CIRCULAIRE 051-22
Le 6 mai 2022

SOLLICITATION DE COMMENTAIRES

**MODIFICATION DES RÈGLES DE BOURSE DE MONTRÉAL INC.
VISANT LA MISE EN PLACE D'EXIGENCES EN MATIÈRE DE SIGNALEMENT
D'INCIDENTS DE CYBERSÉCURITÉ**

Le comité des règles et politiques de Bourse de Montréal Inc. (la « **Bourse** ») et le Comité Spécial de la Division de la réglementation de la Bourse ont approuvé des modifications aux règles de la Bourse afin de mettre en place des exigences en matière de signalement d'incidents de cybersécurité s'appliquant à tous les participants agréés canadiens et étrangers.

Les commentaires relatifs aux modifications proposées doivent nous être présentés au plus tard le **6 JUIN 2022**. Prière de soumettre ces commentaires à :

Dima Ghozaiel
Conseillère juridique
Bourse de Montréal Inc.
1800-1190 av. des Canadiens-de-Montréal
C.P. 37
Montréal QC H3B 0G7
Courriel : legal@tmx.com

Ces commentaires devront également être transmis à l'Autorité des marchés financiers (l'« **Autorité** ») à l'attention de :

M^e^ Philippe Lebel
Secrétaire général et directeur général
des affaires juridiques
Autorité des marchés financiers
Place de la Cité, tour Cominar
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1
Télécopieur : (514) 864-8381
Courriel : consultation-en-cours@lautorite.qc.ca

Veuillez noter que les commentaires reçus par un de ces destinataires seront transmis à l'autre destinataire et que la Bourse pourrait publier un résumé des commentaires qu'elle aura reçus dans le cadre du processus d'autocertification du présent projet. À moins d'indication contraire de votre part, les commentaires seront publiés de manière anonyme par la Bourse.

Annexes

Vous trouverez en annexe le document d'analyse ainsi que le texte des modifications proposées. La date d'entrée en vigueur des modifications proposées sera déterminée par la Bourse conformément au processus d'autocertification, tel que prévu par la *Loi sur les instruments dérivés* (RLRQ, chapitre I-14.01).

Processus d'établissement de règles

La Bourse est autorisée à exercer l'activité de bourse et est reconnue à titre d'organisme d'autoréglementation (« **OAR** ») par l'Autorité. Le conseil d'administration de la Bourse a délégué au comité des règles et politiques l'approbation des règles, des politiques et des procédures, lesquelles sont par la suite soumises à l'Autorité conformément au processus d'autocertification, tel que prévu par la *Loi sur les instruments dérivés* (RLRQ, chapitre I-14.01).

À titre d'OAR, la Bourse assume des responsabilités de réglementation de marché et d'encadrement des participants agréés. L'encadrement du marché et des participants agréés relève de la Division de la réglementation de la Bourse (la « **Division** »). La Division exerce ses activités de façon autonome par rapport à la Bourse, ayant une structure administrative distincte.

La Division est sous l'autorité d'un comité spécial (le « **Comité Spécial** ») nommé par le conseil d'administration de la Bourse. Le Comité Spécial a le pouvoir de recommander au conseil d'administration de la Bourse d'adopter ou de modifier les règles de la Bourse concernant certains aspects de l'encadrement des participants agréés de la Bourse. Le conseil d'administration de la Bourse a délégué au comité des règles et politiques de la Bourse le pouvoir d'adopter ou de modifier ces règles sur recommandation du Comité Spécial.

