L’OCRCVM impose aux entreprises d’investissement réglementées l’obligation de signaler les incidents de cybersécurité

18 novembre 2019

Le 14 novembre 2019, l’Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM) – l’organisme national d’autoréglementation qui surveille les courtiers en valeurs mobilières et leurs activités de négociation sur les marchés canadiens – a publié un avis de modification à sa Règle 3100 et sa Règle 3703 ayant pour effet d’obliger les entreprises d’investissement réglementées par l’OCRCVM à signaler les incidents de cybersécurité. Les règles modifiées sont entrées en vigueur immédiatement après la publication de l’avis. Elles obligent les entreprises qui découvrent un incident de cybersécurité devant être signalé à l’OCRCVM à fournir un rapport initial dans un délai de trois jours et un rapport d’enquête complet dans les 30 jours suivant la découverte de l’incident.

Les obligations de signalement des incidents de cybersécurité imposées par l’OCRCVM se rapportent à des circonstances plus variées que les obligations similaires prévues par les lois canadiennes sur la protection des renseignements personnels. En outre, ces obligations s’appliquent en parallèle à d’autres obligations auxquelles peuvent également être soumises les entreprises d’investissement réglementées par l’OCRCVM, comme les obligations imposées par le Bureau du surintendant des institutions financières en matière de signalement des incidents liés à la technologie et à la cybersécurité. Les entreprises d’investissement réglementées par l’OCRCVM sont tenues de vérifier immédiatement leur capacité à satisfaire à ces nouvelles obligations de signalement et d’apporter les changements nécessaires à leurs systèmes, politiques et procédures, ainsi qu’à leurs contrats avec les fournisseurs de services de technologies de l’information.

Indications antérieures en matière de cybersécurité

Au cours des dernières années, les organismes canadiens de réglementation des investissements et du secteur financier ont souligné l’importance de la cybersécurité et ont publié des directives pour aider les entreprises réglementées à gérer les cyberrisques et à atteindre une plus grande maturité en matière de cybersécurité. Par exemple :

- **OCRCVM :** En décembre 2015, l'OCRCVM a publié un *Guide de pratiques* exemplaires en matière de cybersécurité et un *Guide de planification de la gestion des cyberincidents* pour aider les courtiers en valeurs mobilières à réagir aux cyberincidents et à gérer les risques liés à la cybersécurité. En mars 2018, l'OCRCVM a publié un avis prévenant les courtiers en valeurs mobilières que les incidents de cybersécurité sont de plus en plus fréquents et perfectionnés, et les invitant à signaler volontairement tout incident de cette nature à l'OCRCVM.
- **ACFM :** En mai 2016, l'Association canadienne des courtiers de fonds mutuels (l'« ACFM ») a publié le Compliance Bulletin No. 0690-C-Cybersecurity (en anglais seulement)pour aider ses membres à gérer les risques liés à la cybersécurité.
- **ACVM :** En octobre 2017, les Autorités canadiennes en valeurs mobilières (« ACVM ») ont publié l'Avis 33-321 du personnel – Cybersécurité et médias sociaux afin de rendre compte d'une enquête sur les pratiques en matière de cybersécurité et de médias sociaux des entreprises enregistrées pour négocier des titres ou conseiller leurs clients sur les valeurs mobilières, et de fournir des orientations en la matière. Cet avis complétait l'Avis 11-332 du personnel – Cybersécurité publié en 2016 par les ACVM.
- **BSIF :** En octobre 2013, le Bureau du surintendant des institutions financières du Canada (« BSIF ») a publié ses Conseils sur l'auto-évaluation en matière de cybersécurité pour aider les institutions financières sous réglementation fédérale à gérer les cyberrisques. En janvier 2019, le BSIF a publié un Préavis énonçant les attentes du BSIF à l'égard des institutions financières sous réglementation fédérale en ce qui concerne le signalement rapide (dans les 72 heures) des incidents liés à la technologie et à la cybersécurité dont la gravité est « élevée ou critique ».

