FRAUD IN 3D

Detect, Denounce, Deter

Anyone can be the victim of a scam,
regardless of age, education
or place of residence.

Most incidents of fraud can be avoided.
To protect yourself effectively, stay vigilant
and learn to recognize fraud.

BANK OF CANADA
BANQUE DU CANADA

TABLE OF CONTENTS

Bank note counterfeiting 03

Identity theft and fraud 06

Payment cards fraud 10

Urgent Request scam 12

Romance scam 14

Corporate fraud 16

Ransomware 17

Bank scam 18

Fraud related to crypto assets 19

To get help or report fraud 22

BANK NOTE COUNTERFEITING

Checking bank notes: It's on the money!

Cash is a convenient and quick method of payment. Everyone uses it, which is why counterfeiters are interested in it. Each time you accept a bank note without checking it, you are at risk of becoming a victim of counterfeiting.

Whether you're the clerk or the customer, you can help stop counterfeit notes from entering the cash flow. When businesses lose money to fraud, the cost is often passed on to you, the consumer.

Canadian bank notes have security features that are easy to check and hard to counterfeit. Routinely checking the security features of all notes is your best defense against counterfeiting. Here are some tips:

- Compare a suspicious note to one you know is genuine.
- Check two or more security features.
- Look for differences, not similarities.
- If you do not know how to check a paper note, ask for a polymer note instead.

How to check polymer notes?

Feel, look and flip

- Feel the smooth, unique texture of the note. It's made from a single piece of polymer with some transparent areas.
- Look for transparency in the large window.
- Look at the detailed metallic images and symbols in and around the large window.

The Vertical $10 Note

Here are some additional security features to be checked for this note:

- Look at the pattern in the eagle feather. Tilt the note to see the pattern move up and down, and the colour shift from gold to green.
- Feel the raised ink on the portrait, the word "Canada" and the large number at the bottom.
- Flip the note to see the library ceiling and maple leaves repeated in the same colours and detail on the other side.

Older series

To learn more about the security features of older bank note series, visit **www.bankofcanada.ca/banknotes/bank-note-series/#past**.

Did you know?

- **It is a criminal offence to knowingly pass counterfeit bank notes on to someone else.**
- **You are not legally required to accept a bank note if you doubt its authenticity.**

If, **DURING** a transaction, you suspect that you have been given a counterfeit note:

- politely refuse the note and explain that you suspect it might be counterfeit;
- ask for another note (and check it too);
- advise the person to check the suspicious note with local police;
- inform your local police of a possible attempt to pass counterfeit money.

If, **AFTER** a transaction, you notice that you have accidentally accepted a note that may be counterfeit, give it to your local police for examination. If it turns out to be genuine, you'll get your money back.

TO GET HELP OR REPORT FRAUD

Report the incident or take the suspect note to local police.

For more information on bank notes, contact the Bank of Canada at **1-800-303-1282** or visit **www.bankofcanada.ca/banknotes**.

IDENTITY THEFT AND FRAUD

WHAT IS IT?

Identity theft occurs when a person obtains your personal information for criminal activity without your knowledge or consent. **Identity fraud** is the fraudulent use of this information to:

- gain access to your bank accounts, apply for loans or credit cards, or open accounts (bank, client);
- sell your property without your knowledge;
- obtain passports or receive government benefits; or
- obtain medical services;
- make purchases without your knowledge;
- impersonate your social media profile to promote fraudulent ads;
- obtain cell phone accounts;
- conceal criminal activities.

WHAT DO FRAUDSTERS DO?

- Steal your wallet, purse or residential mail.
- Search your garbage or recycling for bills, bank statements or other documents.
- Complete a change of address form to redirect your mail.
- Call you, pretending to be your creditor, your landlord, your employer, a government agent, an investigator or an alleged lover.
- Send unsolicited emails or text messages that appear legitimate to collect your personal information or create imitations of legitimate websites or applications (such as banking websites, business websites or social media websites).
- Trick you into giving them access to your electronic devices (computer, phone or tablet) in order to hack them.
- Tamper with automated banking machines and point-of-sale terminals.

MAIN PERSONAL INFORMATION / IDENTIFIERS

- **Full name**
- **Date of birth**
- **Home address**
- **E-mail address**
- **Telephone number**
- **Passwords**
- **Social Insurance Number (SIN)**
- **Health insurance number**
- **Signature (handwritten or digital)**
- **Passport number**
- **Driver's license number**
- **Payment card data**
- **Finger or voice print**
- **Retina or iris image**
- **DNA profile**

HOW CAN YOU PROTECT YOURSELF?

