What is identity theft?

Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss.

The person whose identity has been assumed may suffer adverse consequences if they are held responsible for the perpetrator's actions.

Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.

How to protect your identity?

- Don't carry your birth certificate or Social Insurance Number (SIN) card with you. Keep them in a safe place.
- Be suspicious of emails that ask you for personal or account information. Call the comapany or organization directly to verify the emails authenticity.
- Don't list all your personal information on social media. Fraudsters can use the details you post to steal your identity.
- Check your account histories often and your credit report at least once a year to look for any discrepancies or changes your have not authorized.

How to protect your payment cards?

- When you receive a new debit or credit card, sign it immediately.
- Don't choose an obvious Personal Identification Number (PIN), such as your phone number or date of birth.
- Carry only the cards that you use and leave the others at home in a safe place.
- Check your monthly statements and notify the credit union if you see any unfamiliar transactions.
- Change your PIN often.
- Cover your PIN when punching it in.
- Keep your card insight when conducting transactions.
- Memorize your PIN. Never write it down.
- Don't tell your PIN to anyone.

How to protect yourself online?

- Change your passwords regularly.
- Don't use the same password for everything.
- Install anti-virus software to protect your data and apply security updates as soon as you receive them.
- Install anti-spyware software to keep others from gathering information about your online habits or making unauthorized changes to your computer.
- Implement a firewall to prevent unauthorized access.
- If an email looks suspicious, stop before you click.
  - Look carefully at what it claims and think about whether it makes sense.
  - Check the branding, language and spelling to judge whether it seems legitimate.
  - Call the company and make sure the email came from them.
  - Report phishing to the authorities.
- Don't clik on banner ads or pop-up windows that say "Agree", "OK" or "I Accept".
- Sign up for Direct Banking Alerts that allow you to receive notifications via text message or email about your online account activity.

Direct Banking Alerts

Direct Banking Alerts allow you to receive notifications via text message or email about your online account activity including:

- New bill payment vendor account added
- Online banking Personal Access Code changed
- Increased Authentication locked after 3 attempts
- *New* Login occurred
- *New* INTERAC e-Transfer New Recipient Added

In order to receive alerts via your email or mobile phones, you must register an email or mobile phone contact via online banking.

Before registration, you must accept the user agreement that contains the terms and provisions for use of the alerts feature. You then can proceed to register your email address and/or mobile phone to receive alerts. You can elect to receive alerts only via email, only via a mobile phone, or via both.

Registration Process

The registration process to use the Alerts feature consists of the following steps:

1. Add an email and/or a mobile contact.
2. Select the Alert you wish to receive.
3. Create the Alert.

Register for Alerts

To register for Alerts, select **Messages and Alerts > Get Started Today**

Direct Alerts provides you with an additional layer of protection and allows you to detect possible fraud quickly.

What to do if it happens to you?

Acting quickly can minimize the damage and help prevent further fraud or theft.

- Notify the credit union immediately if you suspect fraud or identity theft. They can provide advice on how to limit access to your credit card or financial accounts and investments.
- Call the police and file a report. Keep a copy of the report for your records.
- Change your PIN and passwords immediately.

Where can you get more information?

Visit any of our 6 branch locations

3rd Avenue Branch
1320 3 Ave S
Lethbridge AB T1J 0K5

Fairmont Branch
45 Fairmont Blvd S
Lethbridge AB T1K 1T1

Westgate Branch
332 University Dr W
Lethbridge, AB T1J 5C9

Taber Branch
5227 48 Ave
Taber, AB T1G 1S8

Magrath Branch
81 West Harker Ave
Magrath, AB T0K 1J0

Cardston Branch
70 3 Ave W
Cardston, AB T0K 0K0

Contact our Service Centre
Phone Number **403.320.4600**
Toll Free Number **1.866.803.0733**

Visit **www.1stchoicesavings.ca** for hours of operation and contact information.

Protect Yourself

Learn what you can do and the precautions you can take to protect yourself and your money.

1st Choice Savings and Credit Union Ltd.