Annexe 3 - Libellé des modifications apportées à la Règle 3100 des courtiers membres (version nette)

Les Règles des courtiers membres sont modifiées par les présentes par l'ajout de la section suivante à la Règle 3100 :

RÈGLE 3100
OBLIGATIONS DE DÉCLARER ET DE TENIR DES REGISTRES

…

I. B. 1.1 DÉCLARATION LIÉE À LA CYBERSÉCURITÉ

1. Aux 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 *courtier membre*, 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 ce qui suit :

   (i) il cause un grave préjudice à une *personne*,

   (ii) il a d'importantes répercussions sur une partie des activités normales du *courtier membre*,

   (iii) il déclenche le plan de continuité des activités ou le plan de reprise après sinistre du *courtier membre*,

   (iv) il oblige le *courtier membre*, conformément aux lois applicables, à en aviser un organisme gouvernemental, une autorité en valeurs mobilières ou un autre organisme d'autoréglementation.

2. Le *courtier membre* doit déclarer par écrit un incident de cybersécurité à la *Société* dans les trois jours civils suivant la découverte de l'incident de cybersécurité.

3. La déclaration que le *courtier membre* transmet à la *Société* conformément à l'article 2 doit préciser les renseignements suivants :

   (i) une description de l'*incident de cybersécurité*,

   (ii) la date à laquelle, ou la période durant laquelle, l'*incident de cybersécurité* s'est produit et la date à laquelle le *courtier membre* l'a découvert,

   (iii) une évaluation provisoire de l'*incident de cybersécurité*, notamment le préjudice qu'il risque de causer à une personne et/ou les répercussions qu'il risque d'avoir sur les activités du courtier membre,

   (iv) la description des mesures d'intervention immédiate que le courtier membre a prises pour réduire le risque de préjudice auquel s'exposent les personnes et les répercussions sur ses activités,

(v) le nom et les coordonnées d'une *personne physique* chargée de répondre, au nom du *courtier membre*, aux questions de suivi de la *Société* au sujet de l'*incident de cybersécurité*.

4. Le *courtier membre* doit transmettre par écrit à la *Société*, dans les 30 jours civils, sauf accord contraire de la *Société*, suivant la découverte d'un *incident de cybersécurité* un rapport d'enquête sur l'incident qui précise les renseignements suivants :

(i) la description de la cause de l'*incident de cybersécurité*,

(ii) une évaluation de l'étendue de l'*incident de cybersécurité*, notamment le nombre de personnes ayant subi un préjudice et les répercussions sur les activités du *courtier membre*,

(iii) la description détaillée des mesures que le *courtier membre* a prises pour réduire le risque de préjudice auquel s'exposent les *personnes* et les répercussions sur ses activités,

(iv) la description détaillée des mesures que le *courtier membre* a prises pour réparer les préjudices subis par des *personnes*,

(v) les dispositions que le *courtier membre* a prises ou prendra pour améliorer son état de préparation à un *incident de cybersécurité*.