Communication of personal information

- Be vigilant in all your communications, whether in person, on the phone or online. Provide your personal information only when strictly necessary. Before giving your information, make sure that you know the people or organizations you are doing business with and that it was you who made contact with them.

Security and privacy settings

- Check your privacy and security settings before downloading applications, registering on a website or sharing personal information on social media. Consider everything you post to be public information.
- If possible, use two-factor (or multi-factor) authentication. This additional protection measure makes it possible to associate information that you know (your password) with information that you have (a code sent by SMS, a token, a fingerprint, etc.).
- Deactivate the automatic geolocation feature on your telephone. Carefully review usage and privacy policies before activating a location service.
- Protect your information. Lock your computer and mobile devices whenever you are not using them.
- Use secure websites (beginning with "https://") whenever you have to communicate personal or financial information.
- Avoid consulting personal information, making financial transactions or purchases on public wireless (Wi-Fi) networks (e.g., in a café, in an airport).
- Make sure you are conducting your transactions on legal websites. Choose to download a retailer's mobile application from their secure website.
- Log out before leaving your computer.
- Never keep photos of your driver's licence, passport or health insurance card on your mobile devices unless you lock them with a password.

Antivirus software and passwords

- Install antivirus software, a spam filter, a firewall and a spyware blocker on your electronic devices. Activate the spam filter in your inbox. These measures will help reduce your vulnerability to hacking.
- Update your devices regularly.
- Protect your home's Wi-Fi network with a complex password that contains at least 10 characters. Avoid dictionary words. Insert special characters in the middle of the word (avoid using upper-case letters at the beginning and numbers or special characters at the end of the word). Avoid replacing letters with special characters (e.g., a = @).
- Memorize your passwords and change them regularly (including your router password). Never use the same password for more than one site. Never allow a website to "remember your password."

Personal identification number (PIN)

- Memorize your PINs so that you do not have to keep a written record of them. When entering your PIN, make sure that no one around you can see it, including the clerk.

Social Insurance Number (SIN)

- Protect your Social Insurance Number (SIN). The S.I.N. is issued by the federal government for employment purposes, access to government programs and benefits, and for tax purposes. Refer to Service Canada for a list of public agencies that have legislated or regulated the collection of the SIN

Official statements

- Check your bank and credit card statements regularly. Immediately dispute any purchase you do not recognize.
- Shred all documents containing personal information before you discard them.

Free software and applications

- Before you install free software or applications, read the licence agreement and privacy policy to avoid giving virtually unlimited access to your personal information.

Email / Text messages

- Check the sender's email address on every message you receive. Always think twice before you click on a link or open a file of unknown origin. Delete the email if you do not know the sender. Never confirm personal information by email.
- Report a fraudulent text message for free by forwarding it to your mobile phone provider at 7726 (SPAM).

Mail

- Make sure you receive your mail.

Notify your post office, service providers and financial institutions if you move away.

TO GET HELP OR REPORT FRAUD

- Immediately contact your financial institution and credit card company.
- Report the incident to local police.
- Report stolen or lost documents or identification (e.g., driver's license, immigration document, health card) promptly to the appropriate authorities.
- Contact both national credit rating agencies and request that a fraud alert be added to your credit report.

Equifax Canada: 1-800-465-7166
TransUnion Canada: 1-877-713-3393

Contact government agencies for additional protection measures:
Revenu Québec: 1 800 267-6299
Canada Revenue Agency (CRA): 1 800 959-7393
Service Canada: 1 866 274-6627

Report the incident to the organizations or companies that hold your personal information (e.g. RAMQ, SAAQ, Hydro-Québec, Canada Post).

Contact the **Canadian Anti-Fraud Centre** to report the fraud at **1-888-495-8501** or visit **www.antifraudcentre-centreantifraude.ca**.

On a regular basis

- Check your credit file with TransUnion or Equifax. Make sure there are no errors.
- Check your tax information to detect any irregularity with the revenue agencies.

PAYMENT CARDS FRAUD

WHAT IS IT?

Payment cards fraud refers to fraud committed using credit or debit cards, or the information from these cards, to obtain funds or acquire goods.