Pour en savoir plus, consulter les bulletins de BLG intitulés *Cybersecurity Guidance from Investment Industry Organization* (janvier 2016), *Cybersecurity Guidance from Investment Industry Organization* (mai 2016), *Cybersecurity Guidance from Canadian Securities Administrators*, *OSFI Issues Advisory on Technology and Cybersecurity Incident Reporting*, et *Investment Funds Institute of Canada Issues Cybersecurity Guide* (en anglais seulement).

Règles de l'OCRCVM – Signalement obligatoire des incidents de cybersécurité

Contexte

Les règles modifiées de l'OCRCVM sur le signalement obligatoire des incidents de cybersécurité ont été proposées pour la première fois en avril 2018 par l'OCRCVM, dans un *Avis* qui exposait en détail et analysait les modifications proposées. L'avis explique que l'obligation pour les courtiers membres de l'OCRCVM (« courtiers ») de signaler les incidents de cybersécurité vise à permettre à l'OCRCVM 1) d'aider immédiatement le courtier à réagir à l'incident de cybersécurité; 2) d'alerter les autres courtiers et de leur communiquer les meilleures pratiques en matière de préparation aux incidents; 3) d'évaluer les tendances et établir des données complètes sur la cybersécurité; 4) de favoriser la confiance envers le courtier et l'intégrité du marché.

L'avis invitait le public à formuler des commentaires sur les nouvelles règles proposées. L'OCRCVM a présenté un résumé des commentaires reçus et de ses réponses à ces commentaires dans son *Avis* d'avril 2018 et dans une Réponse aux commentaires du *public*.

À la suite du processus de consultation publique, l'OCRCVM a apporté des modifications mineures aux modifications proposées et a publié une note d'orientation, Foire aux questions – Signalement obligatoire des incidents de cybersécurité, afin de fournir des conseils sur la conformité aux règles modifiées.

Précisions sur les règles modifiées

Les Règle 3100 et Règle 3703 modifiées sont entrées en vigueur immédiatement après leur publication le 14 novembre 2019. Voici un résumé des principaux aspects des modifications :

- **Incident de cybersécurité :** Selon les règles, « incident de cybersécurité » désigne tout acte visant à obtenir un accès non autorisé au système informatique d'un courtier membre ou à l'information qui y est stockée, à désorganiser ce système informatique ou cette information ou à en faire mauvais usage, et qui a, ou qui est raisonnablement susceptible d'avoir, les conséquences suivantes : 1) il cause un grave préjudice à une personne; 2) il a d'importantes répercussions sur une partie des activités normales du courtier; 3) il déclenche le plan de continuité des activités ou le plan de reprise après sinistre du courtier; 4) il oblige le courtier à aviser d'autres autorités ou organismes de réglementation.
- **Rapport initial :** Les règles obligent le courtier à transmettre à l'OCRCVM un rapport écrit dans les trois jours civils suivant la découverte d'un incident de cybersécurité. Le rapport doit contenir les éléments suivants : 1) une description de l'incident de cybersécurité; 2) 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; 3) 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 les activités du courtier; 4) la description des mesures d'intervention immédiate que le courtier a prises pour atténuer le risque de préjudice aux personnes et les répercussions sur ses activités; 5) le nom et les coordonnées d'une personne physique chargée de répondre aux questions de suivi de l'OCRCVM.
- **Rapport d'enquête détaillé :** Les règles obligent le courtier qui a découvert un incident de cybersécurité à transmettre un rapport d'enquête écrit complet à l'OCRCVM dans les 30 jours, ou dans un délai plus long convenu par l'OCRCVM. Le rapport doit contenir les éléments suivants : 1) la description de la cause de l'incident de cybersécurité; 2) une évaluation de l'étendue de l'incident de cybersécurité, notamment du nombre de personnes ayant subi un préjudice et des répercussions sur les activités du courtier; 3) des renseignements détaillés sur les mesures prises par le courtier pour atténuer le risque de préjudice aux personnes et les répercussions sur ses activités; 4) des renseignements détaillés sur les mesures prises par le courtier pour remédier au préjudice causé à toute personne; 5) les dispositions prises par le courtier pour améliorer son état de préparation à un incident de cybersécurité.

Le défaut d'un courtier de se conformer aux obligations de signalement des incidents de cybersécurité pourrait entraîner l'imposition de pénalités financières ou autres potentiellement importantes par l'OCRCVM.

