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
Appel à commentaires
Règles des courtiers membres

Date limite pour les commentaires : le 22 mai 2018

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

18-0070
Le 5 avril 2018

Projet de modification concernant le signalement obligatoire des incidents de cybersécurité

Récapitulatif

L'OCRCVM propose d'apporter des modifications aux Règles des courtiers membres (les **RCM**) et des modifications correspondantes au projet de Manuel de réglementation en langage simple des courtiers membres de l'OCRCVM (le **projet de Manuel de réglementation RLS**[1]) afin d'exiger que les courtiers membres (les **courtiers**) signalent à l'OCRCVM tout incident de cybersécurité (le **projet de modification**). Nous soumettons le projet de modification pour les raisons suivantes :

- La fréquence et la complexité des incidents de cybersécurité augmentent sans cesse;
- L'échange de renseignements est un outil essentiel à l'atténuation des cybermenaces.

Le projet de modification :

- exige que les courtiers signalent promptement les incidents de cybersécurité à l'OCRCVM;
- dresse la liste des renseignements que les courtiers doivent transmettre.

[1] Le 9 mars 2017, nous avons de nouveau publié le projet de Manuel de réglementation RLS dans l'Avis 17-0054. Le 18 janvier 2018, nous avons publié l'Avis 18-0014, qui ne contenait que les sections du projet de Manuel de réglementation RLS auxquelles des modifications de fond avaient été apportées en réponse aux commentaires reçus.

Pendant que le projet de modification est soumis au processus habituel d'élaboration des règles, nous demandons aux courtiers de continuer à nous signaler volontairement tous les incidents de cybersécurité dans le cadre de leur gestion des cyberrisques.

Effets

Nous prévoyons que les courtiers tireront profit du signalement rapide des incidents de cybersécurité. Lorsque l'OCRCVM reçoit un avis d'incident, il peut fournir rapidement un soutien aux courtiers touchés et, s'il y a lieu, informer les autres courtiers des cybermenaces de l'heure, contribuant ainsi à en gérer les répercussions sur eux et les investisseurs. Le projet de modification témoigne de la collaboration que nous maintenons avec les courtiers pour améliorer leur état de préparation en matière de cybersécurité.

Envoi des commentaires

Nous sollicitons des commentaires sur tous les aspects du projet de modification, y compris toute question qui n'y est pas abordée. Les commentaires sur le projet de modification doivent être faits par écrit et transmis au plus tard le ***22 mai 2018*** à :

Erica Young
Avocate aux politiques
Organisme canadien de réglementation du commerce des valeurs mobilières
121, rue King Ouest
Bureau 2000
Toronto (Ontario) M5H 3T9
Courriel : eyoung@iiroc.ca

Il faut également en transmettre une copie aux autorités de reconnaissance à :

Services de la réglementation des marchés
Commission des valeurs mobilières de l'Ontario
20, rue Queen Ouest
Bureau 1903, C.P. 55
Toronto (Ontario) M5H 3S8
Courriel : marketregulation@osc.gov.on.ca

Il est porté à l'attention des personnes qui présentent des lettres de commentaires qu'une copie de leur lettre de commentaires sera mise à la disposition du public sur le site Internet de l'OCRCVM, à l'adresse www.ocrcvm.ca.

Avis sur les règles – Table des matières

1. Exposé du projet de modification

1.1 Contexte

La cybersécurité est une préoccupation fondamentale des courtiers et de l'OCRCVM. La gestion active des cyberrisques est essentielle à la stabilité des courtiers, à l'intégrité des marchés financiers et à la protection des investisseurs.

Au cours des dernières années, nous nous sommes engagés à aider les courtiers membres à renforcer leurs méthodes de gestion des risques et à accroître leur capacité d'intervention en matière de cybersécurité. Nous avons notamment accompli les tâches suivantes :

- en décembre 2015, publication de deux ressources, le Guide de pratiques exemplaires en matière de cybersécurité et le Guide de planification – Gestion des cyberincidents;
- en juin 2016, coordination d'un sondage d'autoévaluation de la cybersécurité auquel ont participé tous les courtiers;
- transmission à chaque courtier de rapports confidentiels d'évaluation de leur pratiques de cybersécurité;
- consultation d'experts du secteur et d'experts en cybersécurité;
- suivi de spécialistes de la cybersécurité de l'OCRCVM auprès des courtiers dont le degré de préparation est inférieur à la cible établie pour leur groupe de pairs.