WHAT DO FRAUDSTERS DO?

- They look over your shoulder during a transaction (e.g. at self-service checkouts) to see your personal identification number (PIN).
- They create a diversion or take advantage of a momentary lapse of attention to steal your personal belongings, including those left in your vehicle (e.g. steal your wallet or your payment cards).
- They use different techniques — phishing, hacking, extortion, or cloning — in order to obtain your credit card information (e.g. number, expiration date and security number/CVV).

HOW CAN YOU PROTECT YOURSELF?

If you are a consumer:

- Keep only the cards you need with you and make sure the rest are in a safe place.
- Report your card as lost or stolen as soon as you notice it's missing.
- Never lend your payment card to anyone and never share your PIN.
- Check your bank and credit card statements regularly. Immediately dispute any purchases you do not recognize.
- Swipe your card yourself when you make a transaction and never let it out of your sight.
- Protect your PIN. Choose one that cannot be easily guessed, memorize it, and change it regularly. Do not use your date of birth, telephone number or address. Make sure that your PIN is not recorded on any documents and shield it from prying eyes when making transactions.
- Beware of calls, emails or text messages that claim to be from your financial institution or a government agency requesting personal or banking information.
- Sign your new credit card and don't lend it to anyone.
- Destroy your expired payment cards in a safe manner.
- Report any unusual situation to your merchant, financial institution or your local police department.

If you are a merchant:

- Be wary of equipment purchases over the phone, especially when high value merchandise is involved. Confirm the identity of the credit card holder with identification.
- Report any unusual situation to your financial institution or your local police department.

TO GET HELP OR REPORT FRAUD

- Contact your financial institution or credit card company immediately.
- Report the incident to local police.
- Contact both national credit rating agencies and request that a fraud alert be added to your credit report.

Equifax Canada: 1-800-465-7166

TransUnion Canada: 1-877-713-3393

- Contact the **Canadian Anti-Fraud Centre** to report the fraud at **1-888-495-8501** or visit **www.antifraudcentre-centreantifraude.ca**.

URGENT REQUEST SCAM

WHAT IS IT?

In this scam, the victim is solicited by telephone, text message or email by individuals posing as government agents (revenue or immigration), police officers or head office employees. They may also pose as an investigator for a credit card company, or an advisor for a financial institution. Fraudsters will invoke a variety of urgent reasons (e.g. unpaid taxes or incomplete administrative records) to induce you to pay a sum of money or reveal personal information.

WHAT DO FRAUDSTERS DO?

- Create a sense of panic or urgency. They tell you that your payment card, social insurance card or bank account has been defrauded. They use threats (fines, lawsuits, deportation, arrest warrants) made in an aggressive tone or strong pressure to scare you into immediate payment.
- Ask you to buy prepaid cards and provide the activation codes on the back of the card; to buy cryptoactives or prepaid vouchers; or to transfer a sum of money by wire transfer or check.
- Maintain constant pressure on the victim, even going so far as to accompany them over the phone throughout the payment process.

HOW CAN YOU PROTECT YOURSELF?

- **Hang up.** Do not give in to pressure. Be careful and skeptical.
- Be aware and remember that government agencies and police forces never:
  - ➤ contact citizens in the purpose of exorting or demanding personal or financial information;
  - ➤ use a threatening tone or exercise undue pressure when making requests for payment;
  - ➤ accept payments for reimbursements using prepaid cards.
- Never assume that the phone number on your call display is accurate. Fraudsters use software or applications to fool their victims. Find the official telephone number of the agency that contacted you, and call to verify the authenticity of the request.

TO GET HELP OR REPORT FRAUD

- Report the incident to your local police.
- Contact the **Canadian Anti-Fraud Centre** to report the fraud at **1-888-495-8501** or visit **www.antifraudcentre-centreantifraude.ca**.

FRAUD ALERT TARGETING SENIORS!

FAKE REPRESENTATIVE OF A BANKING INSTITUTION

The fraudster impersonates a so-called "financial advisor" or "investigator" and states that you have been a victim of fraud (e.g., fraudulent transactions have been identified on your credit card). They may ask you to confirm personal information and encourage you to purchase prepaid cards to assist in the investigation or to transfer money. Under the pretext of protecting your money or obtaining new cards, (s)he asks you to hand over your cards and your passwords (e.g. PIN) in an envelope, which an accomplice (e.g. a fake police officer, a fake courier, a fake Canada Post employee) will pick up at your home.

