Part 2

Protecting your money

The purpose of Part 2 is to provide information about how to protect your money and where to keep it. One of the most effective ways to prevent scams and fraud is to increase your awareness and level of caution. Knowing your banking options, being aware of common scams like phishing and understanding factors like interest rates will help you make informed decisions about your money.

Contents

- Part 2.1: All about banks 2
- Part 2.2 : Traditional vs. Non-traditional financial institutions 2
- Part 2.3: Protecting yourself from scams and fraud 3
- Part 2.4: Preventing elder financial abuse 5
- Part 2.5: Payday loan and cheque-cashing establishments 6
- Activity: Detecting suspicious activity 8

First Nations Child & Family Caring Society of Canada

Part 2.1: All about banks

A bank is a type of financial institution. It is an incorporated company under the Bank Act with a board of directors who are elected by shareholders of the bank.

Banks offer a place to keep your money in bank accounts and investments. You can deposit, withdraw or borrow money from a bank. Banks provide numerous financial services for a fee.

Banks are a safe place to keep your money whether you are planning to spend it, save it or invest it.

Most Canadian banks are insured by the Canada Deposit Insurance Corporation (CDIC), which protects up to $100,000 of your eligible deposits. This means that if the bank where you deposit your money goes bankrupt, up to $100,000 of your money will be safe.

- What is covered? Savings accounts, chequing accounts, guaranteed investment certificates (GICs), other term deposits, foreign currency
- What is not covered? Mutual funds, stocks, bonds, exchange-traded funds (ETFs), cryptocurrencies[1]

Part 2.2: Traditional vs. Non-traditional financial institutions

Traditional financial institutions	Non-traditional financial institutions
Banks or credit unions that have clients who keep their money in various accounts and investments. Banks lend money through credit cards and loans.	Finance companies that offer similar banking services but don't meet the legal definition of a bank.
Examples: ■ Banks: RBC, TD, BMO, Scotia, CIBC ■ Credit unions: Alterna Savings and Credit Union Limited	**Examples:** ■ Insurance firms such as Chubb Limited ■ Non-financial companies that offer banking services ■ Technology companies that offer payment options such as Apple Pay ■ Technology companies that offer small business loans such as Amazon

Why do people choose non-traditional financial institutions?

- Some people prefer specific products and services, interest rates, conveniences or perks.
- Some people may be loyal to a specific company or like that the company is dedicated to a specific service, such as an insurance company that is dedicated to providing only insurance.
- Keep in mind that non-traditional financial institutions are insured differently than traditional financial institutions.
- People may use both traditional and non-traditional financial institutions for their banking activities.

Part 2.3: Protecting yourself from scams and fraud

Anyone can become a victim of a scam or fraud. It's important to take precautions and know what to do if you become a victim.

Scam: A dishonest scheme such as phishing emails, texts or calls.

- Phishing is when a fraudster sends fake messages that try to get you to give up your personal information.
- Example: An email that claims to be from a bank saying they need to confirm your identity and you need to click on a link to confirm your account. Do not click on the link! Report it to the authorities as a phishing email.

Fraud: Deceiving behaviour with the goal of personal gain.

- Example: A cheque not written by the actual account holder that someone tries to cash or deposit for their personal gain.

Best practices

- Do not trust phone calls from someone who claims they are from a financial institution unless they already have your personal information and are not requesting it. Banks should not demand that you disclose personal information such as passwords, unless you are a client and **are calling them** or you are accessing telephone banking.
- Protect your debit or credit card PIN (personal identification number) when you are at an ATM or using a card machine. This can be done by covering the keypad with your hand.
- Do not give out private or personal information such as passwords, PIN numbers or personal facts to friends, family or companies.
- Visit or call your bank if you are unsure about transactions, calls or emails you have received.

Predatory credit and loan offers

- Predatory loans are loans with unfair, abusive or illegal terms. Or loans that the borrower cannot realistically pay back.
- A borrower can be deceived by exploitive and confusing language or miscommunication.
- Examples of predatory offers:
  - **Unsolicited offers**: A lender sends you by mail, email or telephone credit information you have not requested.
  - **Guaranteed approval:** A lender promises you a credit approval before assessing your credentials such as your credit report or income.
  - **Many and high fees:** The loan offer looks attractive at first glance, but there are fees that are not clearly addressed at the outset.
  - **Aggressive lenders:** The individual offering the credit is in a rush to complete the offer and does not want to accept your refusal.

