

# Identity Theft

It's becoming more common – someone using your name and personal information to commit fraud. You may be a victim of identity theft if:

- A creditor informs you that an application for credit was received with your name and address, which you did not apply for.
  - Telephone calls or letters state you have been approved or denied by a creditor that you never applied to.
  - You receive credit card statements or you notice that not all of your mail is delivered.
- A collection agency informs you it is collecting for a defaulted account established with your identity.



: fU X'DfYj Ybh]cbH]dg'



10 Kirkwood Dr Charlotteown,  
P.E. CIA 7K2 P.O. BOX 98  
Phone: 902-629-4041  
Fax: 902-894-5508



# If it sounds too good to be true... it may be a scam

Thousands of Canadians are defrauded each year. The scams come in a number of ways – over the phone, on the Internet, or in the mail. Minimize your risk by being aware of the following common scams:

## Telemarketing

- Callers offer you “free” prizes if you buy something first.
- Callers offer you “free” or “low cost” vacations which have hidden costs.
- Callers demand that you act immediately.

## Cheque Overpayment

- You are selling an item, the buyer wants to overpay, asks you to deposit their cheque, and send them the extra money. The cheque may be fraudulent and you may lose your money.

## Letter/Email/Fax Schemes

- You are informed of an investment you didn't know you had and asked for personal information in order to claim the money.
- You are informed that a relative you didn't know you had has left you money and you are asked for personal information to claim the money.

## Pyramid Schemes

- Certain companies claim to sell products, but are more interested in recruiting people.

## Phishing

- Internet scammers pretend to be a legitimate banking site and obtain your passwords and financial data from your computer. Financial institutions DO NOT ask for personal information over the Internet or through an email.



## Skimming

- Data is obtained from the magnetic strip on the back of your debit card at banking machines or in store debit card machines. These machines have been manipulated by a fraudster.

## Identity Theft

- Personal information is retrieved from stolen mail (taken from your mailbox or garbage), your stolen wallet or purse, diverted mail delivery, a break-in to your home or business, telemarketing, or online resumes, applications or surveys.

## Protect Yourself

- Do not give out personal information on the phone or Internet unless you have initiated the contact or know who you're dealing with.
- Buy a shredder and shred mail you would otherwise throw away.
- Protect your PIN number.
- Verify all of your transactions.
- Give your SIN only when absolutely necessary. Ask to use other types of identifiers when possible.
- Don't carry your SIN card, birth certificate, or health card unless you need them. Leave them in a secure place at home.