Some tips:

- Refuse. Don't be afraid to say no and hang up. Fraudsters may raise their voice, be insistent or use false threats (e.g. putting you under arrest) to get your cooperation.
- Keep in mind that no government agency uses a threatening tone or applies undue pressure to such requests.

GRANDPARENT SCAM

In this type of scam, a fraudster specifically targets seniors over the phone pretending to be a member their family or someone close to them.

- A fraudster may ask a senior if he or she recognizes him or her;
- If a senior responds by giving the name of a relative they think they recognize over the phone, the fraudster uses this identity to establish a bond of trust with the senior.

The fraudster will then use a situation of distress (e.g., an accident, arrest) that requires immediate financial assistance (e.g., wire transfer, cash, gift cards). They will ask the senior not to tell anyone about the situation.

They may also ask the victim to lie to the financial institution employee about the reasons for the withdrawal (e.g., for renovations).

Fraudsters count on a sense of urgency and capitalize on the victim's emotional response to obtain what they want. Their accomplices can impersonate a police officer or a professional (e.g., doctor, lawyer), to increase the credibility of the scenario.

A few tips:

- Be careful if someone calls you and asks if you recognize them. Don't answer and ask them to identify themselves instead.
- Authenticate the identity of the person by asking personal questions that only your relative would be able to answer.
- Contact another family member to verify the validity of the request.
- Never send money to someone you do not know.
- Do not hesitate to end the communication.
- Stay calm and resist the urge to act quickly (even if the situation seems urgent).

ROMANCE SCAM

WHAT IS IT?

In a romance scam, the scammer contacts his or her victim through social media, apps or dating sites. Using seduction techniques (flattery, compliments), the scammer builds trust with the victim and reveals romantic feelings for them. Once the relationship is established, the scammer uses various pretexts to extract money from his victim.

WHAT DO FRAUDSTERS DO?

- Create fake profiles on social media, apps or online dating sites and show an interest in developing a "serious" relationship.
- Patiently build the "relationship." The fraudster makes his victim experience a love story that meets his/her ideal of love, his/her dreams and his/her needs.
- Pretend an urgent need of money for reasons such as: come and meet you, visit a sick parent or child, pay hospital bills, deal with customs problems, because of a job loss or a financial problem.
- Use various pretexts to justify the impossibility of video or telephone contact.
- Contact their victim again to ask for forgiveness (following a fraudulent transaction), reiterate their feelings and try to get more money from their victim using a new strategy.
- Isolate the victim from her family or circle of friends and insist to keep their relationship secret from them.
- Manipulate the victim in such a way as to increase their feeling of guilt and hold them responsible for any drama or "failure" linked to the relationship.
- Use emotional blackmail or psychological violence (e.g. threatening to break up) when the victim refuses a request or expresses doubts.

HOW CAN YOU PROTECT YOURSELF?

- Be careful and skeptical on dating sites, apps and social media.
- Stick to official platforms where you can retrace your exchanges.
- Do not accept friend requests from people who you do not know.
- Never send money to someone you only know virtually. Refuse any transaction for a third party.
- Never share your banking information.
- Do not share explicit photos or videos.
- Keep screenshots or photos of fraudulent identities to report them, if necessary.

- When in doubt, talk about the situation with someone you trust.

Advice for the senior's family and friends.

Be on the lookout for unusual aspects. Be a good listener, avoid confronting the person directly. He or she is really in love. Instead, sow small doubts by asking about certain unusual aspects of the situation. The most important thing is to preserve the communication link with your loved relative or friend.

TO GET HELP OR REPORT FRAUD

If you suspect or know that you have been a victim of a romance scam, report the incident to:

- your financial institution
- your local police
- the **Canadian Anti-Fraud Centre** at **1-888-495-8501** or at **www.antifraudcentre-centreantifraude.ca**.

CORPORATE FRAUD

CEO fraud: The scammer claims to be an executive (for example, the chief executive officer [CEO] of a company) and requests that a significant amount of money be transferred to a foreign bank account, using the pretext of an urgent and confidential tender offer. A so-called "lawyer" may follow up by providing specific instructions for the transfer of funds. When this type of fraud occurs, the actual CEO is frequently out of the country.

Fake supplier: The scammer claims to be a supplier and requests an online payment to a different bank account than the one normally used. It is only during a real exchange with the legitimate supplier that the company discovers the fraud.

