IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

AVIS DE L'OCRCVM

Avis sur les règles
Avis d'approbation/de mise en œuvre
Règles des courtiers membres [Règles de l'OCRCVM]

Destinataires à l'interne :
Affaires juridiques et conformité
Audit interne
Détail
Haute direction
Institutions
Opérations

Personne-ressource :

Erica Young
Avocate aux politiques
Téléphone : 416 646-7211
Courriel : eyoung@iiroc.ca

19-0194
Le 14 novembre 2019

Modifications concernant le signalement obligatoire des incidents de cybersécurité

Récapitulatif

Les Autorités canadiennes en valeurs mobilières (**ACVM**) ont approuvé les modifications apportées aux Règles des courtiers membres et les modifications correspondantes apportées au Manuel de réglementation en langage simple des courtiers membres de l'OCRCVM (les **Règles de l'OCRCVM**) qui exigent que les courtiers membres (les **courtiers**) signalent à l'OCRCVM tout incident de cybersécurité (les **modifications**).

Les modifications :

- exigent que les courtiers signalent à l'OCRCVM tout incident de cybersécurité dans les trois jours suivant la découverte de celui-ci;
- exigent que les courtiers fournissent à l'OCRCVM un rapport d'enquête sur l'incident de cybersécurité dans les 30 jours suivant la découverte de celui-ci;
- dressent la liste des renseignements que les courtiers doivent transmettre.

Les modifications entrent en vigueur immédiatement.

1. Contexte

Le 5 avril 2018, nous avons publié l'Avis 18-0070 sollicitant des commentaires sur les modifications apportées aux Règles des courtiers membres et aux Règles de l'OCRCVM correspondantes concernant l'obligation, pour les courtiers, de signaler les incidents de cybersécurité à l'OCRCVM.

Les modifications :

- exigent que les courtiers signalent à l'OCRCVM tout incident de cybersécurité dans les trois jours suivant la découverte de celui-ci;
- exigent que les courtiers fournissent à l'OCRCVM un rapport d'enquête sur l'incident de cybersécurité dans les 30 jours suivant la découverte de celui-ci;
- dressent la liste des renseignements que les courtiers doivent transmettre.

Les modifications visent à créer un cadre permettant à l'OCRCVM :

- d'aider immédiatement le courtier à réagir à un incident de cybersécurité;
- d'alerter s'il y a lieu d'autres courtiers à propos des dangers et de leur communiquer les pratiques exemplaires en matière d'interventions;
- d'évaluer les tendances et d'établir des données complètes sur la cybersécurité;
- de promouvoir la confiance dans les courtiers et l'intégrité du marché.

Ces modifications font partie du travail continu que l'OCRCVM accomplit pour améliorer le degré de préparation des courtiers en matière de cybersécurité. Entre autres choses, nous avons récemment mené des exercices de simulation et effectué un deuxième sondage d'autoévaluation sur la cybersécurité. Nous reconnaissons également que certains courtiers nous ont fait des signalements sur une base volontaire depuis la publication de l'Avis 18-0063 le 22 mars 2018.

Depuis que l'OCRCVM a publié le Guide de pratiques exemplaires en matière de cybersécurité, en décembre 2015, les cyberrisques n'ont cessé d'évoluer et représentent une menace encore plus critique pour les investisseurs, les participants au marché et les courtiers. En outre, alors que l'OCRCVM cherche de nouvelles façons de soutenir la transformation du secteur, nous reconnaissons que les courtiers recueillent de plus en plus de données et utilisent de plus en plus des systèmes informatiques complexes. Cette évolution souligne l'importance d'échanger rapidement des renseignements afin d'atténuer les cyberrisques.

2. Commentaires reçus

Nous avons reçu huit lettres de commentaires de la part du public en réponse à notre appel à commentaires. Ci-dessous, vous trouverez un résumé des points qui y sont soulevés et de nos réponses. Un résumé complet des lettres de commentaires reçues et de nos réponses se trouve à l'**Annexe 1** – Réponses aux commentaires du public.

