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

Annexe 1 – Commentaires reçus en réponse à l'Avis sur les règles 18-0070 – Avis sur les règles – Appel à commentaires – Règles des courtiers membres – Modifications concernant le signalement obligatoire des incidents de cybersécurité

Le 5 avril 2018, nous avons publié l'Avis 18-0070 sollicitant des commentaires sur les modifications (les **Modifications**) apportées aux Règles des courtiers membres et au Manuel de réglementation en langage simple des courtiers membres de l'OCRCVM (le **Manuel de réglementation RLS**) concernant l'obligation, pour les courtiers membres (les **courtiers**), de signaler les incidents de cybersécurité à l'OCRCVM. L'OCRCVM a reçu huit lettres de commentaires des intervenants suivants :

Association canadienne du commerce des valeurs mobilières
Gestion de patrimoine Assante ltée
Gestion MD Limitée
Placements Manuvie
Services de compensation Fidelity Canada s.r.i.
SIFMA
Société financière IGM Inc.
Valeurs mobilières Desjardins inc.

Il est possible de consulter ces commentaires sur le site Web de l'OCRCVM. Le tableau ci-dessous résume ces commentaires et nos réponses.

	Résumé des commentaires	Réponse de l'OCRCVM
Commentaires d'ordre général		
1.	Dans l'ensemble, la plupart des intervenants appuient l'approche de l'OCRCVM et s'engagent à faire de la gestion des risques liés à cybersécurité une priorité. Les intervenants reconnaissent que le signalement des incidents de cybersécurité est un outil essentiel à l'atténuation des cybermenaces dont les courtiers et le public tireront profit.	Nous vous remercions pour vos commentaires.
2.	L'OCRCVM pourrait mettre à profit la structure de signalement actuellement exigée par le Commissariat à la protection de la vie privée du Canada en vertu de la *Loi sur la protection*	Nous nous sommes efforcés d'harmoniser les Modifications avec les exigences de déclaration de la

	Résumé des commentaires	Réponse de l'OCRCVM
	des renseignements personnels et les documents électroniques (**LPRPDE**) et par des organismes de réglementation comme le Bureau du surintendant des institutions financières (**BSIF**), au lieu de créer un nouveau système de signalement parallèle. Le document du BSIF intitulé *Major Cyber Security Incident Reporting*, auquel plusieurs courtiers sont assujettis, oblige les courtiers à signaler certains incidents. Le BSIF exige des courtiers qu'ils tiennent compte des caractéristiques suivantes pour déterminer s'ils doivent signaler un incident : • les répercussions sur les systèmes d'information ou les données critiques; • les répercussions opérationnelles importantes sur les utilisateurs à l'interne; • les niveaux importants de perturbation des systèmes et des services; • les perturbations prolongées des systèmes et activités essentiels; • le nombre important ou croissant de clients externes touchés; • les répercussions négatives imminentes sur la réputation; • le signalement d'un incident aux pouvoirs publics. Étant donné que la disposition semble porter sur le même type de préjudice (à l'endroit de personnes) et que les Modifications obligent le courtier à signaler les incidents à propos desquels il doit, conformément aux « lois applicables », aviser « un organisme gouvernemental, une autorité en valeurs mobilières ou un autre organisme d'autoréglementation », il serait bon d'harmoniser les Modifications avec la LPRPDE ou les normes du BSIF, selon le cas, ou de donner préséance à celles-ci. En adoptant les exigences de déclaration de la LPRPDE, l'OCRCVM s'alignerait sur les lignes directrices actuelles du Commissariat à la protection de la vie privée du Canada et sur les exigences en matière de déclaration obligatoire des atteintes à la sécurité de l'Union européenne. L'OCRCVM devrait aussi envisager d'accepter les déclarations produites en vertu de la LPRPDE ou conformément aux exigences du BSIF dans les mêmes délais. Les courtiers ne	LPRPDE et du BSIF autant qu'il était raisonnablement possible de le faire. Il faut toutefois noter que : i) les courtiers ne sont pas tous assujettis à la surveillance du BSIF; ii) même si tous les courtiers sont assujettis aux obligations de déclaration prévues par la LPRPDE (qui sont entrées en vigueur en novembre 2018), les objectifs de la LPRPDE sont légèrement plus restreints que ceux des Modifications. La LPRPDE porte plus particulièrement sur la protection des *renseignements personnels* (tout renseignement factuel ou subjectif concernant une personne identifiable) et sur le risque de préjudice grave *à l'endroit d'un individu*. Les modifications englobent toute déclaration qu'un courtier peut produire en vertu de l'article 10.1 de la LPRPDE. Cependant, elles exigent également le signalement d'autres incidents de cybersécurité que ceux qui touchent les renseignements personnels d'une personne et qui causent un préjudice grave à son endroit. Il peut par exemple s'agir d'incidents liés aux systèmes d'information qui causent ou qui sont raisonnablement susceptibles de causer un grave préjudice à une personne morale (comme un client institutionnel). Compte tenu de la mission de l'OCRCVM, qui est de veiller à la protection des investisseurs, de renforcer l'intégrité