Fake representative: The scammer claims to be a representative of the company's financial institution and explains that they need to implement or update the IT platform. This deception leads the victim to divulge the account number and password. The fake representative tells the victim not to perform any transactions for the next 24 to 48 hours (which gives the scammer enough time to transfer funds to international bank accounts).

HOW CAN YOU PROTECT YOURSELF?

- Educate your staff about these strategies, your company's transaction (or transfer) procedures and all other safety measures that have been established.
- Validate that the person is who they say they are in all your communications. Be vigilant about any requests to change suppliers' bank details.
- Use a complete security solution that offers protection against ransomware, spam and Web navigation.

TO GET HELP OR REPORT FRAUD

Were the funds transferred within the past 24 to 48 hours? Contact your financial institution immediately to block the international transfer.

- Report the incident to local police.
- Contact the **Canadian Anti-Fraud Centre** to report the fraud at **1-888-495-8501** or **www.antifraudcentre-centreantifraude.ca**.

RANSOMWARE

WHAT IS IT?

Criminals use a malware which, when it infects a computer, locks access to files and the operating system, making data inaccessible. A ransom, payable by a crytpocurrency (such as bitcoin), appears on the screen in exchange for the decryption key.

The infected computer remains functional overall, but work documents are inaccessible.

The user is unable to open them with the usual software. Fraudsters may even go so far as to invite the victim to contact a fake computer technician.

HOW CAN YOU PROTECT YOURSELF?

- Do not click on a link or open a file of unknown origin in an email or text message. Request assistance from a dedicated technician (if required) and avoid contacting "online technicians."
- Regularly install updates of your computer's operating system: most ransomware takes advantage of flaws that can be avoided.
- Use a complete security solution offering protection against ransomware, spam and Web navigation.
- Establish a procedure for backing up the contents of your devices: consider the frequency of backups based on the nature and value of the data. Make sure backups are stored outside the common network (e.g. on an external hard drive).
- Secure your remote desktop services: use secure remote access services such as a virtual private network (VPN), which requires double authentication and strong passwords (fees apply).
- Limit the use of administrator accounts on your operating system: users should only have the access necessary to perform their tasks.
- Raise awareness of other users of the network, if it is shared (e.g., family using the same Wi-Fi at home, a company using a shared network).

WHAT SHOULD YOU DO IF YOU ARE A VICTIM OR RANSOMWARE?

- Quickly unplug the computer to prevent theft or encryption of files.
- Report the incident to the Canadian Anti-Fraud Centre and your local police department.
- Do not pay the ransom. Paying the ransom does not guarantee that you will recover your data and encourages the attacker to strike again.

BANK SCAM

WHAT IS IT?

This is a strategy where a scammer contacts victims (e.g. at school, at work, on social media) to offer them the chance to win money very easily.

WHAT DO FRAUDSTERS DO?

- They convince their victim to "lend their bank account" for the purposes of one or several transactions in exchange for financial compensation.
- They ask the victim to divulge their personal information as well as their bank account and debit card details.
- They deposit funds to the victim's account (e.g., by a bank transfer or using a photo of a cheque).
- They go to the victim's home to collect their debit card. They attempt to withdraw money at the automated banking machine. When this fails, the victim is threatened by the scammer.
- They geolocate a victim and thus obtain personal information (e.g. where they live or work), in order to threaten or blackmail them if they refuse to take part in a fraud.

HOW CAN YOU PROTECT YOURSELF?

- Never "lend" anyone your bank account for payment. Never let anyone borrow your debit card.
- Never share your banking information (PIN).

TO GET HELP OR REPORT FRAUD

- Report the incident to local police.
- Contact the **Canadian Anti-Fraud Centre** to report the fraud at **1-888-495-8501** or **www.antifraudcentre-centreantifraude.ca**.

What if you receive an offer to make "easy money" or you are offered a job "without an interview"?

Refuse it. It's probably a scam.

Anyone who participates in this type of fraud will have their record with the financial institution marred for fraudulent bank account use.

Criminal charges for fraud may also be laid against you for participating in the fraud.

FRAUD RELATED TO CRYPTO ASSETS

WHAT ARE THEY?

These are schemes that use crypto assets. These currencies are accessible worldwide and can easily cross borders, which makes them very interesting for fraudsters outside the country. Fraudsters take advantage of the benefits of crypto assets to facilitate fraud (as payment) and to perpetrate it through various schemes (e.g. fraudulent investments or investment platforms).

