Identity Theft & Credit Cards

Consumer Tips for Prevention

Identity Theft takes many forms, but the objective of the identity thief is the same – to make a profit at your expense. A large proportion of incidents involve the fraudulent use of credit cards. Although the misuse of credit cards cannot totally be prevented, measures can be taken to reduce the risk of exposure – whether we use our cards in a store or restaurant, or make a transaction over the Internet.

"An ounce of prevention is worth a pound of cure," and if we are careless and casual when conducting credit card transactions, we expose ourselves to unnecessary risk. A conscious effort to be more vigilant can prevent a lot of grief and stress.

Applying for a NEW or REPLACEMENT card:

Card issuers offer several ways for consumers to submit an application including fax and regular mail. Once an application has been approved, it does not take more than a couple of weeks to mail a new or replacement card.

As theft from mail is a widespread problem, an unreasonable delay could be an indication of a problem in the delivery process. Incomplete, or wrong information on the application form, could also cause a delay.

- Ensure correct information is placed on a credit card application, especially a current address.
- If your expected card does not arrive within a reasonable period of time, contact the issuer to inquire about the status of the card.
- Check with your manager if you rent an apartment to see if mail has been stolen at the point of delivery.

Checking your MONTHLY CREDIT CARD STATEMENT:

Checking your monthly credit card statement is a good exercise to reconcile your record of purchases with your bank's records. Here is when you may discover that an identity thief has stolen your credit card information, even though you may still have physical possession of your card.

- Keep receipts and check off each item on the written statement, to confirm that you made the purchase, as well as to confirm the amount the merchant submitted to the bank.
- Report any discrepancies to your card issuer.
- Sign up for Internet access to your banking statements. This will allow you to review transactions before waiting for a printed statement to be delivered.

In Partnership with
The Provincial
Safe Communities Working Group

Supported by:
British Columbia
Ministry of Public Safety
and Solicitor General

Check your Credit Report:

A credit report is the key to your financial standing in the eyes of the credit industry, and may contain surprises such as inquiries from credit grantors about your credit history where an identity thief as applied for a credit card in your name.

- Obtain a **FREE** copy of your credit report from the credit bureaux. You can also pay a fee to receive an online credit report of your information.
- Look for strange credit inquiries – these could be signs of identity theft.
- Alert the publisher of the credit report as well as the credit grantor who made the enquiry about the fraud.

Identity Theft and SHOPPING:

Consumers are more likely to make purchases from restaurants, retail stores, and gas stations – where there is a physical transaction with a merchant.

Unscrupulous employees may use electronic "skimmers" to make a copy of your card information. This risk increases if you give up your card for a few minutes.

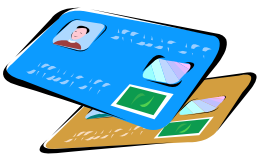
- Pay for goods and services at the cash register where you can maintain control of your card.
- Ensure your card has not been swiped more than once.
- Double check to confirm your card has been returned to you after the transaction is complete.

SHOPPING ONLINE:

- Avoid purchasing from on-line businesses that do not accept credit cards. This may be an indication of a fraudulent website.
- Purchase from well established household companies.
- Watch for indicators of a secure website: *"https"* indicates the website is **SECURE** in addition to a padlock symbol on the bottom right of your screen.
- Look for additional security features such as a ***Verisign*** symbol and/or a BBB Online Reliability Seal.
- Click on security symbols to ensure the certification is valid and issued for the website you are visiting.

Telephone "Social Engineering" – Be wary that fraudsters may pose as employees of credit card companies, for the purpose of deceiving cardholders into disclosing their credit card information.

- If you have doubts about the authenticity of the caller, take the caller's name, position and phone number. Call the issuer back using a published phone number on your monthly statement.
- Be alert to this trap! Credit companies will have your information on file, and should not ask for confirmation.



For more information on Identity Theft, please contact:

- BC Crime Prevention Association www.bccpa.org
- Consumer Measures Committee http://cmcweb.ca Click on ***"Identity Theft Kits"***
- Canadian Bankers Association 1-800-263-0231 or www.cba.ca

In Partnership with
The Provincial
Safe Communities Working Group

Supported by:
British Columbia
Ministry of Public Safety
and Solicitor General