Note d'orientation de l 'OCRCVM

La note d'orientation de l'OCRCVM, Foire aux questions – Signalement obligatoire des incidents de cybersécurité, fournit des indications importantes pour le respect des règles modifiées, notamment des réponses aux questions posées dans les commentaires sur les propositions de règles modifiées. Voici un résumé des points importants de ce document d'orientation.

- **Évaluation :** Le courtier doit faire preuve de jugement pour déterminer si un incident correspond à la définition d'incident de cybersécurité et doit être signalé, notamment si l'incident a entraîné, ou est susceptible d'entraîner, un « grave préjudice » à une personne (physique ou morale) ou des répercussions « importantes » sur ses activités normales. La probabilité d'un préjudice grave peut concerner un client autre qu'un particulier et peut aller au-delà de la simple utilisation abusive de renseignements personnels. La gravité de la situation varie selon la taille et le modèle commercial des courtiers. Un courtier qui ne sait pas si un incident constitue un incident de cybersécurité devant être signalé doit demander conseil à son responsable des relations avec l'OCRCVM.
- **Rapport initial :** Le rapport initial d'un incident de cybersécurité ne contient qu'une évaluation préliminaire, ou un « bref aperçu des renseignements de base » sur l'incident. L'OCRCVM reconnaît qu'un courtier n'aura vraisemblablement pas le temps d'effectuer une analyse complète d'un incident dans les trois jours suivant sa découverte, et s'attend à ce qu'il lui soumette les renseignements les plus pertinents dont il dispose au moment du signalement. L'OCRCVM s'attend également à ce qu'un courtier lui communique tout complément d'information sur l'incident à sa disposition.
- **Rapport détaillé :** Le rapport détaillé d'un incident de cybersécurité doit comprendre (outre les éléments prévus dans les règles) tous les renseignements pertinents et utiles concernant la nature, l'étendue, la portée, les répercussions et les causes profondes de l'incident, ainsi que les mesures prises par le courtier pour réagir à l'incident, y remédier et reprendre ses activités.
- **Délai de dépôt du rapport détaillé :** Si un courtier a besoin de plus de 30 jours pour remettre son rapport d'enquête détaillé, il peut demander une prolongation à l'OCRCVM. La demande doit mentionner les éléments suivants : 1) la raison pour laquelle le courtier a besoin de plus de temps; 2) la date à laquelle il prévoit terminer le rapport; 3) la date à laquelle il soumettra le rapport. Le courtier qui a obtenu une prolongation doit tenir l'OCRCVM informé de l'avancement de son enquête sur l'incident et des mesures qu'il a prises.
- **Fausses alertes :** Un courtier qui soumet un rapport initial d'incident n'est pas tenu de soumettre un rapport détaillé s'il détermine par la suite que le cas ne constitue pas un incident de cybersécurité devant être signalé. L'OCRCVM recommande vivement aux courtiers de consulter un conseiller juridique externe et des professionnels de la cybersécurité avant de prendre cette décision.
- **Fournisseurs de services de TI :** Le fait qu'un incident de cybersécurité soit survenu chez un fournisseur de services du courtier ne dispense pas ce dernier de ses obligations de signalement. Le « système informatique » d'un courtier ou

« l'information qui y est stockée », selon le sens donné à ces termes dans les règles, comprennent les éléments fournis par des fournisseurs de services tiers.

- **Experts en enquête informatique externes :** Si le courtier ne possède pas les connaissances spécialisées, les outils et les ressources nécessaires pour mener une enquête approfondie sur l'incident de cybersécurité et souhaite gérer les conflits d'intérêts potentiels, l'OCRCVM recommande de faire appel à un expert en enquête informatique externe pour enquêter sur l'incident et en déterminer les causes profondes.
- **Utilisation par l'OCRCVM des renseignements signalés :** L'OCRCVM prévoit transmettre à sa communauté de courtiers des renseignements généraux sur les incidents de cybersécurité et des renseignements anonymes sur les incidents de cybersécurité qui lui sont signalés. Ce partage de renseignements, qui vise à permettre à d'autres courtiers de comprendre la nature des risques de cybersécurité auxquels ils pourraient faire face, est conforme au récent rapport du commissaire à la protection de la vie privée fédéral sur les tendances en matière de signalement obligatoire des violations, selon lequel les agresseurs reprennent souvent les mêmes attaques contre plusieurs organisations du même secteur. (Pour en savoir plus, consulter le bulletin de BLG intitulé Mandatory Breach Reporting: Lessons from Year One (en anglais seulement).