Example of a predatory credit offer that comes in the mail

It could be a letter that includes the following points:

> ***Do you need extra cash? We have loans available!***
>
> *Apply even if you have bad credit history. There are no upfront fees and the approval process will take a maximum of 24 hours. Your money can be available as early as next week!*
>
> *Call 1-333-4567 for more information, to receive our advice or to apply!*
>
> *Thanks,*
> *William*

The above points are all very attractive at first glance. The offer is targeting those who need a sum of money immediately.

Unfortunately, this is a predatory lending offer as it does not provide all the information up front. When considering a credit offer, the interest rate and other conditions should be indicated. Additionally, credit history should be a critical part of the assessment, which can create a longer approval process than 24 hours.

What to do if you become a victim of a scam or fraud?

- Report the incident to your bank.
- Report the incident to the police.
- Contact your bank to change PINs and passwords, or cancel your credit card or debit card if it's related to the incident.
- Request a current credit report from a credit reporting agency (TransUnion‡ or Equifax‡) to ensure it does not include any false or fraudulent information. If it does, report this to the agency.
- Delete and ignore all texts or emails that are fraudulent. Report fraudulent emails to your financial institution or the authorities as phishing!

Resources

- Information about reporting fraud at RBC can be found at https://www.rbc.com/cyber-security/how-to-contact-us/index.html.
- RBC privacy and security information can be found at https://www.rbc.com/privacysecurity/ca/index.html.
- The Government of Canada resources regarding protection from fraud and scams can be found at https://www.canada.ca/en/services/finance/fraud.html.

Part 2.4: Preventing elder financial abuse

Anyone can become a victim of financial abuse, but seniors can be at higher risk – especially those who are dependent on others for care and support, or those who have adult family members who are financially dependent on them.

Elder financial abuse is when a younger person controls the financial decision-making of an older adult without their consent. This person is generally a family member, care provider or friend of the older adult. Receiving a large sum of money may increase the risk of elder financial abuse.

Examples of elder financial abuse

- Taking an older adult's debit or credit card and using it for your own purposes
- Pressuring an older adult to gift money or buy things for others
- Pressuring an older adult to lend you money, then never repaying it
- Taking an adult's groceries or other necessities and leaving them without
- Selling an older adult's property or belongings

Preventing elder financial abuse

- Be aware of red flags including:
  - A new, close friend who tries to become involved in banking or legal matters
  - Sudden bank account changes including large amounts being moved or spent
  - Strange spending patterns including what money is being spent on and how often
- Educate yourself and your loved ones on what elder financial abuse is, along with what the signs and red flags are, before it happens!
- Put a plan in place regarding an elderly adult's Power of Attorney and Will before they become unable to manage their own finances. This will ensure their finances continue to be taken care of properly.
  - **Power of Attorney:** A trustworthy individual chosen to represent an elderly person who has an illness, disability or inability to travel to be present to sign certain documents and complete other banking activities. The Power of Attorney manages their finances and should also have the elderly adult's best interests in mind when it comes to their quality of life.
  - **Will:** A document that should be prepared once an individual becomes a legal adult and is updated regularly to best reflect their current life. A Will specifies how an individual's estate (finances, property, etc.) will be distributed after their death, including what each person in the document will receive. It also appoints an executor, who will carry out the instructions in the Will and administer the estate.

It is important to have written documentation to ensure the appropriate person is responsible for an individual's finances and that an individual's estate is left to the desired people and nobody is left out.

More information on estate services for First Nations can be found at https://www.sac-isc.gc.ca/eng/1100100032357/1581866877231#chp3.

For more information on preventing elder financial abuse, please visit:

- https://www.rbcwealthmanagement.com/ca/en/research-insights/financial-elder-abuse-five-common-signs-/detail/
- https://www.rbcwealthmanagement.com/ca/en/research-insights/how-to-recognize-and-prevent-financial-elder-abuse/detail/#:~:text=Kaufman%20defines%20financial%20elder%20abuse,a%20friend%2C"%20says%20Kaufman

Province-specific information	Check out "Provincial and territorial resources on elder abuse" for province-specific information at https://www.canada.ca/en/employment-social-development/campaigns/elder-abuse/resources-province-territory.html.

