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
Note d'orientation
Règles des courtiers membres [Règles de l'OCRCVM]

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

Personnes-ressources :

Erica Young
Avocate aux politiques
Politique de réglementation des membres
Téléphone : 416 646-7211
Courriel : eyoung@iiroc.ca

Suzanne Lasrado
Chef principale de la conformité des finances et des opérations
Téléphone: 416 943-5880
Courriel : slasrado@iiroc.ca

19-0195
Le 14 novembre, 2019

Foire aux questions – Signalement obligatoire des incidents de cybersécurité

Récapitulatif

L'OCRCVM publie une foire aux questions sur l'obligation qu'ont les courtiers membres (les **courtiers**) de signaler les incidents de cybersécurité en vertu de la Partie I.B.1.1 de la Règle 3100 [paragraphe 3703(1) et alinéa 3703(2)(vii) des Règles de l'OCRCVM] (l'**obligation de signaler les incidents de**

cybersécurité)[1]. Nous avons l'intention de mettre à jour le présent document aussi souvent que cela sera nécessaire[2].

N°	Question	Réponse
1.	Comment un courtier saura-t-il s'il doit signaler un incident de cybersécurité à l'OCRCVM?	Le courtier devrait déterminer si l'incident correspond à la définition d'« incident de cybersécurité »[3]. La définition d'« incident de cybersécurité » a été rédigée de façon souple afin qu'elle tienne compte de la nature changeante et de la diversité des cybermenaces. Les répercussions des incidents de cybersécurité sur les activités d'un courtier peuvent varier selon la nature de son modèle d'affaires et le type d'incident. La définition s'applique aux incidents qui : • touchent des renseignements personnels et pourraient devoir être signalés en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE); • nuisent à la capacité d'un courtier de s'acquitter de ses obligations envers ses clients et contreparties des marchés financiers; • touchent des personnes tant physiques que morales. Le courtier doit signaler un incident de cybersécurité si celui-ci donne lieu aux résultats énumérés dans les règles[4] ou s'il détermine que l'incident est raisonnablement susceptible de donner lieu à de tels résultats.

[1] Dans la présente note d'orientation, lorsque nous faisons référence aux dispositions relatives à l'obligation de signaler les incidents de cybersécurité, nous citons les dispositions des Règles des courtiers membres (les **RCM**), et les exigences correspondantes des Règles de l'OCRCVM sont indiquées entre crochets. Se reporter à l'Avis 19-0144 – Mise en œuvre du Manuel de réglementation en langage simple des courtiers membres de l'OCRCVM. Lorsque les Règles de l'OCRCVM entreront en vigueur, nous supprimerons les références aux RCM.

[2] Nous comptons également publier la présente foire aux questions dans une page FAQ du site Web de l'OCRCVM, laquelle sera périodiquement mise à jour.

[3] Selon la définition énoncée à l'article 1 de la Partie I.B.1.1 de la Règle 3100 [paragraphe 3703(1) des Règles de l'OCRCVM].

[4] Se reporter aux alinéas (i) à (iv) de l'article 1 de la Partie I.B.1.1 de la Règle 3100 [alinéas 3703(1)(i) à (iv) des Règles de l'OCRCVM] :

(i) il cause un grave préjudice à une personne;
(ii) il a d'importantes répercussions sur une partie des activités normales du courtier;
(iii) il déclenche le plan de continuité des activités ou le plan de reprise après sinistre du courtier;
(iv) il oblige le courtier à en aviser d'autres autorités ou organismes de réglementation.

N°	Question	Réponse
2.	Comment un courtier peut-il déterminer si un incident est raisonnablement susceptible de causer un préjudice à une *personne*?	Le courtier devrait faire preuve de jugement pour déterminer si un incident est raisonnablement susceptible de donner lieu à l'un ou l'autre des résultats énumérés aux alinéas (i) à (iv) de l'article 1 de la Partie I.B.1.1 de la Règle 3100 [alinéas 3703(1)(i) à (iv) des Règles de l'OCRCVM]. Un « grave préjudice » peut être causé à une personne tant physique que morale et peut comprendre un événement autre que la simple utilisation inappropriée de renseignements personnels.
3.	Comment un courtier peut-il déterminer l'importance des répercussions d'un incident de cybersécurité sur une partie de ses activités normales?	L'importance des répercussions variera d'un courtier à un autre, selon leur taille et leur modèle d'affaires. Les courtiers devraient faire preuve de jugement pour déterminer ce qui a d'« importantes répercussions » sur leurs activités normales.
4.	Un courtier doit-il signaler un incident de cybersécurité qui est survenu chez un important fournisseur tiers de systèmes informatiques?	Un incident de cybersécurité qui survient chez un fournisseur de services pourrait devoir être signalé. Le courtier devrait évaluer son « système informatique » ou « l'information » qui y est stockée pour déterminer quels sont les éléments qui sont fournis par des fournisseurs de services tiers. Les autres éléments de la définition d'« incident de cybersécurité » doivent être présents pour qu'un signalement soit justifié.
5.	Un courtier doit-il signaler un incident de cybersécurité qui ralentit ses systèmes internes ou la navigation dans son site Web?	Un tel incident ne doit être signalé à l'OCRCVM que s'il remplit les critères énoncés aux alinéas (i) à (iv) de l'article 1 de la Partie I.B.1.1 de la Règle 3100 [alinéas 3703(1)(i) à (iv) des Règles de l'OCRCVM]. Par conséquent, si l'incident ralentit le système interne du courtier au point d'avoir d'importantes répercussions sur une partie de ses activités normales, nous nous attendons à ce que le courtier signale l'incident à l'OCRCVM.
6.	À qui le courtier doit-il signaler un incident de cybersécurité? Qu'arrive-t-il après le signalement de l'incident?	Le courtier devrait communiquer avec le chef de la conformité des finances et des opérations (la **CFO**) de l'OCRCVM responsable de sa société. Celui-ci organisera une rencontre, si possible le jour même, pour discuter des détails préliminaires de l'incident et des prochaines étapes à suivre. Seront présents à cette réunion :