MODIFICATION DES RÈGLES DE BOURSE DE MONTRÉAL INC. VISANT LA MISE EN PLACE D'EXIGENCES EN MATIÈRE DE SIGNALEMENT D'INCIDENTS DE CYBERSÉCURITÉ

TABLE DES MATIÈRES

I. DESCRIPTION

Dans un contexte où les menaces liées à la cybersécurité sont en constante évolution, la Division de la Réglementation (la « Division ») de Bourse de Montréal Inc. (la « Bourse ») propose de mettre en place des exigences en matière de signalement d'incidents de cybersécurité s'appliquant à tous les Participants Agréés canadiens et étrangers (collectivement, les « Participants Agréés »). La Division estime que ces exigences seraient bénéfiques pour tout Participant Agréé touché par un incident de cybersécurité qui aurait des répercussions importantes sur les activités de celui-ci à la Bourse, notamment au chapitre de sa conformité aux exigences réglementaires. Ces exigences de signalement permettraient à la Division et au Participant Agréé d'engager une discussion proactive au sujet des difficultés que ce dernier pourrait éprouver en ce qui concerne la conformité aux exigences réglementaires en raison de l'incident, et de mettre en œuvre des mesures de rechange temporaires au besoin.

II. MODIFICATION PROPOSÉE

La Division propose d'ajouter aux Règles de la Bourse un nouvel article, soit l'article 3.113 intitulé Avis à la Division de la réglementation en cas d'incident de cybersécurité[1].

Les Participants Agréés auront l'obligation de signaler à la Division, au moyen d'un résumé écrit, tout incident de cybersécurité au sens de l'article 3.113 dans les trois jours civils suivant la découverte de l'incident. Les Participants Agréés seront par ailleurs tenus de fournir un rapport d'incident plus détaillé dans les 30 jours civils suivant la découverte de l'incident.

Les exigences de signalement s'appliqueront uniquement aux incidents qui ont ou pourraient avoir des répercussions importantes sur les activités du Participant Agréé concerné sur la Bourse[2], notamment en ce qui concerne sa capacité à se conformer aux exigences réglementaires de la Bourse[3]. Un Participant Agréé doit exercer son jugement lorsqu'il s'agit d'établir si un incident peut avoir des « répercussions importantes » sur ses activités à la Bourse, notamment en tenant compte de sa taille, de son modèle d'affaires et de la nature de l'incident de cybersécurité. Par exemple, un incident pourrait être considéré comme « important » si, dans le cours normal de ses activités, le Participant Agréé le porte à l'attention de son représentant attitré, de son chef de la conformité ou de l'un de ses dirigeants[4].

---

[1] Se reporter à l'annexe 1 pour consulter la modification proposée.

[2] Dans le cas d'un Participant Agréé qui est aussi un membre de la Corporation canadienne de compensation de produits dérivés (« CDCC »), ces exigences viseraient aussi toute répercussion importante sur sa capacité à mener ses activités de compensation à l'égard d'un Instrument Dérivé inscrit à la cote de la Bourse.

[3] Exemples d'exigences réglementaires de la Bourse qui pourraient être touchées : Déclaration des positions en cours importantes; Supervision, surveillance et conformité; Avis obligatoires.

[4] Au sens de l'article 1.101 des Règles de la Bourse.

La Division créera dans le portail des participants un nouveau module permettant la transmission de l'information nécessaire dans un environnement sécurisé. Ce nouveau module deviendra accessible au moment de la prise d'effet des nouvelles exigences. La Division permettra également aux Participants Agréés de faire parvenir l'information nécessaire à l'adresse courriel générale de la Division, info.mxr@tmx.com.

III. ANALYSE

a) Contexte

Des exigences de signalement des incidents de cybersécurité, dont la portée peut varier, sont déjà en place dans certains autres territoires ou marchés (par exemple, les Participants Agréés canadiens sont assujettis aux exigences de signalement des incidents de cybersécurité[5] de l'Organisme canadien de réglementation du commerce des valeurs mobilières (l'« OCRCVM »)). La Division propose d'uniformiser les exigences de signalement qui s'appliqueraient à l'ensemble de ses Participants Agréés, indépendamment du lieu où ils sont situés ou du type d'entreprise. Les exigences proposées sont semblables aux exigences de signalement actuelles de l'OCRCVM, avec les ajustements nécessaires pour tenir compte des incidents qui ont ou pourraient avoir des répercussions importantes sur les activités du Participant Agréé à la Bourse seulement. De plus, même si les délais de signalement sont les mêmes que ceux établis dans les règles de l'OCRCVM, la Division propose le recours à une approche flexible grâce à l'ajout de la mention « sauf accord contraire de la Division de la Réglementation ».

b) **Objectifs**

Les exigences de signalement proposées permettront à la Division d'engager une discussion proactive au sujet des difficultés qu'un Participant Agréé pourrait éprouver en ce qui concerne la conformité aux exigences réglementaires en raison d'un incident de cybersécurité, et de mettre en œuvre des mesures de rechange temporaires au besoin.