	Résumé des commentaires	Réponse de l'OCRCVM
	devraient pas avoir à subir un fardeau réglementaire supplémentaire à l'heure où ils doivent déjà mobiliser des ressources pour réagir aux incidents de cybersécurité et les signaler aux autres organismes de réglementation.	des marchés et de favoriser des marchés financiers sains au Canada, les objectifs des Modifications sont un peu plus vastes que ceux de la LPRPDE. Il ne conviendrait pas de s'en remettre uniquement aux déclarations que les courtiers produisent conformément aux dispositions de la LPRPDE ou aux exigences du BSIF en matière de signalement des incidents liés à la cybersécurité, car ces déclarations ne s'appliquent pas à tous les courtiers et ne tiennent pas compte de tous les incidents de cybersécurité.
3.	La LPRPDE exige qu'une organisation avise « toute autre organisation susceptible de pouvoir atténuer le risque de préjudice aux intéressés », ce qui obligerait les courtiers à signaler une atteinte aux mesures de sécurité à l'OCRCVM ou aux autres autorités en valeurs mobilières, selon le cas. Les Modifications ne font que reprendre ces obligations de déclaration. Si l'OCRCVM oblige les courtiers à se conformer à la LPRPDE, les courtiers satisferont par le fait même aux obligations de signalement à l'OCRCVM.	Les obligations prévues par les Modifications cadrent avec les obligations de signalement du paragraphe 10.2(1) de la LPRPDE, mais elles ne sont pas tout à fait les mêmes. Ce paragraphe exige d'aviser simultanément une personne visée par une atteinte à la sécurité et toute organisation qui peut être en mesure de réduire le risque de préjudice que présente l'atteinte à la sécurité à l'endroit des personnes. Le signalement exigé par les Modifications est plus précis que l'avis requis en vertu du paragraphe 10.2(1) de la LPRPDE, et ce, à deux égards importants : i) les Modifications précisent le contenu des rapports à soumettre à l'OCRCVM et les délais dans lesquels ils doivent être soumis, alors que la LPRPDE parle uniquement d'« avis »;

	Résumé des commentaires	Réponse de l'OCRCVM
		ii) le signalement rapide des incidents de cybersécurité exigé par les Modifications permettra à l'OCRCVM non seulement d'aider immédiatement le courtier touché, mais aussi d'alerter s'il y a lieu d'autres courtiers à propos des dangers, d'évaluer les tendances et de promouvoir la confiance dans les courtiers et l'intégrité du marché. Le seul facteur qui motiverait l'avis prévu au paragraphe 10.2(1) de la LPRPDM serait la capacité de l'OCRCVM d'« atténuer le risque de préjudice aux intéressés ». Comme les objectifs visés par les Modifications ne se limitent pas à l'atténuation du risque de préjudice aux intéressés, l'avis prévu par la LPRPDM ne permettrait pas d'atteindre entièrement ces objectifs.
4.	L'OCRCVM devrait mener des consultations supplémentaires auprès des courtiers au sujet des pratiques de cybersécurité afin d'obtenir leurs commentaires sur les coûts importants ou imprévus susceptibles d'être associés aux Modifications.	Les Modifications se fondent sur le travail continu que l'OCRCVM a accompli avec les courtiers dans le domaine de la cybersécurité au cours des trois dernières années. De plus, après la publication des Modifications, l'OCRCVM en a discuté avec plusieurs de ses comités consultatifs. Par ailleurs, l'OCRCVM met à profit la période de consultation publique pour obtenir des commentaires sur les Modifications, y compris sur tout coût important ou imprévu susceptible d'être associé à celui-ci.

	Résumé des commentaires	Réponse de l'OCRCVM
Définition d'« incident de cybersécurité »		
5.	La définition d'« incident de cybersécurité » comprend plusieurs éléments qui ne sont pas clairement définis. Cela pourrait élargir sensiblement la portée de l'obligation de signalement sans procurer d'avantages concrets qui justifieraient le fardeau supplémentaire lié au signalement.	Les Modifications ont été rédigées de façon à respecter l'approche axée sur l'établissement de règles fondées sur des principes de l'OCRCVM. La définition d'« incident de cybersécurité » a été volontairement rédigée de façon souple afin qu'elle tienne compte de la nature changeante et de la diversité des cybermenaces. De plus, les Modifications prennent en considération les différents modèles d'affaires des courtiers. Les répercussions des incidents de cybersécurité sur les activités d'un courtier peuvent varier selon la nature du modèle d'affaires du courtier et le type d'incident.
6.	L'OCRCVM devrait envisager d'adopter la définition d'« incident de cybersécurité » figurant dans la LPRPDE. Cette définition comprend la notion d'« atteinte aux mesures de sécurité » et le critère de « risque réel de préjudice grave ».	Comme nous l'avons indiqué dans la réponse au commentaire n° 2, les objectifs de la LPRPDE sont plus restreints que ceux des Modifications. L'adoption de la définition d'« incident de cybersécurité » figurant dans la LPRPDE pourrait avoir pour effet de soustraire au signalement certains incidents qui ne sont pas liés à une atteinte à la sécurité des renseignements personnels (selon la définition figurant dans la LPRPDE), mais qui ont néanmoins une incidence sur la protection des investisseurs et le maintien de marchés financiers sains et efficaces. Nous avons rédigé la définition d'« incident de cybersécurité » figurant dans les Modifications de façon à inclure les incidents susceptibles de nuire à la capacité

