

SUPPLEMENTAL NOTICE TO AFFECTED USERS

UNAUTHORIZED IMITATION WEBSITE POSTED AT WWW.QUADRIGACX.COM

In the matter of the Bankruptcy of Quadriga Fintech Solutions Corp., Whiteside Capital Corporation and 0984750 B.C. Ltd. D/B/A Quadriga CX and Quadriga Coin Exchange (collectively the “Estate”).

The Trustee and Representative Counsel have received a number of messages and questions from Affected Users since February 9, 2021 when the imitation of the original website portal of Quadriga at www.quadrigacx.com (the “**Imitation Website**”) surfaced online.

If you visited the Imitation Website and attempted to log in with your Quadriga username and password, **we would suggest that out of an abundance of caution you immediately change your password for your logins for websites or your devices that use the same or similar information as your Quadriga login information.** You may consider changing your password hints or security questions for other websites or devices. If your Quadriga username and password are related to your email address, be aware that you may be contacted at that email address. Attackers may attempt to get you to disclose other personal information or passwords in order to access your online accounts or commit identity theft. Accordingly, you may wish to take the following additional precautions with respect to future email messages that you receive and to further protect your personal information:

- Keep an eye out for suspicious e-mails asking to transfer funds or to provide your account credentials.
- Check the authenticity of senders for e-mails you receive. Attackers may pose as people you know, or companies that you recognize, using names familiar to you, but sending an e-mail from an unfamiliar source. This can be done by looking at the domain name at the end of an e-mail address (e.g. @gmail.com, @outlook.com). Where a domain name does not match, it may be fraudulent. Take care to look for exact matches: fraudsters will often send messages from a domain that looks very similar to a legitimate name, such as by adding an extra letter or character, or exchanging a letter for a similar-looking letter or character (e.g. @outllook.com, @gmai1.com).
- Even if an email contains the logos of a recognized business, review the message carefully for spelling errors, odd syntax or turns of phrase, or other possible signs that the message may not have originated from the real business.
- Even where an email appears to come from a known source, exercise caution with respect to clicking on links or documents that you were not expecting, and do not respond to email requests for your password or log-in credentials.
- Monitor your bank and credit card statements and notify the financial institution if there has been any unauthorized activity with your account.
- Scan your computer/device for viruses and malware. Even if you did not click on any links on the Imitation Website, it is possible for the site to have installed malware on your system. Anti-virus software can examine your computer, alerting you to any files that may have been infected.
- Update your computer software to the most current version.

Finally, please be aware of any e-mail you receive from an "@quadrigacx.com" email address. It may be possible for the Imitation Website owner to send e-mails that appear to be from the Quadriga domain.

Emails in respect of the Quadriga bankruptcy will only come from the Trustee (Ernst & Young Inc.) and Representative Counsel (Miller Thomson).

Official communications and information regarding the ongoing bankruptcy proceedings in respect of Quadriga can be found on the Trustee's website at <https://www.ey.com/ca/quadriga>.

Dated at Toronto, Ontario, this 24th day of February 2021.

ERNST & YOUNG INC.
Licensed Insolvency Trustee
Trustee of the Estate of Quadriga Fintech Solutions Corp.,
Whiteside Capital Corporation and 0984750 B.C. Ltd.