Managing Your Payment 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® bank account 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 members 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 BMO Online Banking for Business support
1-800-565-6444

BMO ⛰® **Financial Group**

We're here to help.™

Common fraud types and prevention tips

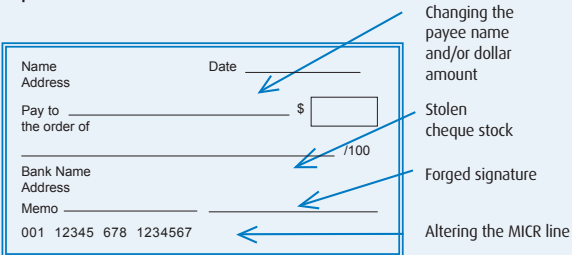| Malware	Tips & Red Flags
Malware AKA malicious software Malware infiltrates your computer system and performs unauthorized activities and transactions. Here are a few examples: · Email takeover · Corporate account takeover/Identity theft · Data breaches and theft · Denial of service	✓ Download IBM Trusteer Rapport®*, a free software download available on the sign in page of BMO Online Banking for Business, and accessible from bmo.com.[1] It works with existing firewall and antivirus software to provide an additional layer of security. ✓ 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 Banking for Business experience, including unusual URLs appearing in your browser window, requests to validate your credentials, unusual slowness of your banking 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, 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 :** Treasury & Payment Solutions Helpdesk 1-800-565-6444.
Phishing	Tips & Red Flags
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.	⚑ 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 PINs. Never give out your security token and token password. 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.

Common fraud types and prevention tips

Internet pop-ups	Tips & Red Flags
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*. The pop-ups then direct you to a site to purchase "security programs" but in reality the site is false and your credit card and other information go directly to the fraudsters.	✓ 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.

Look-a-like free programs	Tips & Red Flags
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. The software is bogus and downloads malware into your system.	**When free isn't such a great deal** ✓ 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.

Compromised websites	Tips & Red Flags
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.	**Accessing websites:** ✓ Type the URL of the site into your browser window; for example, to access Online Banking for Business directly: www21.bmo.com ✓ Select Online Banking for Business within the sign-in tab on bmo.com ✓ Bookmark the official site.

Cheque fraud	Tips & Red Flags
Cheque fraud Cheque fraud can affect both organizations issuing cheques and organizations receiving and depositing cheque payments. Cheque fraud is still the most common type of business fraud. It includes the theft and use of legitimate cheque information, forgery, altering cheque details or even removing the cheque information altogether to be replaced with counterfeit data.	✓ Use magnetic ink – this makes photocopies easier to detect. ✓ Use high-security cheques – these come with a number of features to make forgeries more difficult such as bonding ink and heat-reactive circles. ✓ Check the cheque. Verify that the signature is legitimate and that there are no misspellings, and that the amount, payee and other information are all accurate.

Changing the payee name and/or dollar amount

Name

Address

Date

Pay to the order of

$

Stolen cheque stock

/100

Bank Name

Address

Memo

Forged signature

001 12345 678 1234567

Altering the MICR line

Common fraud types and prevention tips

Electronic Payments Fraud	Tips & Red Flags
Electronic File Transfer (EFT) **Wire Fraud** Typical fraud schemes begin with fraudsters compromising an account by using credentials and information gained through phishing or other methods.	✓ Always validate email and fax requests for electronic transfer payments by talking with the requestor and by ensuring that the person speaking is the real requestor. You can do this by verifying the phone number against your records or asking questions only the legitimate requestor could answer. ✓ Ensure that your customer service team asks additional authentication questions so that the caller really is who they say they are. ✓ Separate duties of payment initiation and approval to ensure dual validation. For example, an employee who initiates an electronic payment will not be authorized to release it. A second employee is required to review and approve the transaction, including verification of the client instructions, for payment instructions to be executed. In the event that a fraudulent transfer is initiated, those credentials cannot be used to release the payment. ✓ Routinely review electronic payment requests to establish "normal behaviour" by your requestors such as a dollar range, number of payment requests made per month etc. In this way, anything that appears to be out of the ordinary can be spotted and investigated. ⚑ If your experience on BMO Online Banking for Business appears unusual, such as constant requests for your security token passwords, do not give out the information and call our Helpdesk at 1-800-565-6444.

15-320 (02/15) CND TM Tips