Montréal, le 13 février 2025

Me Philippe Lebel
Secrétaire général et directeur général des affaires juridiques
Autorité des marchés financiers
Place de la Cité, tour Cominar, 2640, boul. Laurier, bureau 400
Québec (QC) G1V 5C1
consultation-en-cours@lautorite.qc.ca

Objet: Nouveau formulaire de l'Autorité pour le signalement des incidents de sécurité de l'information

Monsieur,

Nous avons pris connaissance avec grand intérêt du nouveau formulaire pour le signalement des incidents de sécurité de l'information (le « formulaire »), lequel a été soumis à titre de consultation publique.

Étant le premier groupe financier coopératif en Amérique du Nord avec plus de 465 G$ d'actifs et 7,7 millions de membres et clients[1], le Mouvement Desjardins (le « Mouvement ») offre une vaste gamme de produits et services à l'échelle canadienne tant pour les clientèles des particuliers que des entreprises incluant la Gestion de patrimoine, l'Assurance de personnes et l'Assurance de dommages.

Le Mouvement Desjardins apprécie la présente occasion de commenter le formulaire avant sa mise en application. Nos commentaires visent à en faciliter l'utilisation et à s'assurer que les instructions appropriées soient ajoutées au guide d'application et de mise en œuvre du *Règlement sur la gestion et le signalement des incidents de sécurité de l'information de certaines institutions financières et des agents d'évaluation du crédit* (le « Règlement »).

Précisions à apporter au signalement d'incident des tierces parties

D'abord, nous souhaitons obtenir certaines précisions sur l'usage de ce formulaire dans les cas d'incident chez un tiers. Le Règlement prévoit que nous devons divulguer les incidents se produisant au sein de tiers et qui affectent les activités qui leur ont été assignées. Parfois, certains tiers ou fournisseurs ne collaborent pas rapidement et refusent de nous divulguer leurs incidents ou les détails afférents. Nous encourageons l'Autorité à préciser ses attentes dans ces cas notamment en matière de documentation puisqu'il peut s'avérer difficile d'obtenir une information complète et précise sans avoir accès aux systèmes affectés.

[1] Rapport financier au troisième trimestre de 2024

Champs à compléter
Nous notons que dans le formulaire proposé, l'Autorité ne fait pas de distinction entre les champs obligatoires à remplir et ceux qui sont facultatifs. Sachant que plusieurs données ne seront pas disponibles lors du signalement initial, nous sommes d'avis qu'il serait important d'indiquer les champs obligatoires en ajoutant, par exemple un « * » à ces derniers. Cette précision s'inscrit dans une perspective d'harmonisation avec le Bureau du surintendant des institutions financières (« BSIF ») afin de préconiser la cohérence des pratiques et la comparabilité en termes de divulgation. Nous encourageons ainsi l'Autorité à s'aligner autant que possible sur le BSIF pour ce qui est des champs obligatoires et à considérer le rajout de précisions concernant la complétion des champs facultatifs dans le guide d'application du Règlement. Dans ce contexte, nous invitons l'Autorité à rendre facultatif le champs « Temps estimé pour maîtriser l'incident » dans le but d'éviter une divulgation basée sur un faible niveau de certitude pouvant mener à de nombreuses réévaluations et mises à jour du formulaire.

Toujours à des fins d'harmonisation, nous encourageons l'Autorité à ajouter à l'ensemble des listes déroulantes une option « Sans objet/Non applicable et/ou « À déterminer » afin de couvrir les situations lors desquelles l'information n'est pas encore disponible. Dans le même esprit, nous recommandons que le champ « Sévérité de l'incident » présente, à l'image du BSIF, une liste déroulante avec les choix suivants : faible, moyen, élevé, critique, et ce, afin d'assurer une certaine uniformité au sein de l'industrie.

Finalement, nous encourageons l'Autorité à préciser les champs obligatoires à compléter au moment de la clôture de l'incident pour considérer le signalement comme étant complet. Cette information peut être précisée dans le guide d'application du Règlement.

Type d'incident
Nous notons que la taxonomie de l'Autorité ne distingue pas le type et la cause de l'incident. Nous croyons qu'il serait pertinent de distinguer un type d'incident, défini comme la nature ou la catégorie de l'incident, alors que la cause de l'incident se définit comme l'origine ou la raison pour laquelle l'incident s'est produit. Nous suggérons donc de limiter cette section aux types d'incidents et de prévoir un champ distinct pour la cause de l'incident. Nous croyons que le champ « Description de l'incident » pourrait être utilisé à cet effet.

Acteurs
Nous souhaitons nous assurer que le niveau d'information demandé dans ce champ est approprié. En effet, nous comprenons qu'en demandant d'identifier, par exemple les intervenants internes liés à l'incident, l'Autorité s'attend notamment à ce que l'institution financière partage l'identité des employés impliqués. Or, dans un souci de protection des renseignements personnels, nous croyons qu'il n'est pas nécessaire de partager l'identité d'un employé précis, sauf dans les situations où l'employé a fait preuve de malveillance. Dans la majorité des cas, il nous apparaît plus approprié, dans un premier temps, de préciser le type d'acteur et d'indiquer les unités administratives impliquées, le cas échéant. Si l'Autorité le juge nécessaire, l'institution financière pourrait fournir plus d'information sur l'identité des personnes impliquées sur demande.

Organismes ou autorités financières ou non financières informés

Nous notons que les exemples fournis par l'Autorité ne sont pas alignés sur le titre du champ « *Organisme ou autorités financières ou non financières informés* ». Les fournisseurs de services, spécialistes d'enquête, ou encore les médias nous semblent des catégories distinctes de celle des organismes ou des autorités financières. À cet effet, nous sommes d'avis que l'Autorité devrait prévoir dans le titre du présent champ une catégorie additionnelle, soit « *toutes autres parties prenantes externes informées de cet incident* » afin d'éviter toute ambiguïté et ainsi mieux représenter les fournisseurs de services, les spécialistes d'enquête, les médias ou autres. Cette distinction nous apparaît pertinente pour mieux cibler et catégoriser les divers intervenants.

Nous remercions l'Autorité pour cette occasion de partager nos commentaires et attendrons favorablement le guide d'application et de mise en œuvre du Règlement.

Pour tout besoin d'information additionnelle, n'hésitez pas à communiquer avec les soussignés.

Veuillez agréer, Monsieur, nos salutations les plus distinguées.

La directrice principale Affaires réglementaires,

Giuseppina Marra, CPA auditrice, IAS.A

Cc.
M^me^ Marie-Andrée Alain, vice-présidente et chef de la conformité et protection des renseignements personnels
M. Pierre-Alexandre Braeken, vice-président Risques non financiers et chef des risques technologiques et cyber