Help Protect Your Organization Against Fraud Losses

Please read this important notice

Cybersecurity attacks continue to increase in frequency and sophistication. Fraudsters are attacking businesses through compromised emails and social engineering. It is imperative to authenticate requests received via email or other electronic methods before acting upon any such instructions, particularly those directing the movement of funds. Authentication may include verbal or other method of confirming the legitimacy of the email directly with the sender through a previously established phone number.

Banks have seen an increase in compromised emails where fraudsters pose as executives (e.g., President, controller, treasurer, CFO,etc.) and vendors. In this type of attack, it appears that an executive requested a wire or that a vendor changed their wire remittance instructions so that a fraudulent transaction is initiated and approved in an online banking system (e.g., Business NetBanking). To help you be aware of these threats, we wanted to share these typical characteristics:

- *Fraudulent email requests are often well-worded and may be based on previous legitimate emails.*
- *Phrases "code to admin" or "urgent wire transfer" are common.*
- *Email may provide an alternate phone number, advise that the sender is traveling, or otherwise unavailable to discuss verbally, but can be reached through email.*
- *Fraudulent request amounts are similar to normal business transaction amounts.*

To better detect these types of schemes and protect your business:

- *Establish internal communication procedures (e.g., verbal authentication), to verify transaction requests, particularly any requests to a new beneficiary.*
- *Do not confirm a request using information contained in the email which you are trying to validate.*
- *Authenticate all wire remittance change requests from vendors via a phone call to a known contact or known number.*
- *Be suspicious of requests that pressure you take action quickly, are to foreign beneficiaries that are not consistent with historical requests, or to a beneficiary name different from the vendor.*

Additional information regarding online banking security is available on Business NetBanking under Important Documents. Contact your Relationship Manager or Treasury Management Specialist immediately if you suspect a transaction may be fraudulent.

Sincerely
CIBC