	Résumé des commentaires	Réponse de l'OCRCVM
		d'un courtier de s'acquitter de ses obligations envers ses clients et contreparties des marchés financiers. Le seuil de signalement établi dans les Modifications intègre la notion d'incident « raisonnablement susceptible de causer un grave préjudice ».
7.	La LPRPDE exige la déclaration des atteintes à la sécurité lorsqu'il existe un « risque réel de préjudice grave »; par « préjudice grave », on entend notamment « la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles ». Les Modifications exigent le signalement d'un incident « raisonnablement susceptible » de causer « un grave préjudice ou désagrément à une personne ». En quoi un « risque réel » diffère-t-il d'un incident « raisonnablement susceptible » de causer un tel préjudice, et les termes « préjudice grave » et « grave préjudice » recoupent-ils les mêmes notions?	Les expressions « risque réel » et « raisonnablement susceptible » renvoient à des notions semblables, mais doivent être comprises dans leur contexte. Selon le document d'orientation publié par le Commissariat à la protection de la vie privée du Canada, pour établir si une atteinte aux mesures de sécurité présente un risque réel de préjudice grave, les organisations peuvent tenir compte de la probabilité que les renseignements personnels aient été mal utilisés ou soient en train ou sur le point de l'être. De la même façon, pour déterminer si un incident est « raisonnablement susceptible » de causer un « grave préjudice » à une personne, les courtiers devraient tenir compte de la probabilité qu'une personne (y compris une personne morale cliente) subisse un grave préjudice en raison, *entre autres*, du mauvais usage de renseignements personnels. Pour l'application des Modifications, l'expression « grave préjudice » comprend les concepts énumérés dans la définition de « préjudice grave » qui figure au paragraphe 10.1(7) de la LPRPDE, mais peut aussi

	Résumé des commentaires	Réponse de l'OCRCVM
		comprendre d'autres types de préjudices à l'endroit de personnes morales. La liste non exhaustive de la LPRPDE est axée sur le préjudice à l'endroit d'une personne et peut probablement être interprétée comme excluant le préjudice à l'endroit d'une personne morale comme une société par actions.
8.	Les lois fédérales et provinciales sur la protection des renseignements personnels donnent aux organisations un certain pouvoir discrétionnaire lorsqu'il s'agit de déterminer si un incident présente un « risque réel de préjudice grave » à l'endroit d'une personne. L'OCRCVM devrait songer à accorder un pouvoir discrétionnaire semblable pour l'évaluation des incidents de cybersécurité, ce qui serait cohérent avec l'approche adoptée par le BSIF.	Nous nous attendons effectivement à ce que les courtiers exercent leur pouvoir discrétionnaire pour déterminer si un incident est raisonnablement susceptible de donner lieu à l'un ou l'autre des résultats énumérés aux paragraphes 1(i) à (iv) de la Partie I.B.1,1 de la Règle 3100 [alinéas 3703(1)(i) à (iv) des RLS][1].
9.	Qu'entend-on par « désagrément »? Si l'ordinateur de l'employé d'un courtier doit être nettoyé en raison du protocole de sécurité du courtier, cela constitue-t-il un « désagrément »? Qu'en est-il si le même ordinateur appartient à un conseiller qui est un mandataire et non un employé du courtier et qu'il contient des données concernant une activité professionnelle externe? Le désagrément doit-il se répercuter sur l'investisseur pour que le seuil de signalement soit atteint?	L'adjectif « grave » est censé s'appliquer au terme « désagrément ». Nous avons toutefois tenu compte de ces commentaires et du fait que l'expression « grave désagrément » pouvait être interprétée de façon à élargir déraisonnablement la portée des Modifications. Nous avons donc supprimé le mot « désagrément » des Modifications.

[1] Dans les renvois aux Modifications, nous indiquons les sections des Règles des courtiers membres, ainsi que les sections correspondantes du Manuel de réglementation RLS entre crochets.

	Résumé des commentaires	Réponse de l'OCRCVM
10.	L'OCRCVM devrait envisager de supprimer la notion de « désagrément », car elle fixe le seuil à un niveau trop bas pour que la procédure de signalement soit efficace.	Comme nous l'avons indiqué ci-dessus, nous avons tenu compte de ce commentaire et supprimé le mot « désagrément » des Modifications.
11.	L'expression « tout acte visant à obtenir un accès non autorisé » est trop générale et exigerait des courtiers qu'ils signalent toute *tentative* non autorisée d'accéder à des données. Les incidents à signaler devraient se limiter aux tentatives *réussies* d'obtenir un accès non autorisé. Les courtiers ont des systèmes et des protocoles de sécurité perfectionnés qui bloquent habituellement les maliciels et les autres tentatives d'accès à leur système. Un intervenant indique que ses systèmes internes produisent environ 2 300 alertes par semaine qui pourraient être considérées comme des « incidents de cybersécurité » en vertu des Modifications; de ce nombre, 103 sont désignées prioritaires ou soumises à une enquête plus poussée et, en moyenne, seulement deux ou trois problèmes par mois sont signalés à l'interne. Les Modifications pourraient donner lieu au signalement quotidien des tentatives infructueuses. Cela pourrait grever indûment les ressources de l'OCRCVM.	Bien que la définition d'« incident de cybersécurité » comprenne « tout acte visant à obtenir un accès non autorisé », l'OCRCVM s'attend uniquement à ce que les courtiers lui signalent tout acte 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, iii) il déclenche le plan de continuité des activités ou le plan de reprise après sinistre du courtier, iv) il oblige le courtier, conformément aux lois applicables, à en aviser un organisme gouvernemental, une autorité en valeurs mobilières ou un autre organisme d'autoréglementation. Nous avons évité de faire référence au caractère réussi ou non de l'acte en cause dans la définition d'« incident de cybersécurité ». Nous avons préféré rendre le signalement conditionnel à ce que les résultats susmentionnés soient produits ou à ce que le courtier détermine que ces résultats sont raisonnablement susceptibles d'être produits.

