ID Theft

Identity fraud thieves do not discriminate. They will steal information from anyone, no matter what your choice in lifestyle, financial means or overall situation. Public awareness and education is the key to preventing and reducing the number of reported incidents of Identity Fraud. While it may not be possible to guarantee the safety of everyone's identity, following some general guidelines and being aware of current trends will help minimize your risk and exposure to these incidents.

What is Identity Fraud?

Commonly referred to as identity theft, identity fraud involves the unauthorized acquisition, possession or trafficking of personal information. The information is used to create a fictitious identity, assume or takeover an existing identity that may result in financial gain, goods or services, or concealment of criminal activity. Changes to the Criminal Code of Canada in 2010, added specific charges for Identity Theft/Fraud.

Thieves look for information such as a name, address, date of birth, social insurance number, mother's maiden name, usernames and passwords of on-line services as well as drivers' license numbers. This information allows the thief to take over the your financial accounts, open new bank accounts, transfer bank balances, apply for loans, credit cards and other services, purchase vehicles and take luxury vacations.

How is your information obtained?

Identity fraud is facilitated by technology, commonly through the Internet**. "Phishing"** attacks are becoming more sophisticated as criminal elements gather profiles of potential victims through the use of fake internet websites. Computer spy-wares and viruses, designed to acquire personal information are common methods of Phishing.

Another sophisticated avenue used is **"Vishing,"** where technology is used to capture telephone and computer keyboard strokes. Fan out calls are placed to unsuspecting victims requesting banking and other personal information. These normally seem to come in the form of a text. The text may ask for personal information or there may be a link. Once you access the link it requests information or downloads the key stroke program.

A third type of scam which is becoming very prominent in the age of the smart phone is called **"Smishing".** Like Phishing and Vishing, Smishing uses use Smart/Cell Phone texts to "bait" a victim into going to a URL address Link attached to a text in order to obtain information on that persons phone. Once the victim goes to the website they inadvertently upload a Computer Virus commonly known as a Trojan horse which hides within a program pretending to be something it is not. Uploading a Trojan

horse may allow a suspect to gain unfettered access to the data on their phone. This is commonly called "phone hacking". Smishing has become infamous in the media because numerous celebrities have had their phones accessed this way and personal photos and other data have ended up on the internet for public access.

Other less sophisticated, but effective, techniques include stealing wallets, break and enters to homes and vehicles, picking through someone's garbage, Watching over someone's shoulder while they enter Pin information into a debit machine, redirecting/stealing mail, posting job offers and sending out mail or emails requesting extensive personal information.

Don't forget, what may be garbage to some is a treasure to others. SHRED SHRED SHRED!!!!

What can you do to protect yourself?

Remove identification from your wallet you are not using such as your birth certificate and Social Insurance Number (SIN). A SIN is a confidential number which is only required by law for tax reporting if a customer is earning income (either employment or investment). While many companies may ask for you SIN for other purposes, you have the right to refuse under these circumstances.

Keep track of your credit cards. Cancel any that you do not use and always sign them when they are received. Review your on-line banking or paper statement regularly and contact your credit card company if there are any questionable charges.

Never provide personal information including your SIN, date of birth and credit card security code unless you initiate the call. Your bank will never call you and ask you for your banking information, account numbers and debit card passwords. Shred your paper mail, statements, credit card offers, bills and receipts before putting them in the recycling bin.

Ensure your computer anti-virus, anti-spyware and firewall programs are up-to-date, turned on and working properly. Don't save passwords and sensitive banking information in a file titled 'passwords.' Destroy your old computer hard drive. Information is left behind even after you delete it. Never use a public access computer to access your personal or financial information. Software can be installed without the knowledge of the business owner to capture key strokes. Once the suspect downloads the information, you or anyone else who previously entered will have access to your bank, email, social networking account.

Avoid embedded links in an e-mail claiming to bring you to a secure site. In some cases, the offending site can modify your browser address bar to make it look legitimate, including the web address of the real site and a secure "https://" prefix. If the site appears suspicious contact the company directly by

phone or entering the site address in manually. If you need to access the site, do not use the link provided, type in the web address you normally use. Access your accounts on-line regularly to monitor the transactions.

Reviewing your credit bureau history on a regular basis is a good step to making sure your credit has not been compromised. If your information has already been used to create a fictitious identity, contact your local police service. Contact your credit and debit card issuers and notify your bank about the incident. Finally, contact a credit bureau to request a fraud alert be placed on your account.

For further information, contact:

Constable Matthew Mirasty
Commercial Crime Section
RCMP “F” Division (Saskatoon Office)
Phone: 306-975-5652