Habib Canadian Bank
Tips and Safeguards against Fraud and Financial abuse

Financial abuse is the most common form of abuse in Canada. This brochure explains the type of fraud and scams, how you can become a victim of fraud, what you should do if you think you are a victim of fraud, and how to report fraud and scams.

Common Types of frauds and scams

GRANDPARENT SCAM

When Fraudsters target customers by calling and pretending to be a family member in distress, the police or a justice official claiming that a loved one or grandchild is in trouble, and needs money immediately. Victims are told there's a gag order, and can't speak to anyone.

- Customers should respond to situations as detailed below:

When there is a call demanding immediate payment for bail, or fines to avoid going to jail: **Remember** that the courts won't ask for cash to bail out someone in custody, and will require people to be present in court.

When someone claims to be a lawyer, police or family member in an emergency situation demanding funds: **Be suspicious** of calls that require immediate action. **Hang up!** Call your local police and contact the family member directly.

When someone requests cash and send couriers for pick up, or demand you to send by cash by courier services or via cryptocurrency: **Never send** cash, cryptocurrencies or any other funds to unknown persons, unverified addresses or bank accounts.

IDENTITY THEFT

When someone steals the personal information from another person so they can pretend to be that person and attempt to apply for a credit card, withdraw funds and much more.

There have been cases where fraudsters have obtained mortgages on a property owned by someone else by using their identity. You should keep checking your credit bureau report at regular intervals to determine if lending facilities that you don't know about have been extended under your name

MORTGAGE FRAUD

When someone provides false information on an application to qualify for a mortgage you would not otherwise get. It also includes representing on the loan application that you are going to live in the home, when you have no intention to do so.

CREDIT/DEBIT CARD FRAUD

When someone uses another person's card, or a copy of the card to make purchases or withdraw funds.

Ignore the text messages or emails sent to you mentioning that your bank account has been blocked and they require certain information to change the passwords.

ONLINE SCAMS

There are many online scams, more recently, there are many online scams involving COVID-19 and false information. Most online scams come in the form of an email or a text message being sent from what seems to be an organization or person that you know, when in reality they are not.

Many times people receive text messages or emails mentioning that their bank account has been blocked and they need to change the password to access it. For such cases, contact your nearest Branch Manager to validate the message. Ignore emails from unknown senders and block the sender from sending additional suspicious emails.

PHONE & DOOR-TO-DOOR SCAMS

When someone calls or comes to your door posing as a representative from an organization and tries to get you to give them money or personal information."

Crime and abuse by relatives and caregivers

This includes the full range of crime and abuse, including physical, emotional, and sexual abuse, as well as financial exploitation and neglect. There are three general categories of offenders:

1. Adult children, grandchildren, and other relatives;
2. Professional caregivers; and
3. Close friends or others in a position of trust

Financial exploitation occurs when a person in a position of trust steals, withholds, or in some way misuses the victim's money or property for personal benefit.

The indicators of exploitation may include:

- A new acquaintance shows an interest in finances, offers care, and ingratiates him/herself with the victim;
- A relative or caregiver is experiencing financial problems and is showing undue interest in the financial affairs;
- Basic bills are not being paid;
- A relative or caregiver isolates the victim, by limiting access to him/her by phone or in person;
- Bank and credit card statements are sent to the relative or caregiver, rather than to yourself;
- There is an unusual amount of banking activity after joint accounts are set up or someone new begins to help with finances;

Financial crimes by strangers

A variety of fraudulent schemes fall in this category, which includes:

1. Ponzi schemes (investment);
2. False promises of prizes;
3. Aggressive telemarketing;

4. Schemes involving health products and;
5. Fraudulent home repairs

Factors increasing fraud committed by strangers includes:

- Home ownership;
- A tendency to not solicit advice before making a purchase;
- Financial risk-taking behaviour;
- Lack of knowledge of consumer rights;
- Lack of awareness of fraudulent schemes;
- Openness to marketing appeals;
- A reluctance to hang up the phone on telemarketers

Tip and safeguards

1. Protect yourself–keep your financial and personal information in a safe place.
2. Have an enduring or continuing power of attorney prepared appointing someone you can trust to look after you, so that even if you are ill and unable to look after yourself, your finances will be protected from others who might try to take advantage of you.
3. Ask for help if you think you are experiencing financial abuse.
4. Keep a record of money you give away and note whether it is a loan or a gift.
5. For major decisions involving your home or other property, get your own legal advice before signing documents.
6. Ask someone you trust to look over contracts and other papers before you sign them.
7. Be very cautious if you open a joint bank account – the other person can take away all the money without asking.
8. Make an effort to keep in touch with a variety of friends and family so you don't become isolated.
9. Keep all personal documents in a secure place. If you don't need them, do not carry your birth certificate, passport or SIN card.
10. Never tell another person your PIN or account passwords and take care to cover your hand when entering your PIN at bank machines and when making store purchases.
11. Safely dispose of old bills and statements–shredding is best.
12. Do not click on pop-up windows or respond to e-mails, open attachments or go to Website links sent by people you do not know. Your bank or credit union will not send you anything by e-mail unless you ask them to.
13. Never give out your credit card, bank account, or personal information to someone over the phone, at the door, or over the Internet unless you know the person or organization you are dealing with, or you made the contact.
14. Do not sign an agreement or contract to buy anything without giving yourself time to think it over. If a salesperson insists that an "offer" is "time limited" and you must decide that moment, it is probably better not to buy.
15. Be suspicious if someone you don't know asks you to send them money or a cheque, or to return money they "accidentally" sent you.
16. Before hiring someone or agreeing to have work done on your home, ask for proof of identity and references and check them.
17. Avoid using old e-mail chain threads, especially where old threads are continuously used to send new messages

Report the Fraud and Scam

If you believe you have been scammed, contact your local police and the Canadian Anti-Fraud Centre at: 1 (888) 495-8501.

All fraud and scams should be reported, even if the amount of money is too small. You can help to stop others from being victims of such abuse by reporting the fraud and scam at the above number. If you have a hearing or speech impairment and use a teletypewriter (TTY), call 1-800-926-9105. The Government of Canada offers a variety of programs to help you. Visit Canada.ca/Seniors or call 1-800-OCanada (1-800-622-6232) to learn more.

Contact us at Habib Canadian Bank

If you have any questions or concerns, please contact us at:

Email: concerns@habibcanadian.com

Fax: 905-276-5400

Mail: 6450 Kitimat Rd, Mississauga, ON L5N 2B8