	Résumé des commentaires	Réponse de l'OCRCVM
12.	L'obligation de signaler tout acte qui a « d'importantes répercussions sur une partie des activités normales du *courtier membre* » crée de l'incertitude, ne cadre pas avec les dispositions de la LPRPDE et semble plus contraignante que les exigences du BSIF. Lorsqu'un incident a d'importantes répercussions sur les activités normales du courtier, mais n'expose pas les données du client à un risque ou ne nuit pas aux activités au point d'avoir un effet important sur le service à la clientèle, on ne voit pas pourquoi il devrait être signalé. Cela pourrait imposer un fardeau supplémentaire aux courtiers sans procurer d'avantages correspondants au secteur. L'OCRCVM devrait préciser que les « activités normales » sont celles qui sont importantes pour la sécurité des données des clients.	L'OCRCVM impose une obligation de signalement lorsqu'un incident de cybersécurité nuit aux activités normales d'un courtier, même si cet incident n'expose pas les données des clients à un risque, parce que sa mission consiste notamment à renforcer l'intégrité des marchés et à favoriser des marchés financiers sains au Canada. À cette fin, l'OCRCVM surveille la situation financière et les activités des courtiers, conformément aux règles en matière de capital et d'opérations. Comme l'indique la réponse au commentaire n° 6, nous avons rédigé la définition d'« incident de cybersécurité » figurant dans les Modifications de façon à inclure les incidents susceptibles de nuire à la capacité d'un courtier de s'acquitter de ses obligations envers ses clients et contreparties des marchés financiers et, implicitement, de menacer l'intégrité des marchés et le maintien de marchés financiers sains au Canada. De plus, nous nous attendons à ce que tout incident qui a d'importantes répercussions sur les activités normales du courtier ait un effet important sur le service à la clientèle. Le fait de préciser la définition d'« incident de cybersécurité » afin qu'elle ne s'applique qu'activités importantes pour la sécurité des données des clients limiterait indûment la portée des Modifications.

	Résumé des commentaires	Réponse de l'OCRCVM
13.	Un incident qui ralentit le site Web ou les systèmes internes du courtier ferait-il partie du type d'incident visé par les Modifications?	Un incident qui ralentit le site Web ou les systèmes internes du courtier devrait être signalé conformément aux Modifications seulement s'il résulte d'un acte visant à obtenir un accès non autorisé au système informatique ou à l'information qui y est stockée 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, iii) il déclenche le plan de continuité des activités ou le plan de reprise après sinistre du courtier, iv) il oblige le courtier, conformément aux lois applicables, à en aviser un organisme gouvernemental, une autorité en valeurs mobilières ou un autre organisme d'autoréglementation. Par conséquent, si l'incident ralentit le système interne du courtier au point d'avoir d'importantes répercussions sur une partie des activités normales de celui-ci, nous nous attendons à ce que le courtier signale l'incident, conformément aux Modifications.
14.	Ce qui constitue des répercussions « importantes » variera sans doute selon que la société est de très grande taille ou de petite taille. Cela devrait être pris en considération. Les	Nous convenons que ce qui est « important » peut varier selon la taille du courtier et reconnaissons que les

	Résumé des commentaires	Réponse de l'OCRCVM
	courtiers devraient avoir le pouvoir discrétionnaire de déterminer ce qui est important pour leurs activités particulières.	courtiers devront faire preuve de jugement pour déterminer ce qui a d'« importantes répercussions » sur leurs activités normales.
15.	L'OCRCVM devrait décrire clairement les situations dans lesquelles un incident de cybersécurité doit être signalé à l'OCRCVM, de façon à éviter les signalements excessifs ou insuffisants. Les définitions des expressions « grave préjudice », « désagrément » et « importantes répercussions » devraient être illustrées au moyen d'exemples et d'orientations préparés de concert avec les courtiers.	Tout en s'efforçant d'aider les courtiers à comprendre la nouvelle obligation de signalement, l'OCRCVM doit aussi tenir compte de la nature complexe et de l'évolution rapide des cybermenaces. Nous voulons éviter de publier des orientations qui risquent de devenir rapidement désuètes. Nous envisagerons toutefois d'élaborer une note d'orientation après la mise en œuvre des Modifications.
16.	La définition d'« incident de cybersécurité » figurant dans les Modifications devrait établir une distinction entre les incidents de cybersécurité et les incidents liés à la confidentialité de l'information. Les incidents liés à la confidentialité de l'information résultent souvent de l'erreur humaine, alors que les incidents de cybersécurité résultent habituellement d'une tentative, par une tierce partie, de faire un mauvais usage des données du courtier ou des actifs des clients. Les mesures prises pour corriger ces incidents diffèrent.	Nous ne considérons pas les incidents de cybersécurité et les incidents liés à la confidentialité de l'information comme des concepts distincts et pensons au contraire qu'ils peuvent se chevaucher. Un incident lié à la cybersécurité peut en effet entraîner la divulgation inappropriée de renseignements personnels. Un tel incident pourrait donc être considéré à la fois comme un incident lié à la confidentialité de l'information et comme un incident de cybersécurité.
17.	La définition d'« incident de cybersécurité » qui figure dans les Modifications comprend les termes « importantes répercussions sur une partie des activités normales du courtier membre ». L'alinéa 500.17(a)(2) du règlement sur la cybersécurité du Department of	L'établissement d'un seuil supplémentaire d'importance pourrait restreindre indûment la portée de l'obligation de signalement. Les règles de l'OCRCVM exigent des courtiers et des personnes inscrites qu'ils respectent des