De plus, les renseignements fournis par le Participant Agréé permettront à la Division de mieux comprendre les menaces liées à la cybersécurité auxquelles sont exposés les Participants Agréés et de leur fournir des indications supplémentaires s'il y a lieu.

[5] Signalement à faire par le courtier membre à l'OCRCVM - Article 3703 de la Règle 3700

c) Analyse comparative

Outre l'OCRCVM, qui a adopté des exigences de signalement des incidents de cybersécurité pour ses membres, la National Futures Association[6] des États-Unis et la Financial Conduct Authority[7] du Royaume-Uni ont établi des exigences en la matière pour les firmes sur lesquelles elles ont compétence, dans chaque cas selon des modalités et une portée qui leur sont propres.

La Division estime que la mise en place, à l'égard de ses Participants Agréés, des exigences de signalement des incidents de cybersécurité proposées, qui portent uniquement sur les incidents qui ont ou pourraient avoir des répercussions importantes sur les activités du Participant Agréé à la Bourse, constitue une mesure équilibrée et raisonnable.

d) Analyse des incidences

i. Incidences sur le marché

La modification proposée n'aura aucune incidence directe sur le marché des dérivés, outre le fait qu'elle permettra à la Division de mieux coordonner les mesures appropriées à mettre en œuvre, le cas échéant, avec un Participant Agréé touché par un incident de cybersécurité qui entraîne des répercussions importantes sur ses activités à la Bourse.

ii. Incidences sur les systèmes technologiques

La modification proposée n'aura aucune incidence sur les systèmes technologiques des Participants Agréés. La Division créera dans le portail des participants un nouveau module permettant la transmission de l'information nécessaire dans un environnement sécurisé. Ce nouveau module deviendra accessible au moment de la prise d'effet des nouvelles exigences[8].

iii. Incidences sur les fonctions réglementaires

La modification proposée aidera la Division à travailler avec un Participant Agréé qui éprouve de la difficulté à se conformer aux exigences réglementaires en raison d'un incident de cybersécurité, de manière à mettre en œuvre des mesures de rechange temporaires s'il y a lieu. La modification proposée permettra aussi à la Division de mieux comprendre les menaces liées à la cybersécurité auxquelles sont exposés les Participants Agréés et de leur fournir des indications supplémentaires s'il y a lieu.

---

[6] Cybersecurity | NFA

[7] Operational Resilience | FCA

[8] La Division permettra également aux Participants Agréés de faire parvenir l'information nécessaire à l'adresse courriel générale de la Division : info.mxr@tmx.com.

iv. Intérêt public

La Bourse est d'avis que la modification proposée n'est pas contraire à l'intérêt public.

IV. PROCESSUS

La modification proposée est soumise à l'approbation du Comité spécial de la Division et du Comité des règles et politiques de la Bourse. Elle sera également soumise à l'Autorité des marchés financiers, conformément au processus d'autocertification, et à la Commission des valeurs mobilières de l'Ontario, à titre informatif.

V. DOCUMENTS EN ANNEXE

Annexe 1 – Modification proposée

ANNEXE 1 – MODIFICATION PROPOSÉE

VERSION MODIFIÉE

Article 3.113 Avis à la Division de la Réglementation en cas d'incident de cybersécurité

(a) Pour les fins du présent Article, un « incident de cybersécurité » comprend tout acte visant à obtenir un accès non autorisé au système informatique ou à l'information qui y est stockée d'un Participant Agréé, à désorganiser ce système informatique ou cette information ou à en faire mauvais usage et qui donne lieu, ou qui est raisonnablement susceptible de donner lieu, à des répercussions importantes touchant:

(i) les activités normales du Participant Agréé relativement à son accès au Système de Négociation Électronique, ou

(ii) la capacité du Participant Agréé à se conformer à l'une ou l'autre de ses obligations prévues par la Réglementation de la Bourse.

