CIRCULAR 051-22
May 6, 2022

REQUEST FOR COMMENTS

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 applicable to all Canadian and foreign approved participants.

Comments on the proposed amendments must be submitted at the latest on **JUNE 6, 2022**. Please submit your comments to:

Dima Ghozaiel
Legal Counsel
Bourse de Montréal Inc.
1800-1190 av des Canadiens-de-Montréal
P.O. Box 37
Montreal, Quebec H3B 0G7
E-mail: legal@tmx.com

A copy of these comments shall also be forwarded to the *Autorité des marchés financiers* (the "**Autorité**") to:

M[e] Philippe Lebel
Corporate Secretary and
Executive Director, Legal Affairs
Autorité des marchés financiers
Place de la Cité, tour Cominar
2640 Laurier boulevard, suite 400
Québec (Québec) G1V 5C1
Fax : (514) 864-8381
E-mail: consultation-en-cours@lautorite.qc.ca

Please note that comments received by one of these recipients will be transferred to the other recipient and that the Bourse may publish a summary of such comments as part of the self-certification process concerning this file. Unless specified otherwise, comments will be published anonymously by the Bourse.

Appendices

You will find in the appendices an analysis as well as the text of the proposed amendments. The implementation date of the proposed amendments will be determined by the Bourse, in accordance with the self-certification process as established by the *Derivatives Act* (CQLR, chapter I-14.01).

Process for Changes to the Rules

The Bourse is authorized to carry on business as an exchange and is recognized as a self-regulatory organization ("**SRO**") by the Autorité. The Board of Directors of the Bourse has delegated to the Rules and Policies Committee of the Bourse its powers to approve and amend the Rules, the Policies and the Procedures, which are thereafter submitted to the Autorité in accordance with the self-certification process as determined by the *Derivatives Act* (CQLR, chapter I-14.01).

In its SRO capacity, the Bourse assumes market regulation and supervision responsibilities of its approved participants. The responsibility for regulating the market and the approved participants of the Bourse comes under the Regulatory Division of the Bourse (the "**Division**"). The Division carries on its activities as a distinct business unit separate from the other activities of the Bourse.

The Division is under the authority of a Special Committee (the "**Special Committee**") appointed by the Board of Directors of the Bourse. The Special Committee is empowered to recommend to the Board of Directors the approval or amendment of some aspects of the Rules of the Bourse governing approved participants. The Board of Directors has delegated to the Rules and Policies Committee of the Bourse its powers to approve or amend these Rules upon recommendation from the Special Committee.

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

TABLE OF CONTENTS

I. DESCRIPTION

In the context of evolving cybersecurity threats, the Regulatory Division (the "Division") of Bourse de Montreal Inc. (the "Bourse") proposes to introduce cybersecurity incident reporting requirements applicable to all Canadian and Foreign Approved Participants (collectively, the "Approved Participants"). The Division believes that such requirements would be beneficial to any Approved Participant that experiences a cybersecurity incident that would have a material impact on its activities on the Bourse, including its compliance with regulatory requirements. These reporting requirements would allow the Division and the Approved Participant to proactively discuss any potential challenges faced by the Approved Participant when complying with regulatory requirements as a result of such an incident, and to implement temporary alternative measures if required.

II. PROPOSED AMENDMENTS

The Division proposes to introduce a new Article 3.113 in the Rules of the Bourse: Notification to the Regulatory Division of a cybersecurity incident.[1]

Approved Participants will be required to report to the Division a written summary of any cybersecurity incident, as defined in Article 3.113, within three calendar days upon discovering the incident. In addition, Approved Participants will be required to provide a more detailed report of the incident within 30 calendar days upon discovering the incident.