Préparation en vue d'assurer la conformité aux règles de l'OCRCVM

Les règles modifiées de l'OCRCVM concernant le signalement obligatoire des incidents de cybersécurité sont désormais en vigueur. Les courtiers doivent évaluer sans tarder leurs systèmes, politiques et procédures, ainsi que leur état de préparation aux incidents de cybersécurité, pour s'assurer d'être en mesure de présenter en temps utile des rapports d'incidents initiaux et des rapports d'enquête détaillés. Voici des suggestions pour aider les courtiers à se préparer :

- **Politiques/Procédures – Évaluation et intervention** : Les courtiers doivent coucher sur papier les politiques et procédures nécessaires afin que chaque incident potentiel de cybersécurité soit immédiatement signalé au personnel désigné et dûment formé aux fins d'enquête, d'évaluation et d'intervention selon un plan écrit d'intervention en cas d'incident. Ce plan d'intervention doit être conforme aux exigences légales et orientations réglementaires applicables, ainsi qu'aux meilleures pratiques appropriées. Pour en savoir davantage, veuillez vous reporter aux bulletins de BLG intitulés Cyber Incident Response Plans – Test, *Train and Exercise* et Data Security Incident Response Plans – Some Practical *Suggestions* (en anglais seulement).
- **Politiques/Procédures – Rapports à l'OCRCVM :** Les courtiers doivent avoir des politiques et des procédures consignées par écrit pour permettre au personnel désigné et formé de prendre des décisions éclairées et documentées sur le signalement des incidents de cybersécurité à l'OCRCVM.
- **Contrats avec des agents de traitement des données :** Les courtiers doivent veiller à ce que leurs contrats avec les fournisseurs de services de technologies de l'information et de traitement des données (y compris les fournisseurs de services en nuage) contiennent des dispositions appropriées (notamment l'obligation de signaler rapidement au courtier tous les incidents de cybersécurité

et de lui fournir des précisions sur chaque incident) afin qu'il puisse se conformer à ses obligations en matière de signalement des incidents de cybersécurité.

- **Privilège juridique :** Les courtiers doivent disposer d'une stratégie appropriée en matière de privilège juridique afin d'éviter la divulgation involontaire et inutile de conseils juridiques privilégiés concernant des incidents de cybersécurité ou toute renonciation involontaire au privilège juridique. Pour en savoir plus, voir les bulletins de BLG intitulés Cyber Risk Management – Legal Privilege Strategy – *Part 1*, Cyber Risk Management – Legal Privilege Strategy – Part 2, *Legal Privilege for Data Security Incident Investigation Reports* et *Loss of Legal Privilege over Cyberattack Investigation Report* (en anglais seulement).
- **Autres obligations légales de signaler les infractions :** Les courtiers doivent être conscients de leurs autres obligations légales de signaler, notifier et déclarer les incidents liés à la cybersécurité et à la sécurité des données imposées par la loi (y compris les lois sur la protection des renseignements personnels), le droit des contrats, la common law et le droit civil. Pour en savoir davantage, veuillez vous reporter aux bulletins de BLG intitulés Cyber-Risk Management – Data Incident *Notification Obligations*, Cyber Risk Management – Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and *Incidents*,Frequently Asked Questions – Compliance with PIPEDA's Security *Breach Obligations*, and *OSFI Issues Advisory on Technology and Cybersecurity Incident Reporting.* (en anglais seulement).

Par

Lauren Phizicky

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels, Marchés financiers, Différends en matière de valeurs mobilières, Gestion des investissements

---

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary
Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3
T 403.232.9500
F 403.266.1395

Ottawa
World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9
T 613.237.5160
F 613.230.8842

Vancouver
1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2
T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749