Help safeguard your organization against **fraud**

At BMO, we're driven by our Purpose to **Boldly Grow the Good *in business and life*** and this means helping to keep our clients protected. Our Financial Crimes Unit works around the clock to keep you safe, but you also have an important role to play in keeping your financial information secure. Below, you'll find tips to help protect your organization from falling victim to fraud.

Help protect your organization from these common financial frauds

Fraud type	How to help protect your organization
Business email compromise (BEC) & Payment Fraud A form of social engineering, often occurs when a fraudster sends an email message and makes it appear to come from a known source such as an executive or accounts payable representative, who is making a legitimate request. BECs frequently lead to payment fraud scams.	• Establish a callback process for any changes to payments or account numbers, particularly electronic instructions. • Adopt internal controls such as a secondary approver. • Limit what is posted on social media, particularly for those in sensitive roles.
Credit card fraud Involves a credit card transaction not performed by the cardholder including lost or stolen cards, merchant terminal tampering and identity theft.	• Report a lost or stolen card as soon as possible. • Whenever possible remember to use the chip technology over the magnetic stripe. • Monitor your accounts for transactions you don't recognize. • Never share personally identifiable information (PII) on an unsolicited call. • Sign up for security software that monitors your information on the dark web.
Cheque/check fraud One of the most common frauds affecting businesses today. Cheques are often intercepted via the mail and altered, washed or reproduced as a counterfeit.	• Consider using electronic payments instead. • Adopt controls: Disable dormant cheques, close unneeded accounts, review accounts report, complete account reconciliation. • Take advantage of BMO Business Technology Services such as Positive Pay. • Keep cheques in a secure location and destroy unneeded ones.
Account takeover (ATO) Occurs when a bad actor gains unauthorized access to a client account and executes fraudulent transactions. Primarily it occurs through digital channels but can also occur in-person or via phone.	• Limit what's posted on social media. • Establish process where every payment requires a separate initiator and active approver (dual approval). • Delete emails containing private OLBB information such as Customer and User ID. • Ensure any sensitive site has a closed lock in the address bar. • Segregate work and personal technology and implement and maintain anti-virus software. • Implement multifactor authentication.

Continued

Tips to help protect your organization

Follow these tips to help protect your organization from fraud

Effective oversight

- ✓ Implement transaction monitoring and multifactor authentication.
- ✓ Create checklist of what to do in a situation of fraud.
- ✓ Educate employees on common social engineering ploys and methods for cyber and fraud attacks.
- ✓ Carefully establish procedures and controls for vendors with whom you do business.

Separation of duties

- ✓ Require a separate initiator and active approver for payments.
- ✓ Encourage mandatory leaves for sensitive positions.
- ✓ Create and train back-up administrators to cover leaves or emergencies.
- ✓ Speak to BMO about designating a Fraud Contact.

Managing access

- ✓ Review employee access privileges regularly for suitability and departures.
- ✓ Restrict access to personnel master records.
- ✓ Control vendor and master files and cheque writing capabilities.
- ✓ Communicate the importance of using work technology for only work.

Avoiding fraudulent websites

- ✓ Do not access BMO's Online Banking for Business (OLBB) website using a search engine; when in doubt navigate to bmo.com.
- ✓ Ensure any sensitive site has a closed lock or tune icon in the URL.
- ✓ Bookmark the bmo.com site for future access.
- ✓ Install Trusteer Rapport.

Working remotely

Adopt these tips to help protect your organization when working from home

- ✓ Change your default Wi-Fi password and set up a guest network.
- ✓ Keep router firmware up to date.
- ✓ Connect IoT devices to a separate network such as a guest network.
- ✓ Consider disabling the mic on virtual assistants such as Alexa and Google Home, unplug them while working, or keep them away from your work area.
- ✓ Be aware of your work conversations and their confidentiality.
- ✓ Always lock your screen when away from your computer.
- ✓ Keep personal and work devices separate.

Quick tips to help protect your personal accounts

- ✓ Never share your password — including with your bank.
- ✓ Use multifactor authentication.
- ✓ Keep your contact information up to date.
- ✓ Sign up for banking alerts.
- ✓ Choose strong and unique passwords.
- ✓ Recognize common scams and the red flags to help avoid them.
- ✓ Keep an eye out for phishing attempts.
- ✓ Secure your devices.
- ✓ Review additional fraud awareness materials on BMO.com. (Canada | U.S.)

Reporting a fraud incident

Develop a fraud reporting plan and share it with your employees

1. Collect all relevant information.
2. Contact your BMO Relationship Team, Client Services team or Help Desk – they will collect information, start an investigation and recovery process (if applicable) and provide guidance.
3. If your systems are potentially compromised:
   - Request your OLBB access be temporarily locked.
   - Contact a reputable local cyber security professional.
4. If your OLBB account has an unauthorized transaction or is compromised:
   - Provide all information to your BMO Representative as soon as possible.
5. File a police report, including as much information as possible.
6. Contact your insurer to report any incident involving possible loss of funds or data.
7. Complete a cyber security forensic analysis to have them check, clean and audit your systems.
8. Contact your BMO Representative to restore OLBB access and services.

Learn more at BMO.com/security