Le 22 mars 2018, nous avons publié l'Avis technique 18-0063 qui :

- mentionnait l'augmentation de la fréquence et de la complexité des incidents de cybersécurité;
- soulignait que nous étions en train d'élaborer le projet de modification;
- demandait aux courtiers de signaler promptement à l'OCRCVM, en attendant, les incidents de cybersécurité.

À l'heure actuelle, les RCM contiennent aucune exigence de signalement obligatoire des incidents de cybersécurité. Cependant, notre Guide de pratiques exemplaires en matière de cybersécurité recommande le signalement rapide des incidents en vertu des politiques de cybersécurité de la société, et certains courtiers le font volontairement. L'échange de renseignements est un outil essentiel à l'atténuation des cybermenaces, étant donné que celles-ci évoluent rapidement.

1.2 Projet de modification

Afin que nous puissions soutenir davantage les courtiers et les aider à renforcer leur gestion des cyberrisques, le projet de modification :

- exige que les courtiers signalent à l'OCRCVM les incidents de cybersécurité dans les trois jours civils suivant la découverte de l'incident;
- précise les renseignements sur les incidents que les courtiers doivent transmettre à l'OCRCVM.

En vertu du projet de modification, les courtiers devront soumettre deux rapports :

- un premier rapport peu après la découverte de l'incident;
- un rapport d'enquête sur l'incident 30 jours après que celui-ci sera survenu, à moins que l'OCRCVM n'ait approuvé un autre délai. Ce rapport sera plus exhaustif et devra contenir des renseignements qui ne seront peut-être pas accessibles immédiatement après la découverte de l'incident. Les courtiers devraient avoir suffisamment de temps pour entreprendre et terminer dans le délai de 30 jours une enquête sur l'incident visant à déterminer, entre autres, la cause de celui-ci.

Le libellé du projet de modification :

- des RCM se trouve à l'**annexe 1**;
- du projet de Manuel de réglementation RLS se trouve à l'**annexe 2** (version soulignée comparant le projet de modification au projet de Manuel de réglementation RLS publié en janvier 2018) et à l'**annexe 3** (version nette).

Pendant que le projet de modification est soumis au processus habituel d'élaboration des règles, nous demandons aux courtiers de continuer à nous signaler volontairement tous les incidents de cybersécurité dans le cadre de leur gestion des cyberrisques.

2. Analyse

Le projet de modification est conforme aux dispositions semblables de lois provinciales et fédérales sur la protection des renseignements personnels, ainsi qu'à celles de règlements régissant les services financiers qui ont été adoptés aux États-Unis. Nous résumons ces dispositions comparables dans la présente section.

2.1 Lois fédérales

En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (**LPRPDE**), les organisations doivent mettre en œuvre des politiques et pratiques afin de protéger les renseignements personnels dont elles ont la garde ou le contrôle contre la perte, le vol, l'accès, la communication, la copie, l'utilisation et la modification non autorisés de ces renseignements.

En juin 2015, la *Loi sur la protection des renseignements personnels numériques* a modifié la LPRPDE, exigeant qu'une organisation avise le commissaire à la protection de la vie privée et les personnes touchées de :

> toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels dont elle a la gestion, s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu »[2].

[2] Se reporter à Modifications non en vigueur, article 10.

Toutefois, ces dispositions concernant le signalement d'une atteinte à la sécurité ne sont pas encore en vigueur. Elles ne prendront effet qu'après que le règlement connexe soulignant les exigences précises aura été élaboré.

