for your personal information through an email).
- **Skimming.** Stealing credit and debit card account numbers. This can happen during a legitimate transaction such as at a restaurant. You give your server or cashier your credit card, they go to where they normally run bankcard transactions, but first, they secretly swipe your card through a portable reader that is about the size of a credit card. They can collect several hundred card numbers this way. Another place for skimming is at ATM machines.
- **Burglary**. A burglar can steal your personal information from your checkbook, account statements, or other files that are not locked up in your home.
- **Divert your mail**. An ID thief can send a completed change of address form to the financial institution that has your credit or debit card. They send your statement to a new address. This way the thief can use your credit card keeping you in the dark that they are running up bills in your name.

Identity Theft– *Your Information is Valuable*

ID thieves have many uses for your personal information:

- *They change the mailing address on your credit card account. The imposter then runs up charges on your account without you knowing.*
- *They open a new credit card account, using your name, date of birth and SSN. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.*
- *They establish phone or wireless service in your name.*
- *They open a bank account in your name and write bad checks on that account.*
- *They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.*
- *They counterfeit checks or debit cards, and drain your bank account.*
- *They buy cars by taking out auto loans in your name*
- *If arrested, they might use your name. Then, when they don't show up at court, the cops go looking for you.*

Identity Theft– *How to Protect Your Good Name*

Here are some ways to avoid becoming an identity theft victim:

- Do not give your Social Security number, mother's maiden name or account numbers to strangers who contact you, especially by phone, Internet or mail.
- Pay attention to what time of month your bills arrive. If they don't arrive on time, call the creditor and verify your address.
- Guard your mail from theft. Don't leave outgoing mail in your mailbox. Take it to a collection box or your local post office. Promptly remove mail after it has been delivered. Better yet, purchase a good locking mailbox. You can find individual locking mailboxes at a hardware store. Or, talk to your local postmaster about locking mailboxes for you and your neighbors.
- Put strong passwords on your credit card, bank and phone accounts.
- Don't carry your Social Security card. Leave it in a secure place such as a safe bolted to the floor in your house or a safety deposit box.
- Don't carry credit cards or ID cards you don't need.
- When ordering new checks, pick them up at the bank instead of having them mailed to your home.
- Tear or shred charge receipts, copies of credit applications, insurance forms, physician statements, bank checks and statements, expired charge cards and credit offers you get in the mail.
- Regularly inspect your credit report for errors, to determine whether accounts have been opened without your knowledge or consent, and to see what entities are requesting your credit history. As of 1/1/04 all Credit Bureaus are required to give out one free credit report per year according to the Fair Credit Reporting Act (FCRA).

Note: The Credit Bureaus are not required to give out your credit score for free. If you want to order your score in addition to your free report, most are charging about $5.95. The free reports are good for 30 days only, so make sure you print your reports if you get them online.

For More Information:

- *Visit the Electronic Privacy Information Center web site:*

www.epic.org/privacy/fcra/

- *Or The Credit Info Center:*

www.creditinfocenter.com/creditreports/credtrpt.shtml

Credit Reporting Bureaus–

Equifax-
Report fraud:
1-800-525-6285
Order copy of report:
1-800-686-1111
Web Site:
www.equifax.com
Address:
PO Box 740241
Atlanta, GA 30374

Experian (formerly TRW)-
Report fraud:
1-888-397-3742
Order copy of report:
1-888-397-3742
Web Site:
www.experian.com
Address:
PO Box 2002
Allen, TX 75013

Trans Union-
Report fraud:
1-800-680-7289
Order copy of report:
1-800-888-4213
Web Site:
www.tuc.com
Address:
PO Box 390
Springfield, PA 19064

Identity Theft– *What To Do If You Are a Victim*

Your Social Security Number-

If someone asks you for your SSN, know why they want it. Employers and financial institutions will need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Others may simply want your SSN for general record keeping. If someone asks for your SSN, ask:

• Why do you need my SSN?
• How will you use my SSN?
• How do you protect my SSN from being stolen?
• What will happen if I don't give you my SSN?

If you don't provide your SSN, some businesses may not provide you with the service you want. Getting satisfactory answers to these questions will help you decide whether you want to share your SSN with the business.

Despite your careful efforts, you could still become a victim of identity theft. Here is what you should do:

- **First, contact the fraud departments of each of the three major credit reporting bureaus.** Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, as well as a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts. This can help prevent an identity thief from opening additional accounts in your name.

- **Second, contact the creditors for any accounts that have been tampered with or opened fraudulently.** Creditors can include credit card companies, phone companies and other utilities, and banks and other lenders. Ask to speak with someone in the security or fraud department of each creditor, and follow up with a letter (send it via Certified Mail and ask for a receipt). It's particularly important to notify credit card companies in writing because that's the consumer protection procedure the law spells out for resolving errors on credit card billing statements.

