



Managing Your Corporate Card Fraud Risk: Tips & Red Flags

No matter the type of business, the risk of fraud is always present. We are committed to providing you with support to help minimize the exposure of your BMO® or your Diners Club® corporate card to fraud. This **Tips & Red Flags** checklist includes a number of best practices you can implement to help prevent payment fraud and protect yourself from data breaches. We strongly recommend that you review and implement the items contained in the checklist and share with other cardmembers in your organization.

Need assistance?

If you have any questions about the information in this checklist, please contact your BMO Representative.

To report suspicious emails and websites

Online.fraud@bmo.com

For Corporate Cards

BMO Corporate Cards:

1-800-361-3361 or call collect 514-877-0330

Diners Club® Corporate Cards:

1-866-890-9552 or call collect 514-877-1577



We're here to help.



Common fraud types and prevention tips



Malware

Malware AKA malicious software

Malware infiltrates your computer system and performs unauthorized activities and transactions.

Here are a few examples:

- Email takeover
- Corporate account takeover/Identity theft
- Data breaches and theft
- Denial of service

Tips & Red Flags

- ✓ Regularly update your anti-virus and anti-malware software.
- ✓ Always verify the source of fund transfer requests
- ✓ Ensure the website you are using is legitimate. If in doubt, type in the URL you know to be true.
- ✓ Be aware of any changes to your online card management experience, including unusual URLs appearing in your browser window, requests to validate your credentials, unusual slowness of your online session or requests for sign-in credentials on any page other than the sign-in page.
- ✗ Beware of emails requesting account information, account verification or banking credentials (such as usernames and passwords). BMO will never contact you by phone, in an email or text message to ask for your User ID, password, personal identification number (PIN), social insurance number or other sensitive information.

If in doubt, contact:

BMO Corporate Cards: 1-800-361-3361 or call collect 514-877-0330

Diners Club Corporate Cards: 1-866-890-9552 or call collect 514-877-1577



Phishing

Phishing and spear phishing

Phishing is one of the most common ways to infect your computer system with malware.

How phishing appears

Typically these come as unsolicited emails that appear legitimate with real company names and logos such as banks and insurance companies.

The email may request your personal or financial information or have you click on a link or direct you to a website.

Successful phishing = malware

By divulging information malware can infect your email accounts, your company's email addresses and your corporate network. This can lead to identity theft, corporate email takeover and facilitate hacking into databases.

Spear phishing is where criminals search social media (Facebook[®]†, Twitter[®]‡, LinkedIn[®]§) to identify individuals who can authorize payments. These individuals are then targeted with emails containing malware.

Tips & Red Flags

- ✗ Be suspicious of requests by email, phone or text for confidential information regardless of real company logos, or letterheads.
- ✗ Never give out your personal identity credentials or any financial information such as account information, usernames, passwords, and personal identification numbers. Note that BMO will never request this kind of information.
- ✗ Never click on a link in a suspicious email. You may be directed to a fraudulent site, or by clicking, enable malware such as spyware to monitor your keystrokes and gain access to financial information.
- ✗ Be wary of making too many professional details public on a social media site, it sets you and the organization up as targets for spear phishing.



Internet pop-ups



Internet pop-ups and scareware

These pop-ups often contain urgent messages such as "security warnings" and "high risk of threats". This is also known as *Scareware*.

Tips & Red Flags

- ✓ Ensure that your company has controls for Internet pop-ups.
- ✓ Educate your users to be cautious of allowing pop-ups to be displayed or responding to the messages.

Common fraud types and prevention tips

<p>Look-a-like free programs</p> <p>Free programs AKA doppelgangers The program has been designed to mirror the look, feel and even code of authentic software and the hook of it being available for “free” tempts users to download it.</p> <p>The software is bogus and downloads malware into your system.</p>	<p>Tips & Red Flags</p> <p>When free isn’t such a great deal</p> <ul style="list-style-type: none"> ✓ Always download software programs from the official site. ✗ Be wary of advertising for free programs on Internet pop-ups even with authentic logos. Only download from trusted websites and verify the URL.
<p>Compromised websites</p> <p>Bogus or compromised websites These appear to be legitimate, but they’re not. You may be asked to validate your credentials even after signing in, or unusual URLs may appear in the browser window. You may be directed to a different website altogether with requests for personal or financial information.</p>	<p>Tips & Red Flags</p> <p>Accessing websites</p> <ul style="list-style-type: none"> ✓ Type the URL of the site into your browser window; for example, to access BMO directly: bmo.com ✓ Bookmark the official site.
<p> Corporate card fraud</p> <p>Corporate card Fraudsters don’t necessarily need your physical card to commit fraud.</p> <p>They can make unauthorized transactions online or by telephone by using only the corporate card number and the expiration date of your corporate card. Some sites or retailers may also require the cardholder name and CVS or CVV code information as well.</p> <p>They can also create a counterfeit card using your card information.</p>	<p>Tips & Red Flags</p> <ul style="list-style-type: none"> ✓ Use Chip and PIN cards when available: The new chip and PIN technology has an encrypted microchip which is very difficult to counterfeit. Instead of a signature that can be forged, it requires a personal identification number (PIN) when making a purchase. ✓ Use the CVS/CVV code when requested: The Card Verification Number Scheme (CVS) or Card Verification Value (CVV) cannot be skimmed and is randomly assigned. It provides an additional layer of security for phone and online transactions. Keep your card and PIN safe: <ul style="list-style-type: none"> ✓ Do not write your PIN down or make it visible to others at payment terminals. ✓ Make your PIN difficult to guess, stay away from easy-to-guess identification such as 1,2,3,4. Online transactions – precautions: <ul style="list-style-type: none"> ✓ A secure website will have a URL starting with https:// <u>not</u> http://. ✓ Secure sites will also show a small lock icon on the screen  ✓ Exit the site securely using the <i>Sign Out or Log Out</i> feature and remember to clear your computer’s cache. Beware of requests for card information: <ul style="list-style-type: none"> ✗ Never give card information unless you can validate that the request is legitimate. BMO will at times ask for your card number, but never your PIN. ✗ Never give card information through email unless the email is encrypted and you are certain that the recipient is genuine.

TM/® Trademarks of Bank of Montreal.

© Diners Club and Diners Club International with the Split Circle Device are registered trade-marks of Diners Club International Ltd.; Bank of Montreal is a licensed user.

®† Facebook is a registered trademark of Facebook, Inc. ®‡ Twitter is a registered trademark of Twitter, Inc. ®# LinkedIn is a registered trademark of LinkedIn Corporation