(b) Le Participant Agréé doit signaler par avis écrit à la Division de la Réglementation, de la façon prescrite par cette dernière, tout incident de cybersécurité,

(i) dans les trois jours civils suivant la découverte d'un incident de cybersécurité, et y préciser, sauf accord contraire de la Division de la Réglementation, les renseignements suivants :

(1) une description de l'incident de cybersécurité;

(2) la date à laquelle, ou la période durant laquelle, l'incident de cybersécurité s'est produit et la date à laquelle le Participant Agréé l'a découvert;

(3) une évaluation provisoire de l'incident de cybersécurité, notamment les répercussions qu'il risque d'avoir sur les activités du Participant Agréé;

(4) la description des mesures d'intervention immédiate que le Participant Agréé a prises pour réduire les répercussions sur ses activités; et

(5) le nom et les coordonnées d'une personne physique chargée de répondre, au nom du Participant Agréé, aux demandes de renseignements de la Division de la Réglementation au sujet de l'incident de cybersécurité.

(ii) dans les 30 jours civils, sauf accord contraire de la Division de la Réglementation, suivant la découverte de l'incident de cybersécurité et y préciser les renseignements suivants :

(1) la description de la cause de l'incident de cybersécurité;

(2) une évaluation de l'étendue de l'incident de cybersécurité, notamment les répercussions sur les activités du Participant Agréé;

(3) la description détaillée des mesures que le Participant Agréé a prises pour réduire les répercussions sur ses activités; et

(4) les dispositions que le Participant Agréé a prises ou prendra pour améliorer son état de préparation à un incident de cybersécurité.

VERSION AU PROPRE

Article 3.113 Avis à la Division de la Réglementation en cas d'incident de cybersécurité

(a) Pour les fins du présent Article, un « incident de cybersécurité » comprend tout acte visant à obtenir un accès non autorisé au système informatique ou à l'information qui y est stockée d'un Participant Agréé, à désorganiser ce système informatique ou cette information ou à en faire mauvais usage et qui donne lieu, ou qui est raisonnablement susceptible de donner lieu, à des répercussions importantes touchant:

(i) les activités normales du Participant Agréé relativement à son accès au Système de Négociation Électronique, ou

(ii) la capacité du Participant Agréé à se conformer à l'une ou l'autre de ses obligations prévues par la Réglementation de la Bourse.

(b) Le Participant Agréé doit signaler par avis écrit à la Division de la Réglementation, de la façon prescrite par cette dernière, tout incident de cybersécurité,

(i) dans les trois jours civils suivant la découverte d'un incident de cybersécurité, et y préciser, sauf accord contraire de la Division de la Réglementation, les renseignements suivants :

(1) une description de l'incident de cybersécurité;

(2) la date à laquelle, ou la période durant laquelle, l'incident de cybersécurité s'est produit et la date à laquelle le Participant Agréé l'a découvert;

(3) une évaluation provisoire de l'incident de cybersécurité, notamment les répercussions qu'il risque d'avoir sur les activités du Participant Agréé;

(4) la description des mesures d'intervention immédiate que le Participant Agréé a prises pour réduire les répercussions sur ses activités; et

(5) le nom et les coordonnées d'une personne physique chargée de répondre, au nom du Participant Agréé, aux demandes de renseignements de la Division de la Réglementation au sujet de l'incident de cybersécurité.

(ii) dans les 30 jours civils, sauf accord contraire de la Division de la Réglementation, suivant la découverte de l'incident de cybersécurité et y préciser les renseignements suivants :

(1) la description de la cause de l'incident de cybersécurité;

(2) une évaluation de l'étendue de l'incident de cybersécurité, notamment les répercussions sur les activités du Participant Agréé;

(3) la description détaillée des mesures que le Participant Agréé a prises pour réduire les répercussions sur ses activités; et

(4) les dispositions que le Participant Agréé a prises ou prendra pour améliorer son état de préparation à un incident de cybersécurité.