Part 2.5: Payday loan and cheque-cashing establishments

Payday loan

- A short term loan provided to borrowers by private companies such as Money Direct and Payday Loan Mart.
- Used sometimes by borrowers when cash is needed fast.
- Borrowers must pay the money back once they receive their paycheque.
- Loans must be paid back in full along with fees, which are higher than rates charged by banks for personal loans and other credit products.

How do you get a payday loan?

Lenders do not require a credit check and will most often ask for proof of your identity, income and bank account information. They will either deposit the loan into a bank account or provide cash.

How do you pay back a payday loan?

Lenders require you to complete a pre-authorized debit form, which allows them to take the funds out of your bank account as soon as your paycheque is deposited. Or they will require a postdated cheque for the loan amount plus the fees.

Why should you avoid payday loans?

Payday loans have high interest rates. There are costly consequences to not paying back a payday loan by the due date. If you have trouble repaying the loan, one payday loan can lead to another and so on. The ongoing use of payday loans without paying them back in full (taking out another loan to cover the first one and then another and another) can cause interest to accumulate fast. If payments are missed or the loan is not paid back, your account could be sent to a collection agency. This will be included on your credit report and will negatively affect your credit rating. Either the lender or collection agency could take you to court. Your bank may also charge you a fee if there is not enough money in your account to cover payments to the payday loan establishment.

Example	
Payday loan amount = \$500 Fee for loan = \$15 per \$100 borrowed Weeks until paycheque is received = 2 If you pay the payday loan back on the due date. $\text{Cost} = \frac{\text{Payday loan amount}}{\$100} \times \text{fee per } \$100 \text{ borrowed}$ $= \frac{\$500}{\$100} \times \$15$ $= \$75$	This means your payday loan will cost you \$75. You will receive \$500 when you receive the payday loan and will have \$575 taken out of your account on the due date when your paycheque is deposited.

For more information about payday loans, visit
https://www.canada.ca/en/financial-consumer-agency/services/loans/payday-loans.html.

Cheque-cashing establishments

- Cheque-cashing establishments allow people without a bank account to turn their cheques into cash immediately.
- Most cheque-cashing establishments charge a fee along with interest, meaning you spend a portion of your cheque just to cash it.
- Cheque-cashing services are provided at payday loan establishments such as Cash Money.

Example	
Cashing a $200 cheque Fee per cashed cheque = $4 Interest rate = 3% Cost = fee + (interest rate x cheque amount) = $4 + (3% x $200) = $4 + $6 = $10	This means that 5% of your cheque will be spent just on cashing it.

Activity: Detecting suspicious activity

Let's check your understanding of scams and fraudulent activity!

Please indicate whether each example is suspicious or not suspicious.

		SUSPICIOUS	NOT SUSPICIOUS
1.	You receive a call from your bank that tells you to confirm your identity by requesting your driver's licence number.	☐	☐
2.	You call your bank using telephone banking and are asked to provide your password.	☐	☐
3.	You receive an email that a deceased relative has left you money in their Will, but you must first pay service fees.	☐	☐
4.	You sell a TV over social media and when you receive the cheque from the buyer, the cheque is made out for $200 more than what you asked. When you contact the buyer, they ask you to refund the extra $200.	☐	☐
5.	While in your bank's mobile app adding a new e-transfer recipient, you are asked to input a code that was texted to you to confirm the action.	☐	☐

Answers on the next page.

Answers

1. *SUSPICIOUS: You should never receive a call from your bank requesting this type of personal information. If you are unsure, call your branch location.*
2. *NOT SUSPICIOUS: When you call to access telephone banking, you are required to provide a passcode to access your account and complete transactions.*
3. *SUSPICIOUS: The inheritance scam is a common type of fraud that leaves victims with a loss if they pay the so-called "service fees". Disregard these types of emails. A notification about funds from a relative's will should not come from an email requesting money immediately.*
4. *SUSPICIOUS: The overpayment scam is where victims are paid an amount above the selling price. The victim then reimburses the fraudster for the overpayment, but the original cheque is fraudulent, so the victim receives no money and loses the money they reimbursed.*
5. *NOT SUSPICIOUS: Inputting a code that was either texted to you or recited to you over the phone to confirm adding a new e-transfer recipient is a normal action. This is to ensure you are the client connected to the account.*

[1] Protecting your deposits, CDIC (2021). https://www.cdic.ca/your-coverage/protecting-your-deposit/

126081 (02/2021)