N°	Question	Réponse
		• les cadres supérieurs de la CFO; • les cadres supérieurs de la Technologie de l'information et de la Sécurité de l'information de l'OCRCVM; • le chef de la direction, le chef des finances, le chef de l'information/de la sécurité de l'information et le chef de la conformité du courtier.
7.	Un courtier est victime d'un incident de cybersécurité. Que doit-il faire?	Le courtier devrait exécuter son plan de gestion des interventions en cas d'incident. S'il n'en a pas un, nous lui recommandons vivement de consulter le représentant de sa police de cyberassurance ou d'avoir recours aux services de professionnels de la cybersécurité et de conseillers juridiques externes pour savoir comment procéder et protéger son entreprise ainsi que ses clients. Le plan de gestion des interventions en cas d'incident devrait préciser les obligations du courtier en matière de signalement.
8.	Quels renseignements le courtier doit-il transmettre à l'OCRCVM dans les trois jours suivant la découverte d'un incident de cybersécurité?	Dans les trois jours suivant la découverte de l'incident de cybersécurité, le courtier doit transmettre au moins les renseignements suivants : • une description de l'incident de cybersécurité; • la date à laquelle, ou la période durant laquelle, l'incident de cybersécurité s'est produit et la date à laquelle le courtier l'a découvert; • une évaluation provisoire de l'incident de cybersécurité, notamment du préjudice qu'il risque de causer à une personne ou des répercussions qu'il risque d'avoir sur ses activités; • la description des mesures d'intervention immédiate qu'il a prises; • le nom et les coordonnées d'une personne qui peut répondre aux questions de suivi de l'OCRCVM. Cependant, si le courtier dispose d'autres renseignements, il devrait les transmettre à l'OCRCVM. Le rapport à soumettre dans le délai de trois jours vise seulement à fournir une évaluation préliminaire de l'incident

N°	Question	Réponse
		de cybersécurité. Il ne vise pas à présenter des observations concrètes concernant l'évaluation ou les mesures correctives. Nous reconnaissons que, trois jours civils après la découverte de l'incident, l'analyse effectuée par le courtier pourrait être incomplète. Nous nous attendons à ce que le courtier soumette la meilleure information dont il dispose au moment du signalement.
9.	Un courtier constate un possible incident de cybersécurité, mais il n'est pas certain que celui-ci correspond à la définition d'incident de cybersécurité et qu'il doit être signalé. Doit-il tout de même communiquer avec l'OCRCVM dans le délai de trois jours?	Dans le doute, le courtier devrait communiquer avec le chef de la CFO responsable de sa société pour obtenir de l'aide.
10.	Après qu'un courtier a signalé un incident de cybersécurité à l'OCRCVM, il conclut qu'il n'y a pas eu d'incident au sens des Règles de l'OCRCVM. Doit-il tout de même transmettre le rapport d'enquête sur l'incident dans le délai de 30 jours (le **rapport à soumettre dans le délai de trente jours**)?	Non. Il lui suffira de nous transmettre un avis pour nous informer de la situation. Toutefois, nous recommandons aux courtiers qui veulent se protéger contre toute responsabilité civile ou réglementaire de demander à un conseiller juridique externe et à des professionnels de la cybersécurité de confirmer que l'incident : • n'a pas entraîné une violation des droits à la protection des renseignements personnels, • n'a pas entraîné d'importantes répercussions sur ses systèmes informatiques ou sur l'information qui y est stockée, et que tout mesure prise est suffisante et conforme à toutes les lois applicables, y compris les lois sur la protection des renseignements personnels.
11.	Quelle est la différence entre le rapport à soumettre dans le délai de trois jours et celui	Le rapport à soumettre dans le délai de trois jours est un bref aperçu des renseignements de base dont dispose le courtier immédiatement après la découverte d'un incident de cybersécurité. Quant au rapport à soumettre dans le délai de