	Résumé des commentaires	Réponse de l'OCRCVM
	Financial Services de l'État de New York[2] prévoit l'obligation de signaler [traduction] « un incident de cybersécurité qui est raisonnablement susceptible de nuire considérablement à n'importe quelle partie *importante* des activités normales de l'entité visée ». Étant donné que le mot « important » ne figure pas dans les Modifications, un incident ayant d'« importantes répercussions » sur une partie négligeable des activités normales du courtier pourrait devoir être signalé. Par exemple, un courtier pourrait avoir un site Web vendant des articles promotionnels marqués de son logo. Même si la gestion de ce site Web ne représente qu'une très petite partie des activités normales du courtier et n'a pas de lien significatif avec ses activités de placement et de négociation réglementées par l'OCRCVM, on pourrait conclure qu'une perturbation du site Web devrait être signalée à l'OCRCVM en vertu des Modifications. L'OCRCVM devrait envisager d'ajouter le mot « important » afin que la définition se lise comme suit : « d'importantes répercussions sur une partie *importante* des activités normales du courtier membre » (italiques ajoutés).	obligations relatives, entre autres, à la conduite des affaires, aux opérations financières et à la conduite de la négociation. L'emploi du terme « activités normales » reflète la portée de la surveillance réglementaire à laquelle l'OCRCVM soumet ses courtiers. Dans l'exemple proposé, un courtier devrait signaler une « perturbation du site Web » uniquement si celle-ci a, ou est raisonnablement susceptible d'avoir, d'importantes répercussions sur les activités normales du courtier. Aux termes des Modifications, c'est l'importance de l'incident par rapport aux activités normales du courtier qui détermine l'obligation de signalement.
18.	Le déclenchement d'un plan de continuité des activités ou de reprise après sinistre est un seuil sensiblement différent de ce que prévoient d'autres définitions d'« incident de cybersécurité ». Étant donné que la Partie I. B. 1,1(1)(iii) de la Règle 3100 des courtiers membres [l'alinéa 3703(1)(iii) des RLS] ne précise pas de seuil d'« importance », l'OCRCVM devrait retirer ce critère de la définition.	Le concept d'importance est implicite dans la Partie I. B. 1,1(1)(iii) de la Règle 3100 des courtiers membres [l'alinéa 3703(1)(iii) des RLS]. Lorsqu'un courtier déclenche son plan de continuité des activités ou son plan de reprise après sinistre, il est censé le faire en réaction à un événement important. En vertu de l'article 16 de la Règle 17 des courtiers membres [article 4712 des RLS], le plan de poursuite des activités du courtier indique les

[2] 23 NYCRR 500 – New York Department of Financial Services Proposed Cybersecurity Requirements for Financial Services Companies (le projet du DFS), https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf (en anglais seulement)

	Résumé des commentaires	Réponse de l'OCRCVM
		procédures que celui-ci compte suivre en cas de perturbation importante des affaires.
Délais de transmission des rapports		
19.	Les délais de transmission des rapports prévus dans les Modifications diffèrent des délais prévus par la LPRPDE, les normes du BSIF et les règlements provinciaux sur la protection des renseignements personnels. La LPRPDE exige qu'une déclaration unique soit faite « le plus tôt possible après que l'organisation a conclu qu'il y a eu atteinte »; l'organisation peut mettre cette déclaration à jour lorsque des renseignements nouveaux sont portés à sa connaissance. Cette structure permet à une organisation d'effectuer une enquête détaillée avant de devoir signaler une atteinte à la sécurité et d'éviter que ce signalement soit fait en fonction d'une analyse incomplète des faits. Le BSIF exige le signalement rapide des incidents importants liés à la cybersécurité. Le règlement sur la protection des renseignements personnels de l'Alberta exige qu'un avis soit transmis « [traduction] dans un délai raisonnable ». Les délais de trois jours et de 30 jours prévus dans les Modifications ne seront peut-être pas suffisants pour permettre une évaluation significative d'un incident de cybersécurité avant son signalement à l'OCRCVM. Selon l'expérience d'un des intervenants, il faut parfois déployer des efforts considérables pour repérer et évaluer correctement les cyberattaques et les incidents de cybersécurité, puis y remédier, en particulier si la portée de la menace ou de l'incident est importante. Un signalement rapide est important, mais un rapport soumis dans les trois jours civils suivant la découverte de l'incident ne contiendra peut-être pas d'observations concrètes concernant l'évaluation de l'incident ou les mesures correctives. De plus, le délai de 30 jours ne sera peut-être pas suffisant pour permettre au courtier d'enquêter sur l'incident.	Le rapport à soumettre dans le délai de trois jours vise seulement à fournir une évaluation préliminaire de l'incident de cybersécurité. Il ne vise habituellement 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 de cybersécurité, l'analyse effectuée par le courtier pourrait être incomplète ou devoir ultérieurement être mise à jour une fois l'enquête terminée. Cependant, le signalement rapide des principales caractéristiques d'un incident de cybersécurité est indispensable à l'atteinte des objectifs des Modifications, en particulier lorsque l'incident est susceptible d'avoir une incidence sur les autres courtiers ou de menacer de façon plus générale les marchés financiers. De plus, les Modifications prévoient expressément une certaine souplesse permettant la transmission du rapport d'enquête sur l'incident après l'expiration du délai de 30 jours, sous réserve de l'accord de l'OCRCVM.

