CIRCULAR 075-22
June 21, 2022

SELF-CERTIFICATION

AMENDMENTS TO THE RULES OF BOURSE DE MONTREAL INC. TO INTRODUCE CYBERSECURITY INCIDENT REPORTING REQUIREMENTS

The Rules and Policies Committee of Bourse de Montréal Inc. (the "**Bourse"**) and the Special Committee of the Regulatory Division of the Bourse approved amendments to the Rules of the Bourse in order to introduce cybersecurity incident reporting requirements.

These amendments were self-certified in accordance with the self-certification process as established in the *Derivatives Act* (CQLR, Chapter I-14.01).

These amendments attached herewith will become effective on **September 6, 2022**.

Please note that the revised articles will also be available on the Bourse's website (www.m-x.ca).

The amendments covered by this circular were the subject of a request for comments published by the Bourse on May 6, 2022 (see Circular 051-22). Following the publication of this circular, no comments were received by the Bourse.

For additional information, please contact Dima Ghozaiel, Legal Counsel, by email at dima.ghozaiel@tmx.com.

Dima Ghozaiel
Legal Counsel
Bourse de Montréal Inc.

ANNEX 1 - PROPOSED AMENDMENTS

AMENDED VERSION

Article 3.113 Notification to the Regulatory Division of a cybersecurity incident

(a) For the purposes of this Article, a "cybersecurity incident" includes any act to gain unauthorized access to, disrupt or misuse an Approved Participant's information system, or information stored on such information system, that has resulted in, or has a reasonable likelihood of resulting in a material impact:

(i) on the normal operations of the Approved Participant in connection with its access to the Electronic Trading System, or

(ii) on the capacity of the Approved Participant to comply with any of its obligations prescribed by the Regulations of the Bourse.

(b) The Approved Participant must report in writing to the Regulatory Division, in the manner prescribed by the Regulatory Division, any cybersecurity incident,

(i) within three calendar days upon discovering a cybersecurity incident, and must include, unless otherwise agreed by the Regulatory Division, the following information:

(1) a description of the cybersecurity incident;

(2) the date on which or the time period during which the cybersecurity incident occurred and the date it was discovered by the Approved Participant;

(3) a preliminary assessment of the cybersecurity incident, including the impact on the operations of the Approved Participant;

(4) a description of immediate incident response steps the Approved Participant has taken to mitigate the impact on its operations; and

(5) the name of and contact information for an individual who can answer, on behalf of the Approved Participant, any of the Regulatory Division's requests for information about the cybersecurity incident.

(ii) within 30 calendar days, unless otherwise agreed by the Regulatory Division, from discovering a cybersecurity incident, and must include the following information:

(1) a description of the cause of the cybersecurity incident,

(2) an assessment of the scope of the cybersecurity incident, including the impact on the operations of the Approved Participant,

(3) details of the steps taken by the Approved Participant to mitigate the impact on its operations, and

(4) actions the Approved Participant has taken or will take to improve its cybersecurity incident preparedness.

CLEAN VERSION

Article 3.113 Notification to the Regulatory Division of a cybersecurity incident

(a) For the purposes of this Article, a "cybersecurity incident" includes any act to gain unauthorized access to, disrupt or misuse an Approved Participant's information system, or information stored on such information system, that has resulted in, or has a reasonable likelihood of resulting in a material impact:

(i) on the normal operations of the Approved Participant in connection with its access to the Electronic Trading System, or

(ii) on the capacity of the Approved Participant to comply with any of its obligations prescribed by the Regulations of the Bourse.

(b) The Approved Participant must report in writing to the Regulatory Division, in the manner prescribed by the Regulatory Division, any cybersecurity incident,

(i) within three calendar days upon discovering a cybersecurity incident, and must include, unless otherwise agreed by the Regulatory Division, the following information:

(1) a description of the cybersecurity incident,

(2) the date on which or the time period during which the cybersecurity incident occurred and the date it was discovered by the Approved Participant,

(3) a preliminary assessment of the cybersecurity incident, including the impact on the operations of the Approved Participant,

(4) a description of immediate incident response steps the Approved Participant has taken to mitigate the impact on its operations, and

(5) the name of and contact information for an individual who can answer, on behalf of the Approved Participant, any of the Regulatory Division's requests for information about the cybersecurity incident.

(ii) within 30 calendar days, unless otherwise agreed by the Regulatory Division, from discovering a cybersecurity incident, and must include the following information:

(1) a description of the cause of the cybersecurity incident,

(2) an assessment of the scope of the cybersecurity incident, including the impact on the operations of the Approved Participant,

(3) details of the steps taken by the Approved Participant to mitigate the impact on its operations, and

(4) actions the Approved Participant has taken or will take to improve its cybersecurity incident preparedness.