2.1 Résumé des commentaires reçus

Les commentaires du public concernent les points suivants :

- les similitudes et les différences entre les présentes obligations de signalement et les exigences de déclaration actuellement prévues par la *Loi sur la protection des renseignements personnels et les documents électroniques* (**LPRPDE**) ou une loi provinciale équivalente ainsi que les obligations de signalement imposées par des organismes de réglementation tels que le Bureau du surintendant des institutions financières (**BSIF**);
- l'utilisation que l'OCRCVM fera des renseignements recueillis sur les incidents de cybersécurité et la façon dont il en assurera la confidentialité, les gérera à l'interne et les transmettra aux courtiers et au public;
- la définition du terme « incident de cybersécurité », notamment des précisions concernant les types d'incidents de cybersécurité qui doivent être signalés;
- le délai de transmission des rapports sur les incidents de cybersécurité et le niveau de détail des renseignements que ceux-ci doivent contenir.

2.2 Résumé des réponses aux commentaires

Nous avons déterminé qu'il n'était pas nécessaire d'apporter des changements de fond aux modifications en réponse aux commentaires reçus. Nous avons plutôt fourni des précisions supplémentaires concernant l'objectif des modifications dans nos Réponses aux commentaires du public (voir l'**Annexe 1**) et la Foire aux questions (décrite plus en détail dans la section 5 ci-dessous).

Plus précisément, dans nos Réponses aux commentaires du public, nous avons :

- expliqué que les incidents de cybersécurité représentent une menace croissante et peuvent avoir une incidence sur les investisseurs et les marchés financiers, et qu'il est donc raisonnable que l'OCRCVM recueille des renseignements à leur sujet;
- précisé notre intention d'établir une définition vaste et souple du terme « incident de cybersécurité » qui tient compte de l'éventail des modèles d'affaires et des activités des courtiers;
- confirmé que les renseignements que l'OCRCVM recueille sur les incidents de cybersécurité seront communiqués aux autres courtiers dans les grandes lignes et de façon anonyme
- précisé la distinction entre les rapports qui doivent être produits dans un délai de 3 jours et ceux qui doivent être produits dans un délai de 30 jours et reconnu qu'un courtier peut disposer de renseignements limités peu de temps après la découverte d'un incident de cybersécurité;
- précisé l'interprétation du terme « système informatique ».

3. Changements de forme

Même si nous n'avons pas apporté de changements de fond aux modifications, nous y avons apporté les modifications de forme suivantes :

- correction apportée à la numérotation des paragraphes dans la Règle 1300 des courtiers membres modifiée;
- suppression du mot « désagrément » de la définition du terme « incident de cybersécurité » (et de l'obligation de signalement correspondante) pour préciser la portée de la définition.

4. Mise en œuvre

Les modifications prennent effet immédiatement.

5. Foire aux questions

En même temps que le présent avis, nous avons publié une note d'orientation sous forme de foire aux questions dans le but d'aider les courtiers à comprendre les obligations que leur imposent les modifications (voir l'Avis 19-0195). Nous avons l'intention de mettre ce document à jour de façon périodique, au besoin.

6. Annexes

Annexe 1 – Réponses aux commentaires du public

Annexe 2 – Libellé des modifications apportées à la Règle 3100 des courtiers membres (Obligations de déclarer et de tenir des registres) (version soulignée montrant les modifications de forme)

Annexe 3 – - Libellé des modifications apportées à la Règle 3100 des courtiers membres (Obligations de déclarer et de tenir des registres) (version nette)

Annexe 4 – Libellé des modifications apportées à l'article 3703 des Règles de l'OCRCVM (Signalement à faire par le courtier membre à l'OCRCVM) (version soulignée montrant les modifications de forme)

Annexe 5 – Libellé des modifications apportées à l'article 3703 des Règles de l'OCRCVM (Signalement à faire par le courtier membre à l'OCRCVM) (version nette)

Annexe 6 – Avis 19-0195 - Foire aux questions – Signalement obligatoire des incidents de cybersécurité