	Résumé des commentaires	Réponse de l'OCRCVM
	Les délais prévus dans les Modifications devraient laisser aux courtiers la plus grande latitude possible afin qu'ils puissent s'acquitter des obligations que leur impose la loi d'une façon compatible avec leur situation particulière.	
20.	Le processus de signalement devrait concorder avec les dispositions des règlements existants, comme celles des lignes directrices du BSIF qui prévoient un délai de cinq jours ouvrables, afin que, une fois le délai écoulé, le courtier puisse négocier avec l'OCRCVM la date de remise d'un rapport plus détaillé ou convenir d'un délai de 90 jours pour lui fournir un rapport définitif décrivant en détail les mesures qu'il entend prendre pour déterminer et contenir l'incident de cybersécurité, y réagir et y remédier. Ces délais proposés cadrent avec les autres obligations de signalement qui s'appliquent, par exemple, aux réponses aux demandes d'accès à des renseignements personnels en vertu des lois sur la protection des renseignements personnels applicables, ainsi qu'au traitement des plaintes des clients selon les règles applicables de l'Association canadienne des courtiers de fonds mutuels et de l'OCRCVM. Les délais de transmission des rapports ne devraient pas être prédéterminés.	Nous pensons que des délais prédéterminés sont nécessaires pour éliminer toute ambiguïté et assurer le signalement rapide des incidents de cybersécurité. Les délais indiqués dans les Modifications tiennent compte de la nature particulière des risques liés à la cybersécurité qui exigent une intervention et un échange de renseignements rapides. Par ailleurs, les Modifications indiquent expressément que les courtiers peuvent demander une prolongation du délai de 30 jours pour soumettre leur rapport.
21.	La transmission d'un rapport dans les trois jours suivant la découverte de l'incident, comme l'exige l'OCRCVM, pourrait dans certains cas être prématurée, en particulier lorsque l'atteinte à la sécurité se produit durant la fin de semaine ou a d'importantes répercussions qui ne sont pas connues trois jours après l'incident.	L'OCRCVM reconnaît que, dans les trois jours civils suivant la découverte d'un incident de cybersécurité, un courtier peut disposer de renseignements limités concernant cet incident. Nous nous attendons à ce que les courtiers soumettent la meilleure information dont ils disposent au moment du signalement.

	Résumé des commentaires	Réponse de l'OCRCVM
		Vu la nature des cybermenaces, il est dans l'intérêt du courtier d'être prêt à réagir à ces menaces en tout temps, y compris durant la fin de semaine.
22.	Le seuil de déclenchement de l'obligation de signalement devrait être le même que dans la LPRPDE, soit la conclusion selon laquelle il y a eu atteinte à la sécurité plutôt que la découverte d'une atteinte à la sécurité.	Nous nous attendons à ce que les courtiers interprètent les seuils de déclenchement prévus par les Modifications et la LPRPDE essentiellement de la même manière.
23.	Le rapport de suivi à soumettre dans le délai de 30 jours impose un fardeau supplémentaire que n'imposent pas les autres organismes de réglementation.	Ensemble, les rapports à soumettre dans les délais de trois jours et de 30 jours prévus dans les Modifications sont censés être cohérents avec les deux rapports qui doivent être soumis aux autres organismes de réglementation à deux moments précis suivant la découverte de l'incident de cybersécurité. Le rapport à soumettre dans le délai de trois jours représente un bref aperçu des renseignements de base dont dispose un courtier immédiatement après la découverte d'un incident de cybersécurité. Le rapport à soumettre dans le délai de 30 jours est un rapport plus détaillé que le courtier doit produire après qu'il a eu la possibilité d'enquêter sur un incident de cybersécurité.
24.	La connaissance que possèdent les courtiers 30 jours après un incident de cybersécurité peut être très limitée, en particulier si un organisme d'application de la loi mène une enquête criminelle sur l'incident. Il se peut que les courtiers ne possèdent pas tous les renseignements requis dans le rapport à soumettre dans le délai de 30 jours. Une analyse et	Nous reconnaissons que, selon la gravité et la complexité de l'incident de cybersécurité, la durée de l'enquête menée par le courtier pourrait dépasser 30 jours. En pareil cas, les courtiers devraient aviser l'OCRCVM et

