

## What your policy provides if you are a victim of Identity Fraud

Some Sovereign General habitational policies include Identity Fraud Recovery Expense coverage. If so, this coverage includes (with limits) reimbursement for:

- costs for notarizing affidavits or similar documents for law enforcement agencies or financial institutions
- costs for sending certified mail to law enforcement agencies or financial institutions
- application fees for re-applying for loan(s) due to the rejection of the original application
- telephone expenses for calls to businesses, law enforcement agencies or financial institutions
- earnings lost by you as a result of time off from work
- reasonable legal fees incurred, with prior notice and approval by us, for:
  - ✓ your defence against any suit(s) by businesses or their collection agencies
  - ✓ the removal of any criminal or civil judgements wrongly entered against you
  - ✓ any challenge to the information in your consumer credit report

Ask your broker for more details about these or other additional coverages.

*The Sovereign is headquartered in Calgary, Alberta, with branch offices in major centres from coast to coast. We are a prominent Canadian provider of insurance and other financial products and services through the independent broker network. Our ability to support and service independent brokers is enhanced by strategic alliances and our position within The Co-operators Group.*

Note: This brochure is for informational purposes only. The provisions of your policy prevail.

### HEAD OFFICE

Calgary

### SOVEREIGN BRANCH & SERVICE OFFICES

Halifax

Montreal

Toronto

Winnipeg

Edmonton

Calgary

Kelowna

Vancouver

Nanaimo



THE SOVEREIGN  
GENERAL INSURANCE COMPANY

A member of The Co-operators group of companies



## Identity Fraud Recovery Expense

THE SOVEREIGN  
GENERAL INSURANCE COMPANY

# Identity Fraud Recovery Expense



## What is Identity Fraud?

Identity fraud and identity theft is the unauthorized collection and use of your personal information, usually for criminal purposes.

Every year, thousands of people are victims of identity fraud. While recent developments in telecommunications and computer processing make it easier for companies and consumers to reach each other, they can also scatter your personal information widely, making life easier for criminals.

Your name, date of birth, address, credit card, Social Insurance Number (SIN), and other personal identification numbers can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, purchase vehicles, equipment or accommodation, and even secure employment.

Identity fraud is a serious crime. People whose identities have been stolen can spend months or years – and their hard-earned money – cleaning up the mess thieves have made of their good name and credit record. Moreover, victims may lose job opportunities, lose assets, be refused loans, education, or even get arrested for crimes they didn't commit.

## How to protect yourself from Identity Fraud

Minimize the risk. Be careful about sharing personal information or letting it circulate freely.

- When you are asked to provide personal information, ask why it is needed, who will be using it and how it will be safeguarded.
- Give out no more than the minimum amount of information, and carry the least possible amount with you.

- Protect your SIN; it is an important key to your identity, especially in credit reports and computer databases.
- Don't give your credit card number on the telephone, by electronic mail or to a voice mailbox, unless you know the person with whom you're communicating, or you initiated the communication yourself and you know that the communication channel is secure.
- Notify creditors immediately if your identification or credit cards are lost or stolen.
- Find out if your cardholder agreement offers protection from credit card fraud.
- Pay attention to your billing cycle. If credit card or utility bills fail to arrive when expected, contact the companies to ensure that they have not been redirected.
- Use technologies to enhance your security and privacy when you use the Internet, such as digital signatures, data encryption and "anonymizing" services.
- Access your credit report from a credit reporting agency once a year to ensure it's accurate and doesn't include debts or activities you haven't authorized or incurred.
- Ask that your accounts require passwords before any inquiries or changes can be made.
- Choose difficult passwords – not your mother's maiden name. Memorize them, and change them often. Don't keep them in your wallet or another obvious place.
- Key in personal identification numbers privately when you use direct purchase terminals, bank machines or telephones.
- Don't use bank machines and terminals if they appear tampered with.
- Be careful what you throw out. Shred personal financial information such as statements, credit card offers, receipts, insurance forms, etc. Insist that businesses you deal with do the same.

## What to do if you are a victim of Identity Fraud

- Report the crime to the police immediately. Ask for a copy of the police report so that you can provide proof of the theft to the organizations that you will have to contact later.
- Take steps to undo the damage. Avoid *credit-repair* companies: there is often nothing they can do, and some have been known to propose a solution – ie: establishing credit under a new identity – that is itself fraudulent.
- Document the steps you take and the expenses you incur to clear your name and re-establish your credit.
- Cancel your bank, phone, and credit cards and request new ones with new passwords. Ask creditors about which accounts have been tampered with or opened fraudulently in your name.
- Have your credit report annotated to reflect the identity theft. Do a follow-up check three months after to ensure that someone has not tried to use your identity again.
- Close your bank accounts and open new ones. Insist on password-only access to them.
- In the case of passport theft, advise the Passport Office immediately.
- Contact Canada Post if you suspect that someone is tampering with your mail.
- Advise your telephone, cable and utilities that someone using your name could try to open new accounts fraudulently.
- Get a new driver's license.
- If you suspect that your SIN has been compromised in any way, contact the Federal Government's Human Resources Department.