



## *News Release*

FOR IMMEDIATE DISTRIBUTION

### **Saskatchewan Policing Agencies Remind Consumers March is Fraud Awareness Month: Focus on Identity Theft and Fraud**

The Commercial Crime and Fraud Sections with the Regina Police Service, Saskatoon Police Service, Saskatchewan Financial Services Commission and RCMP "F" Division have joined forces to promote March as Fraud Awareness Month to Saskatchewan residents and consumers.

During this the second week of Fraud Awareness Month, the fraudulent activity to be profiled is Identity Theft and Fraud. Public education and awareness is the key to prevention and reducing the number of incidents. It may not be possible to guarantee everyone's identity is safe, but following some general guidelines and being aware of current trends will help minimize people's risk. Identity fraud thieves do not discriminate. They will steal information from anyone, no matter what your means or situation is.

#### **What is Identity Fraud?**

Commonly referred to as identity theft, identity fraud involves the unauthorized acquisition, possession or trafficking of personal information where that information is used to create a fictitious identity, assume or takeover an existing identity that results in financial gain, goods or services, or conceals criminal activity. Recent changes to the criminal code added specific charges for Identity Theft/Fraud.

Vital information such as name, address, date of birth, social insurance number, mother's maiden name, username and password of on-line services as well as drivers' license numbers, need to be acquired in order to complete the impersonation. The thief can take over the victim's 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, mainly 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 an emerging trend.

One such way is e-mail takeover. This has happened recently in the province. The suspect sends a pop up message to solicit your username and password. The suspect uses this information to access your e-mail account and change your setting so you cannot access your account any longer. What normally happens is your contact list is sent e-mail requesting money because of a described desperate or bad situation. They ask for the money to be sent by a wire money transfer service. Once the money is sent it can be picked up anywhere in the world, not just the location you send it to.

Another sophisticated avenue used is "Vishing," where technology is used to capture telephone key 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.

Other less sophisticated, but effective, techniques include stealing wallets, break and enters to homes and vehicles, dumpster diving, shoulder surfing, redirecting/stealing mail, posting job offers and sending out mail or emails requesting extensive information.

### **What can you do to protect yourself?**

Remove identification from your wallet you are not using including 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. These are public accessible and there is a chance they could be compromised. 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 has entered they will have access to your bank, email, social networking account. In Saskatchewan, an incident was reported where an individual placed a key stroke logger on a public access computer. Subsequently, personal information was obtained from many people who accessed that public computer. Unfortunately, one person had their financial information accessed and in the hands of the criminal. The loss was significant.

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.

### **What can you do if this happens to you?**

Contact your credit and debit card issuers. Notify your bank about the incident. Contact a credit bureau to request a fraud alert be placed on your account.

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

Through heightened attention of Fraud Awareness Month, the trained staff of Commercial Crime and Fraud Sections with the Regina Police Service, Saskatoon Police Service, Saskatchewan Financial Services Commission and RCMP “F” Division will be able to share their knowledge and inform the general public. Education on fraudulent activities will help prevent consumers from becoming “victims.”

Future fraudulent activities to be profiled in media releases during the month of March as part of Fraud Awareness Month include Mass Marketing Fraud/E-Commerce, Social Networking/On-Line Dating Fraud and Securities Schemes.

For further information, contact:

March 8, 2010

Corporal Trevor Ellis  
Commercial Crime Section  
RCMP “F” Division  
Phone: 306-780-6005

Or visit: [www.sacp.ca/fraudawareness/](http://www.sacp.ca/fraudawareness/)

The following contact information is offered below as additional reference.

RCMP “F” Division: [www.rcmp-grc.gc.ca/sk](http://www.rcmp-grc.gc.ca/sk)  
RCMP: [www.rcmp-grc.gc.ca/scams-fraudes/](http://www.rcmp-grc.gc.ca/scams-fraudes/)  
Regina Police Service: [www.reginapolice.ca](http://www.reginapolice.ca)  
Saskatoon Police Service: [www.police.saskatoon.sk.ca](http://www.police.saskatoon.sk.ca)  
Saskatchewan Financial Services Commission: [www.sfsc.gov.sk.ca](http://www.sfsc.gov.sk.ca)  
Bank of Canada: [www.bankofcanada.ca/en/video\\_corp/dbo/dvd\\_fraud.html](http://www.bankofcanada.ca/en/video_corp/dbo/dvd_fraud.html)  
Better Business Bureau: 1-888-352-7601 [www.sask.bbb.org](http://www.sask.bbb.org)  
Consumer Protection Branch: (306) 787-5560 [www.justice.gov.sk.ca/cpb](http://www.justice.gov.sk.ca/cpb)  
Corporations Branch: (306) 787-2962 [www.corporations.justice.gov.sk.ca](http://www.corporations.justice.gov.sk.ca)



Saskatchewan  
Financial Services  
Commission