	Résumé des commentaires	Réponse de l'OCRCVM
	une évaluation prématurées d'un incident de cybersécurité pourraient porter préjudice au courtier puisqu'elles pourraient donner lieu à des interprétations injustes dans un litige potentiel ultérieur. L'OCRCVM devrait envisager d'exiger uniquement une description générale et factuelle de l'incident dans le rapport à soumettre dans le délai de 30 jours, rapport qui ne serait pas considéré comme un rapport « définitif », dans la mesure où le courtier a accès à ces renseignements.	obtenir de ce dernier une prolongation du délai de transmission du rapport d'enquête sur l'incident, comme le prévoient les Modifications. Nous prévoyons que l'OCRCVM tiendra compte de facteurs pertinents tels qu'une enquête criminelle en cours ou le fait que le courtier a besoin de plus de temps pour évaluer un incident de cybersécurité lorsqu'il devra décider ou non d'accorder une prolongation du délai de 30 jours.
25.	L'OCRCVM devrait envisager de remplacer les expressions « suivant la découverte » dans la partie I. B. 1,1(2) de la Règle 3100 des courtiers membres [le sous-alinéa 3703(2)(vii)(a) des RLS] et « l'a découvert » dans la partie I. B. 1,1(3)(ii) de la Règle 3100 des courtiers membres [la clause 3703(2)(vii)(a)(II) des RLS] par les expressions « suivant l'établissement de l'existence » et « a établi son existence », respectivement. Les procédures d'intervention en cas d'incident de la plupart des sociétés prévoient un point d'établissement précis qui déclenche diverses mesures, alors que la « découverte » d'un incident peut être plus ambiguë. Le point d'établissement se fonde habituellement sur l'exécution de mesures d'enquête préliminaires que les sociétés considèrent comme nécessaires à un programme efficace d'intervention en cas d'incident de cybersécurité. Les expressions proposées atténueraient le risque qu'un signalement complet prématuré cause un préjudice aux courtiers.	Comme nous l'avons indiqué ci-dessus, nous interpréterions les expressions « suivant la découverte » et « suivant l'établissement de l'existence » de la même façon.
Types d'incidents		
26.	L'OCRCVM devrait préciser comment les incidents causés par une source externe à la société (par exemple un vol d'identité dont la source peut se trouver chez un détaillant non	La définition d'« incident de cybersécurité » figurant dans les Modifications peut comprendre les incidents causés

	Résumé des commentaires	Réponse de l'OCRCVM
	apparenté) qui sont susceptibles d'avoir une incidence sur les comptes des clients doivent être traités en vertu de l'exigence de signalement. Ces incidents ne devraient pas être soumis aux obligations de signalement car il ne s'agit pas d'incidents de cybersécurité.	par une source externe au courtier, selon les circonstances. Le courtier devrait tenir compte de cette source externe dans son système informatique. Pour déterminer si ce type d'incident de cybersécurité déclenche une obligation de signalement en vertu des Modifications, le courtier devrait prendre en considération chaque élément de la définition d'« incident de cybersécurité ». Il serait ainsi tenu de signaler l'incident de cybersécurité causé par une source externe si cet incident : • visait 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; • a donné lieu, ou était raisonnablement susceptible de donner lieu, à un des motifs de signalement énumérés, notamment à d'importantes répercussions sur une partie des activités normales du courtier.
27.	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 relativement à un même incident qui touche les mêmes clients?	Les Modifications définissent un « 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. Par conséquent, si l'incident de cybersécurité résulte d'un même acte visant à obtenir un

	Résumé des commentaires	Réponse de l'OCRCVM
		accès non autorisé au système informatique ou à l'information qui y est stockée d'un courtier, à désorganiser ce système informatique ou cette information ou à en faire mauvais usage, le courtier devrait soumettre un rapport unique.
28.	L'OCRCVM devrait envisager d'ajouter une disposition réglementaire obligeant les courtiers à informer leur courtier compensateur des atteintes à la sécurité. Cela serait particulièrement important dans le cas des remisiers lorsque l'incident de cybersécurité est susceptible d'avoir une incidence sur le capital régularisé en fonction du risque. Si l'incident entraîne effectivement une perte de capital, cela aurait d'importantes répercussions sur le courtier compensateur en ce qui concerne : a) les facilités de crédit consenties aux clients du remisier pour leur permettre d'acheter des titres sur marge; b) les services à valeur ajoutée, tels l'accès à des services de bureautique et à des produits bancaires; c) l'information financière et réglementaire.	Nous reconnaissons qu'un incident de cybersécurité touchant un remisier peut avoir des répercussions sur son courtier compensateur. Cependant, les Modifications portent uniquement sur le signalement des incidents de cybersécurité à l'OCRCVM et exclut les obligations de signalement réciproques des remisiers et des courtiers compensateurs. Nous recommandons aux remisiers de veiller à conclure avec leur courtier compensateur des ententes contractuelles suffisantes régissant leurs obligations de signalement réciproques, ainsi que leurs obligations de signalement aux autorités de réglementation concernées.
Échange de renseignements		
29.	L'échange de renseignements en l'absence d'expertise et de protocole établi pourrait exposer le secteur à un préjudice supplémentaire, puisqu'on informerait les cybercriminels des secteurs à risque, ou pour des raisons de responsabilité juridique. Cela pourrait alarmer inutilement les clients. Étant donné que certains organismes d'échange de renseignements possèdent déjà l'expertise permettant de repérer, d'analyser et d'anonymiser rapidement	Les Modifications cadrent avec la mission de l'OCRCVM et avec le travail continu que l'OCRCVM accomplit avec les courtiers depuis 2015. L'OCRCVM reconnaît que des organismes comme le BSFI, dont la compétence ne s'étend pas à tous les courtiers, ont eux-mêmes reconnu l'importance croissante de la cybersécurité et renforcé en

