Yukon
Information
and Privacy
Commissioner

211 Hawkins Street, Suite 201
Whitehorse, Yukon Y1A 1X3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.ombudsman.yk.ca

News Release

November 26, 2015

A Reminder to Protect Your Personal Information during the Holiday Shopping Season

You better watch out, you better beware
Identity thieves are lurking out there
ID thieves are coming to town
They see you while you're shopping
They know when you're online
They'll steal your information and they'll use it for all time
You better watch out, you better beware
Identity thieves are lurking out there
ID thieves are coming to town

WHITEHORSE – Diane Mcleod-McKay, Yukon's Information and Privacy Commissioner (IPC), is reminding Yukoners to actively protect their personal information during this holiday shopping season.

> *Yukoners need to be mindful during the holiday shopping season about the risks to their personal information given that there is a significant amount of personal information in the marketplace. Yukoners need to take care to protect their personal information while holiday shopping to avoid becoming a victim of identity theft and fraud.*

Identity theft occurs when a person assumes your identity. Identity fraud occurs when someone posing as you uses your personal information in a fraudulent way, such as to create a credit card in your name with your credit card number and uses this card to make purchases which are then charged to your credit card account.

The IPC has posted Privacy Tips for Holiday Shoppers on her website to help Yukoners better protect their personal information during this holiday shopping season.

Privacy Tips for Holiday Shoppers

When shopping at a store:

- **Cover up your Personal Identification Number (PIN) for your debit or credit card when you enter it.** PIN codes have been compromised as a result of people watching and recording your PIN code as you enter it. Watchers are everywhere and include the store clerk, other shoppers and video surveillance. Almost everyone now has the ability to take pictures and videos with their cell phones.

- **Don't let your credit or debit card out of your sight.** Credit card information has been stolen by people who take your card where you can't see it and record the information for future use.

- **Be cautious of double-swiping**. This technique has been used to send card information someplace other than the bank, such as a personal computer. This technique has also been used by store clerks who double swipe debit cards to gain direct access to cash by debiting an account for a cash-back transaction.

- **Be wary of personal information being collected.** A store should only require a minimal amount of personal information, such as your debit or credit card, to complete a purchase. If the clerk asks you for additional information such as your name, address, and phone number, ask the clerk what the legal authority is for collecting this information. There are very few circumstances that would authorize a store to collect a driver's licence number. Information on a driver's licence is sought after information by identity thieves and fraudsters. Providing this information to stores should be avoided unless their authority to collect this information is provided to you. Any request for a Social Insurance Number (SIN) should be refused.

- **Be wary of stores that don't truncate credit card numbers on a receipt or who use manual credit card machines.** Ask for your receipt. Examine it to see if your credit card number is displayed. Most receipts should only show a truncated credit card number (the last four numbers). Avoid stores that use the old manual credit card machines with carbon copy receipts as these receipts show your complete credit card information. Where your complete credit card number is shown, you should find out how the store protects this personal information.

- **Keep an eye out for suspicious point-of-sale terminals.** Identity thieves and fraudsters have been known to switch a terminal with a fake one that allows them to directly collect the card information from the terminal. If you have any suspicions regarding the terminal, report it to the store manager.

- **Report any suspicious activity to the store manager.**

When shopping online:

- **Ensure your computer security is up to date.**

- **Don't online shop using a non-secure wireless Internet.** Identity thieves and fraudsters can capture your personal information while it is being entered very easily using programs easily accessible.

- **Examine the website address and contact the store by phone before completing a purchase at an online store.** Identity thieves and fraudsters have been known to set up fake websites that look like legitimate online stores to collect your personal information, including credit card numbers. Website addresses that appear unusual are an indicator that the website is fake. Use another source to obtain the phone number of the store and phone the store to verify you have the correct website. Search comments or reviews on the Internet related to the website or store.

- **Ensure the website is secure when entering personal information.** Look for the padlock symbol to indicate the website is secure. Click on the symbol to see the identity of the website owner and that it comes from a valid Certificate Authority. Also check that the website address begins with "https" rather than just "http" as the "s" indicates it is a secure site.

- **Be wary of a requirement to enter personal information not normally required to complete a purchase, such as a driver's licence number** (see above).

- **Don't use the same username and password for each online store.** Identity thieves and fraudsters target this kind of information when hacking into store databases. They can use this information to access your personal information on other websites, where you have used the same user name and password.

- **Don't share your username and passwords with others.** Sharing your username and password for your debit and credit card may eliminate your ability to recover losses on these cards. Also, sharing this information with others creates risks where these individuals do not take adequate precautions to protect this information when using it.

General privacy tips:

- **Check your bank accounts and credit card purchases often and immediately report any transactions you did not make to your bank or credit card provider, as appropriate.** Fraudsters have been known to make small purchases or take out small amounts from bank accounts daily to avoid detection.

- **Use a low limit credit card to make online purchases.** Using a low limit credit card will eliminate the possibility of an identity thief and fraudster racking up large purchases.

- **Don't provide personal information in response to an email or telephone call.** Identity thieves and fraudsters will use a technique known as phishing to try and obtain personal information from you which can be used to steal your identity and commit fraud.

- **Don't open emails from individuals you don't recognize.** Just opening an email can launch malware or a virus onto your computer. Malware makes it possible for personal information stored on your

computer to be stolen. A virus can corrupt your computer files making them inaccessible.

- **Carry a minimal amount of personal information on you when shopping and keep this information on you at all times to avoid loss or theft.**

-30-

For more information contact:

Diane McLeod-McKay, B.A., J.D.
Information and Privacy Commissioner
867-667-8468
info@ombudsman.yk.ca