



Reminder: Email Requests for Money Transfers/Payments

As the COVID-19 pandemic continues to evolve, some credit union employees are assisting members remotely.

Below are some controls to mitigate and stop wire transfer fraud.

Wire Transfer Fraud

Wire transfer fraud is typically the end result of a compromised email. This can be done through phishing, malware or other forms of cybercrime.

- 1** A member's email account is compromised by criminals.
- 2** The criminal sends an email to the credit union, through the compromised email, requesting a money to be transferred via a wire.
- 3** The email usually states that the member will not be able to be contacted by phone, hoping to stop the credit union employee from using risk controls and procedures.
- 4** The wire transfer is issued, the next time the member reviews their account activity and identifies the unauthorized transaction, it is usually too late to fully recover the funds.

Note: Credit unions and/or business members could also become a victim of fake invoice scams or CEO scams which also attempt to trick a credit union or member to send payments via wire transfer/automated fund transfers.

Risk Control #1



Email requests for wire transfers (or other payments) must be independently confirmed by calling the member using contact information from the member file.

Risk Control #2



Emailed wire transfer requests that have not been confirmed by calling the member must not be processed.

Risk Control #3



Wire transfers are reviewed and authorized by two employees.

Wire Transfer Fraud is Preventable

Always contact members using credentials in their member file for all Email/Online requests and authenticate your member when receiving requests over the phone.

This material is intended to remind employees about some of the risks that may arise when assisting members through virtual channels. Employees are advised to that this does not supersede credit union's policies and procedures.

For more information on scams, visit the Government of Canada's Competition Bureau website .

Source: CUMIS Risk Solutions Group