2.2 Lois provinciales

L'Alberta est la seule province dont la loi sur la protection des renseignements personnels prévoit l'obligation de signaler une atteinte à la sécurité. En Alberta, la LPRPDE ne s'applique pas parce que le gouvernement fédéral a jugé que la loi albertaine était substantiellement similaire à la loi fédérale. La loi albertaine prévoit ce qui suit :

> [Traduction]
>
> 34.1(1) L'organisation qui possède des renseignements personnels doit, dans un délai raisonnable, informer le commissaire de toute perte de renseignements personnels, de tout accès non autorisé à pareils renseignements ou de toute communication desdits renseignements lorsqu'une personne raisonnable pourrait considérer qu'il existe un risque réel de préjudice grave pour une personne en raison d'une perte ou d'un accès ou d'une communication non autorisés.
>
> (2) Un avis adressé au commissaire en vertu du paragraphe (1) doit contenir les renseignements exigés par le règlement[3].

Le règlement de l'Alberta énonce les éléments que doit contenir un avis d'incident :

> [Traduction]
>
> 19 Un avis fourni par une organisation au commissaire en vertu du paragraphe 34.1(1) de la Loi doit être envoyé par écrit et contenir les renseignements suivants :
>
> (a) une description des circonstances relatives à la perte ou à l'accès ou à la communication non autorisés;
>
> (b) la date à laquelle, ou la période durant laquelle, la perte ou l'accès ou la communication non autorisés sont survenus;
>
> (c) une description des renseignements personnels ayant fait l'objet de la perte ou de l'accès ou de la communication non autorisés;
>
> (d) une évaluation du risque de préjudice encouru par des personnes en raison de la perte ou de l'accès ou de la communication non autorisés;
>
> (e) une estimation du nombre de personnes qui risquent réellement de subir un préjudice important en raison de la perte ou de l'accès ou de la communication non autorisés;
>
> (f) une description des mesures que l'organisation a prises pour réduire le risque qu'un préjudice soit causé à des personnes;

[3] Paragraphe 34.1(1) de la *Personal Information Protection Act* (2003, chapitre P-6.5).

(g) une description des mesures que l'organisation a prises pour aviser les gens de la perte ou de l'accès ou de la communication non autorisés;

(h) le nom et les coordonnées d'une personne qui peut répondre, au nom de l'organisation, aux questions du commissaire au sujet de la perte ou de l'accès ou de la communication non autorisés[4].

2.3 Lois américaines

Le Department of Financial Services (**DFS**) de l'État de New York réglemente les services et produits financiers de cet État. En vertu du règlement sur la cybersécurité de l'État de New York, une entité réglementée par le DFS doit :

[Traduction]

aviser le superintendant le plus tôt possible, au plus tard dans un délai de 72 heures, lorsqu'elle a déterminé que l'un ou l'autre des incidents de cybersécurité suivants est survenu :

(1) un incident de cybersécurité qui a des répercussions sur l'entité visée ayant l'obligation de transmettre un avis à un organisme gouvernemental, à un organisme d'autoréglementation ou à tout autre organisme de supervision;

(2) un incident de cybersécurité qui est raisonnablement susceptible de nuire considérablement à n'importe quelle partie des activités normales de l'entité visée[5].

Un « incident de cybersécurité » (*Cybersecurity Event*) est défini comme un acte posé dans le but de pénétrer sans autorisation un système d'information, de le perturber ou d'en faire un mauvais usage, ou comme une tentative, réussie ou non, de poser un tel acte[6].

2.4 Questions et solutions de rechange examinées

Afin de clarifier nos attentes concernant le signalement par les courtiers des incidents de cybersécurité dans le cadre de leur gestion des cyberrisques, nous avons envisagé de modifier nos RCM ou de maintenir le *statu quo*. Nos guides de cybersécurité actuels[7] fournissent aux courtiers des orientations exhaustives à propos des éléments d'un solide programme de cybersécurité. Un programme type prévoit le signalement des incidents de cybersécurité. Nous nous attendons à ce que les courtiers continuent de nous signaler volontairement les incidents de cybersécurité, mais nous avons choisi de modifier nos RCM pour les raisons suivantes :

- le risque accru de préjudice pour les investisseurs, les participants au marché et les courtiers attribuable aux incidents de cybersécurité récents;
- l'importance d'échanger rapidement des renseignements afin d'atténuer ce risque.