N°	Question	Réponse
	qu'il faut transmettre dans le délai de trente jours?	trente jours, il est plus détaillé et doit être produit après que le courtier a mené une enquête plus approfondie sur l'incident de cybersécurité.
12.	Qu'arrive-t-il si un courtier a besoin de plus de temps pour produire le rapport à soumettre dans le délai de trente jours?	Si le courtier a besoin de plus de temps, il devrait en aviser le chef de la CFO responsable de sa société et lui transmettre les renseignements suivants : • la raison pour laquelle il a besoin de plus de temps; • la date où il prévoit terminer le rapport à soumettre dans le délai de trente jours; • la date où il soumettra ce rapport. Si l'OCRCVM accepte de prolonger le délai, le courtier devrait le tenir au courant de l'état d'avancement de son enquête et des mesures qu'il prend.
13.	Quels renseignements un courtier doit inclure dans le rapport à soumettre dans le délai de trente jours?	Le courtier doit y inclure tous les renseignements pertinents qui lui permettent de déterminer la nature, la portée, l'étendue, les répercussions et les causes profondes de l'incident de cybersécurité, ainsi que les mesures qu'il a prises pour réagir à l'incident, y remédier et reprendre ses activités. Le courtier doit à tout le moins inclure ce qui suit dans son rapport : (a) la description de la cause de l'incident de cybersécurité; (b) une évaluation de l'étendue de l'incident de cybersécurité, notamment du nombre de personnes ayant subi un préjudice et des répercussions sur ses activités, par exemple : • le nombre d'appareils touchés, • le nombre de jours ouvrables pendant lesquels ses activités ont été touchées, • une estimation des coûts engagés pour clore l'incident, y compris (s'il y a lieu) le montant de la franchise de la cyberassurance,

N°	Question	Réponse
		• l'information stockée dans son système informatique qui a été touchée, y compris les données sur les clients; (c) des renseignement détaillés sur les mesures qu'il a prises pour atténuer le risque qu'un préjudice soit causé à des personnes et que les activités de la société soient touchées, y compris le nom des autres organismes de réglementation ou des parties externes qui ont été avisés; (d) des renseignements détaillés sur les mesures qu'il a prises pour remédier au préjudice causé à toute personne, y compris (s'il y a lieu) le nom du conseiller juridique dont il a retenu les services; (e) les dispositions qu'il a prises pour améliorer son état de préparation à un incident de cybersécurité.
14.	Si un courtier compte plusieurs divisions (p. ex. un service de gestion de patrimoine et un service de courtage en valeurs mobilières), devra-t-il soumettre des rapports distincts sur un incident qui touche les mêmes clients?	Si l'incident de cybersécurité résulte d'un même acte visant à obtenir un accès non autorisé à son système informatique ou à l'information qui y est stockée, à désorganiser ce système informatique ou cette information ou à en faire mauvais usage, le courtier devrait soumettre un seul rapport, en mentionnant les divisions touchées. Nous avons défini le terme « incident de cybersécurité » du point de vue de l'acte non autorisé à l'origine de l'incident et non du point de vue des clients touchés par l'incident.
15.	Quand un courtier devrait-il avoir recours à des experts en enquête informatique? Peut-il charger son propre personnel des TI ou fournisseur de services gérés d'enquêter sur les causes profondes de l'incident de cybersécurité?	Nous recommandons au courtier d'avoir recours à des experts en enquête informatique s'il : • ne possède pas les connaissances, ressources et outils spécialisés dont il a besoin pour mener une enquête approfondie sur l'incident de cybersécurité; • souhaite gérer les conflits d'intérêts potentiels. La détermination des causes profondes de l'incident de cybersécurité est une mesure essentielle que le courtier devrait prendre pour s'assurer que l'incident ne se reproduira pas et que les risques continus qui pourraient être associés à l'incident ont été efficacement atténués.

N°	Question	Réponse
16.	Comment saurai-je si l'OCRCVM considère l'incident comme clos?	Nous informerons le courtier lorsque nous aurons terminé notre examen de l'incident et que la production de rapports ne sera plus nécessaire. Cependant, si le courtier obtient par la suite des renseignements concernant l'incident, il devra les communiquer à l'OCRCVM.
17.	Que fera l'OCRCVM des renseignements qui lui sont transmis au sujet d'un incident de cybersécurité?	Nous prévoyons transmettre à l'ensemble des courtiers : • des renseignements généraux concernant les incidents de cybersécurité, selon le volume et la nature des incidents signalés à l'OCRCVM; • des renseignements au sujet des incidents de cybersécurité signalés à l'OCRCVM qui décrivent suffisamment la nature des incidents et le risque auquel ils exposent les autres courtiers et les investisseurs. Nous n'avons pas l'intention de révéler aux autres courtiers ou au public le nom des courtiers qui ont signalé des incidents de cybersécurité. Tous les renseignements concernant les incidents de cybersécurité signalés que nous communiquerons au public ou aux autres courtiers auront été préalablement anonymisés.

1. Dispositions applicables

La présente note d'orientation se rapporte aux dispositions suivantes des Règles de l'OCRCVM :

- Article 1 de la Partie I.B.1.1 de la Règle 3100 [paragraphe 3703(1) et alinéa 3702(2)(vii) des Règles de l'OCRCVM].

2. Documents connexes

La présente note est aussi publiée dans l'Avis d'approbation/de mise en œuvre 19-0194.