- **Third, file a report with your local police department or the Sheriff's Office.** ID theft is a felony, and charges may be filed against the thief in the county where you live. Ask the police to file a police report and give you a copy. You will need this to help correct your credit rating. Send a copy of the police report to the credit reporting bureaus and to your creditors. Requests for copies of Snohomish County Sheriff's Office Reports must be in writing. Information on requesting a copy of a SCSO Report is available at: http://www1.co.snohomish.wa.us/Departments/Sheriff/Services/Request_a_Report.htm

- **Tell the prosecuting attorney that if the person who stole your identity is found guilty, you'd like the court to issue you an Order Correcting Public Records.** This is a court order you can use to correct public records damaged by identity theft. You may also want to send copies of the Order Correcting Records to your financial institution and creditors to assist you correcting non-public records maintained by them.

- **Ask businesses to provide you with information about transactions made in your name.** Under a new Washington State law, businesses must give you this information but may require proof of your identification including a copy of the police report and a statement from the Washington State Patrol that your fingerprints are on file.

(Continued on page 5)

Identity Theft– *What To Do If You Are a Victim, cont.*

(Continued from page 4)

- **If the ID thief has stolen and used your checks (or made counterfeit checks), you will probably be contacted by collection agencies that want you to pay the debts.** Explain to each collection agency in writing that you have been the victim of identity theft. You will need to provide the following information: a copy of a government issued photo identification issued prior to the alleged identity theft; a certified copy of a police report; a written statement describing the nature of the fraud or identity theft; information regarding the relevant financial institutions, account numbers, check numbers, etc; and a statement that the subject debt is being disputed because of an identity theft.

Your Computer– *Protecting Your Sensitive Files*

You may use your computer to keep your financial records, purchase goods over the internet or to check on your bank and investment accounts. As a result, your Social Security, bank account and other sensitive information will be stored on your computer. Follow these suggestions to protect your computer files:

- Update your virus protection software regularly, ideally, automatically each week.
- Do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard.
- Use a firewall program. Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.
- Use a secure browser – software that encrypts or scrambles information you send over the Internet – to guard your online transactions. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.
- Before you dispose of a computer, delete all the personal information it stored with a reliable "wipe" utility program to overwrite the entire hard drive.
- Look for website privacy policies. They should talk about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If you don't see a privacy policy – or if you can't understand it – consider doing business elsewhere.

Your Laptop– *Don't Store Sensitive Information On It*

Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password – a combination of letters (upper and lowercase), numbers, and symbols. A good way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "I love Felix; he's a good cat," would become 1LFHA6c. Don't use an automatic log-in feature that saves your user name and password, and always log off when you're .finished. That way, if your laptop is stolen, it's harder for a thief to access your personal information.

File Sharing–

For information about file sharing see "File Sharing: A Fair Share? Maybe Not" and "Spyware", publications from the FTC at: www.consumer.gov/idtheft

NEIGHBORHOOD CRIME WATCH
IF I DON'T CALL THE POLICE MY NEIGHBOR WILL

COMMUNITY POLICING in Snohomish County

Snohomish County Sheriff
M/S 606 - 3000 Rockefeller Ave.
Everett, WA 98201

Inside This Issue

Rick Bart, Sheriff
Snohomish County
3000 Rockefeller Ave.
M/S 606
Fourth Floor County Courthouse
Everett, WA 98201
(425) 388-3393
www.co.snohomish.wa.us/sheriff/

Steve Moller– Editor

CRIME STOPPERS™ Of Puget Sound **1-800-CRIME-13**

Identity Theft– *Where To Go For More Information*

To get more information or help with identity theft:

- If you are a victim of identity theft, contact your local law enforcement agency and the Federal Trade Commission's (FTC) Identity Theft Hotline, **1-877-IDTHEFT**.
- The FTC and Attorney General post step-by-step directions on their websites for reporting identity theft and protecting your credit history. The Internet addresses are:
- Federal Trade Commission: ***www.ftc.gov*****.** The FTC also posts a document called "TAKE CHARGE– Fighting Back Against Identity Theft". You can find it at: ***www.consumer.gov/idtheft/index.html***
- Washington State Attorney General's Office ***www.wa.gov/ago/consumer/idtheft/***

The Attorney General's Identity Theft experts in its statewide Consumer Resource Centers can help refer you to the proper authorities, assist victims with referrals, and help resolve problems with credit reporting and collections. Consumer Resource Centers can be reached at **1-800-551-4636**.