	Résumé des commentaires	Réponse de l'OCRCVM
	les renseignements, il n'est pas certain que la participation de l'OCRCVM à ce genre d'activité serait utile, et elle pourrait même être préjudiciable.	conséquence leur surveillance des cybermenaces et des niveaux de risque au sein des institutions financières fédérales.
30.	Le processus de soumission des rapports d'incident de cybersécurité devrait garantir que les renseignements, y compris les données touchées, demeurent confidentiels, afin de ne pas exposer les courtiers à d'autres incidents de cybersécurité. L'OCRCVM devrait développer un système de courriel ou un portail sécurisé et crypté pour la réception des rapports. La divulgation des noms des courtiers déclarants pourrait nuire à leur réputation et à la confiance qu'on leur témoigne. Les noms des courtiers déclarants devraient rester confidentiels et ne pas être révélés au public ni aux autres courtiers.	Compte tenu de la nature sensible et confidentielle des renseignements figurant dans un rapport d'incident de cybersécurité, les courtiers peuvent soumettre leurs rapports à l'OCRCVM par des moyens sécurisés, par exemple en format crypté ou protégé par mot de passe. Les courtiers ont toute la latitude voulue pour déterminer la meilleure façon de soumettre leurs rapports. Nous n'avons pas l'intention de révéler aux autres courtiers ou au public les noms des courtiers qui ont signalé des incidents de cybersécurité. Nous rendrons anonymes tous les renseignements concernant les incidents de cybersécurité signalés que nous communiquerons au public ou aux autres courtiers.
31.	L'OCRCVM devrait préciser la portée des renseignements échangés avec d'autres parties au sujet des incidents de cybersécurité, et indiquer à quelle fréquence, comment et quand ils le seront. Les renseignements relatifs aux incidents de cybersécurité signalés à l'OCRCVM seront-ils communiqués aux autres courtiers, aux institutions financières, aux autorités de réglementation et au grand public? Quel sera le niveau de détail des renseignements communiqués?	Comme nous l'indiquons dans notre réponse au commentaire n° 30, en ce qui concerne les renseignements communiqués au public et aux autres courtiers : • nous rendrons anonyme tout renseignement communiqué; • nous ne divulguerons pas les noms des courtiers déclarants;

	Résumé des commentaires	Réponse de l'OCRCVM
	L'identité du courtier qui signale l'incident de cybersécurité sera-t-elle divulguée? Sinon, comment rendra-t-on les renseignements anonymes afin de limiter le risque qu'elle le soit? L'échange de renseignements devrait être anonyme et se limiter à des renseignements généraux afin de ne pas porter préjudice au courtier déclarant ni entraîner une panique injustifiée chez les investisseurs.	• nous communiquerons périodiquement les renseignements concernant les incidents de cybersécurité, selon le volume et la nature des incidents signalés à l'OCRCVM; • nous communiquerons suffisamment de renseignements au sujet des incidents de cybersécurité signalés à l'OCRCVM pour décrire la nature de l'incident et le risque auquel il expose les autres courtiers et les investisseurs, tout en évitant de divulguer de l'information permettant d'identifier le courtier touché. Nous prévoyons communiquer de façon semblable les renseignements concernant les incidents de cybersécurité aux organismes de réglementation comme les Autorités canadiennes en valeurs mobilières, mais pourrions divulguer le nom du courtier touché au besoin.
32.	Les courtiers qui souhaitent recevoir des renseignements sur les menaces devront-ils signer une entente de non-divulgation leur interdisant de divulguer ces renseignements à des tiers, sauf : a) si ces tiers sont tenus de fournir des services de sécurité de l'information à ces courtiers? b) si ces tiers ont également signé l'entente de non-divulgation?	Nous n'avons pas l'intention d'obliger les courtiers qui souhaitent recevoir des renseignements sur les menaces à signer une entente de non-divulgation. L'OCRCVM rendra anonymes les renseignements concernant les rapports d'incident de cybersécurité reçus avant de les communiquer aux autres courtiers.
Dispense		

	Résumé des commentaires	Réponse de l'OCRCVM
33.	Bon nombre des lois sur le signalement des incidents de cybersécurité promulguées par les États américains prévoient des dispenses pour tenir compte des enquêtes menées par les organismes d'application de la loi. Un signalement rapide pourrait en effet nuire à l'enquête criminelle que l'organisme d'application de la loi concerné mène sur l'incident. Les organismes d'application de la loi concernés pourraient déterminer que l'inclusion de descriptions ou d'évaluations détaillées dans les rapports serait susceptible de compromettre leur enquête. L'OCRCVM devrait envisager d'accorder une dispense à l'égard des délais de transmission et du contenu des rapports pour les besoins de l'application de la loi.	Nous ne jugeons pas nécessaire d'accorder une dispense explicite. Si un courtier a besoin de plus de temps pour terminer le rapport à soumettre dans le délai de 30 jours, les Modifications prévoient explicitement qu'il peut demander à l'OCRCVM de lui accorder un délai plus long.