The reporting requirements will focus solely on incidents that have or could have a material impact on the activities of the concerned Approved Participant on the Bourse[2], including its capacity to comply with the Bourse regulatory requirements.[3] An Approved Participant should use its judgment when assessing whether an incident can have a "material impact" on its activities on the Bourse, taking into consideration the Approved Participant's size, business model and the nature of the cybersecurity incident. For instance, an incident could be considered to be "material" if the Approved Participant would, in the normal course of operations, escalate it to its Designated Representative, chief compliance officer or one of its Officers.[4]

The Division will develop a new module on the Participant Portal to facilitate the transmission of the required information in a secure environment. The new module will be available at the same

[1] See Annex 1 for the proposed amendments.
[2] For an AP that is also a member of the Canadian Derivatives Clearing Corporation ("CDCC"), it would also include any material impact on its capacity to conduct its clearing activities in connection to any Derivative Instrument listed for trading on the Bourse.
[3] Some examples of the Bourse regulatory requirements that could be impacted: Large Open Position Reporting; Supervision, Surveillance and Compliance; Mandatory Notices.
[4] As defined in Article 1.101 of the Rules of the Bourse.
.

time that the new requirements take effect. Alternatively, the Division will also allow Approved Participants to send the required information via the Division's general email address: info.mxr@tmx.com.

III. ANALYSIS

a. Background

Notification requirements for cybersecurity incidents, the scope of which vary, are already in place in certain other jurisdictions or markets (e.g., Canadian Approved Participants are subject to the Investment Industry Regulatory Organization of Canada ("IIROC") reporting requirements of a cybersecurity incident[5]). The Division proposes uniform notification requirements that would apply to all its Approved Participants regardless of location or type of business. The proposed requirements are similar to the current IIROC reporting requirements, with the necessary adjustments to address incidents that have or could have a material impact on the activities of the concerned Approved Participant on the Bourse only. Moreover, while the reporting deadlines are the same as those set forth in IIROC's regulation, the Division proposes a flexible approach when necessary by adding the phrase "unless otherwise agreed by the Regulatory Division".

b. Objectives

The proposed cybersecurity incident reporting requirements will allow the Division to proactively discuss any potential challenges faced by an Approved Participant when complying with its regulatory requirements as a result of a cybersecurity incident, and to implement temporary alternative measures if required.

In addition, the information provided by the Approved Participants will enable the Division to better understand the potential cybersecurity threats facing the Approved Participants and to provide additional guidance as appropriate.

c. Comparative analysis

In addition to IIROC, which has adopted cybersecurity incident reporting requirements for its members, the National Futures Association[6] in the United States and the Financial Conduct Authority[7] in the United Kingdom also have in place such requirements for firms subject to their jurisdictions, each with its own terms and scope.

---

[5] Reporting by a Dealer Member to IIROC - Section 3703 of IIROC Rule 3700
[6] Cybersecurity | NFA
[7] Operational Resilience | FCA

The Division believes that the proposed cybersecurity incident reporting requirements for its Approved Participants, which focus solely on incidents that have or could have a material impact on the activities of the concerned Approved Participant on the Bourse, is a balanced and reasonable approach.

d. Analysis of impacts

i. Impacts on market

The proposed amendments will have no direct impact on the derivatives markets, other than enabling the Division to better coordinate appropriate measures to be implemented, if required, with an Approved Participant that experiences a cybersecurity incident that has a material impact on its activities on the Bourse.

ii. Impacts on technology

The proposed amendments will have no impact on the technological systems of Approved Participants. The Division will develop a new module on the Participant Portal to facilitate the transmission of the required information in a secure environment. The new module will be available at the same time tha the new requirements become effective.[8]

iii. Impacts on regulatory functions

The proposed amendments will help the Division work with an Approved Participant that is having difficulty complying with regulatory requirements after a cybersecurity incident, so as to implement temporary alternative measures if required. The proposed amendments will also enable the Division to better understand the cybersecurity threats potentially facing all Approved Participants and to provide additional guidance as required.

iv. Public interest

The Bourse is of the view that the proposed amendments are not contrary to the public interest.

IV. PROCESS

The proposed amendments are subject to the approval of the Special Committee of the Division and of the Rules and Policies Committee of the Bourse. They will also be submitted to the Autorité des marchés financiers in accordance with the self-certification procedure and to the Ontario Securities Commission for information purposes.

[8] Alternatively, the Division will also allow the Approved Participants to send the required information via the Division's general email address: info.mxr@tmx.com.

V. ATTACHED DOCUMENTS

Annex 1 - Proposed amendments

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.