---

[4] *Personal Information Protection Act Regulation,* AR 366/2003, article 19.
[5] 23 NYCRR 500 – Cybersecurity Requirements for Financial Services Companies, paragraphe 500.17.
[6] 23 NYCRR 500 – Cybersecurity Requirements for Financial Services Companies, alinéa 500.01(d).
[7] Guide de pratiques exemplaires en matière de cybersécurité et Guide de planification – Gestion des cyberincidents.

Grâce à un signalement rapide des incidents à l'OCRCVM, nous pouvons :

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

3. Effets du projet de modification

Nous prévoyons que l'OCRCVM, les courtiers et leurs clients tireront profit du signalement rapide et obligatoire des incidents de cybersécurité. Comme nous l'avons mentionné ci-dessus, l'échange de renseignements est un outil essentiel à l'atténuation des cybermenaces.

Le projet de modification n'impose aucun fardeau ni aucune contrainte à la concurrence ou à l'innovation qui n'est pas nécessaire à la promotion des objectifs de réglementation de l'OCRCVM. Il pourrait entraîner des coûts de conformité supplémentaires, mais ces coûts ne sont pas supérieurs à ceux qu'imposent certaines lois provinciales sur la protection des renseignements personnels et la loi fédérale à venir. Par conséquent, étant donné que les courtiers doivent apporter des modifications à leurs systèmes, politiques et procédures pour se préparer à l'entrée en vigueur du règlement fédéral, nous croyons que nombre d'entre eux ont déjà effectué ces modifications ou s'apprêtent à le faire.

4. Mise en œuvre

4.1 Incidences technologiques

Nous prévoyons que la mise en œuvre du projet de modification n'aura pas d'incidences technologiques importantes.

4.2 Plan de mise en œuvre

Si le projet de modification est approuvé, nous prévoyons le mettre en œuvre de la façon suivante :

- Les modifications de la Règle 3100 des RCM seront mises en œuvre aussitôt que les autorités de reconnaissance les auront approuvées;
- Les modifications de l'article 3705 du projet de Manuel de réglementation RLS seront mises en œuvre lorsque le Manuel de réglementation RLS prendra effet. Nous intégrerons le projet de modification au projet de Manuel de réglementation RLS lorsque nous publierons l'avis d'approbation.

5. Processus d'établissement des politiques

5.1 Objectif réglementaire

L'objectif du projet de modification est le suivant :

- promouvoir des normes et pratiques commerciales justes, équitables et conformes à l'éthique;

- promouvoir la protection des investisseurs;
- atténuer un risque élevé de préjudice important pour les investisseurs, les participants au marché et les courtiers membres.

5.2 Processus de réglementation

Le conseil d'administration de l'OCRCVM (le **conseil**) a établi que le projet de modification est dans l'intérêt public et a approuvé, le 28 mars 2018, sa publication sous forme d'appel à commentaires.

Après avoir examiné les commentaires reçus en réponse au présent appel à commentaires ainsi que ceux des autorités de reconnaissance, l'OCRCVM pourra recommander d'apporter des changements au projet de modification. Le conseil a autorisé le président à approuver les changements et les commentaires reçus s'ils ne sont pas importants, et le projet de modification, dans sa version révisée, sera alors soumis à l'approbation des autorités de reconnaissance. Si les changements ou les commentaires sont importants, nous soumettrons le projet de modification, dans sa version révisée, à la ratification du conseil et, s'il est ratifié, il sera publié dans le cadre d'un nouvel appel à commentaires ou mis en œuvre selon le cas.

6. Annexes

Annexe 1 – Libellé du projet de modification de la Règle 3100 des courtiers membres (*Obligations de déclarer et de tenir des registres*)
Annexe 2 – Libellé du projet de modification de l'article 3703 du Manuel de réglementation RLS (*Signalement à faire par le courtier membre à l'OCRCVM*) (version soulignée)
Annexe 3 – Libellé du projet de modification de l'article 3703 du Manuel de réglementation RLS (*Signalement à faire par le courtier membre à l'OCRCVM*) (version nette)