In Canada, only the Canadian dollar is legal tender.

WHAT DO FRAUDSTERS DO?

- They run misleading ads on social media, or use influencers, to capture a victim's interest, and lure him or her in with glowing returns.
- They entice a victim to view their content online and make contact with them.
- They establish a relationship of trust with a victim thanks to their alleged knowledge.
- They invite a victim to invest or transfer their crypto assets to fake online trading platforms. For a period of time, the victim thinks they'll see their investments grow, when in reality they're being hijacked without their knowledge. However, they become aware of the scam, for example, when they are asked to pay additional sums to withdraw their false earnings, or when they realize that they can no longer withdraw their assets from the platform.
- Fraudsters may also impersonate a government official or develop a virtual relationship with a victim, in order to extract crypto assets under various pretexts (see urgent request scam and romance scam).

HOW CAN YOU PROTECT YOURSELF?

Be an informed investor

- Visit the **Autorité des marchés financiers** and the **Canadian Anti-Fraud Centre** websites to stay informed about new trends in fraud and crypto assets.
- Beware of promises of high returns on low-risk investments.
- Don't be charmed by a visually appealing website or a dynamic platform. Fraudulent sites are well-designed and give the appearance of being professional and reliable.
- Carefully read and keep all documents related to your crypto assets.

Do your due diligence before investing

- Check the crypto asset trading platform's **registration** on the AMF's web site.
- Consult the **blacklist** available on the AMF website which lists websites or online platforms whose activities involve high risks. Yet, remain vigilant since this list is not exhaustive. Do not assume that the platform is reliable just because it is not on the blacklist.
- Make sure that the broker you are dealing with is duly registered with the AMF.
- Verify the legitimacy of your contact, whether in person, by telephone, by e-mail, by Internet, etc. To provide a legal financial service, your contact must have an authorization. Beware of advisors who claim to be licensed overseas and who solicit clients in Canada.
- Do some research on the Internet about the companies or platforms that are being offered to you. Often, a short search will reveal that other users, organizations, or individuals, are reporting that it is a scam.

Be careful on the Internet and more specifically in your crypto asset transactions

- Use secure sites (beginning with "https:\\").
- Be vigilant, keep your personal information safe. Never disclose your private keys or passwords to third parties.
- Be wary of platforms that keep private keys when making purchases.
- Never give access to your computer remotely.
- Substitute your virtual wallet for one or more physical wallets to store your crypto assets.

TO GET HELP OR REPORT FRAUD

If you suspect or know you have been a victim of crypto asset fraud, report the incident:

- To your local police department.
- To the **Canadian Anti-Fraud Centre**
  by phone at **1-888-495-8501**
  or via the Internet at
  https://antifraudcentre-centreantifraude.ca/.

Notes

TO GET HELP OR REPORT FRAUD

If you suspect that you are a victim of fraud, contact your local police.

For information on currency counterfeiting prevention, contact the Bank of Canada at **1-800-303-1282** or visit **www.bankofcanada.ca/banknotes**.

To learn about the security features on American bank notes, visit **www.uscurrency.gov**.

To contact the Sûreté du Québec: **911**
If not urgent, dial **310-4141** or ***4141** (from your cell phone)

To contact the Service de police de la Ville de Montréal: **911**

If not urgent, dial **514-280-2222** or contact your neighbourhood police station directly at **514-280-01XX** (**XX** represents the number of your neighbourhood police station).

To contact the Service de police de l'agglomération de Longueuil: **450-463-7011**

To contact the Service de police de Laval: **450-662-4242**

To report fraud to the Canadian Anti-Fraud Centre: **1-888-495-8501** or visit **www.antifraudcentre-centreantifraude.ca**.

To report fraud or any other criminal activity anonymously and confidentially:
For the Montréal region, call Info-Crime at **514 393-1133** or visit **www.infocrimemontreal.ca**.

Outside the Montréal region, call Échec au crime at **1-800-711-1800** or visit **www.echecaucrime.com**.

For support, contact :
Info-Social 811
1 866 LE CAVAC (532-2822) or visit **www.cavac.qc.ca**

To download a copy of Fraud in 3D:
https://www.bankofcanada.ca/wp-content/uploads/2020/02/fraud-3d.pdf

March 2024