Montréal, le 20 février 2024

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

Objet : Consultation sur le 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

Monsieur,

Nous avons pris connaissance avec grand intérêt du projet de 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 ») de l'Autorité des marchés financiers (« l'Autorité »), soumis à titre de consultation publique.

Étant le premier groupe financier coopératif en Amérique du Nord avec plus de 414,1 G$[1] d'actifs et 7,5 millions de membres et clients[2], 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.

La protection de la confidentialité, de l'intégrité et de la disponibilité des informations utilisées dans le cadre de nos activités est au cœur des priorités du Mouvement Desjardins qui investit considérablement, chaque année, en développement des technologies de l'information afin de continuellement rehausser la sécurité et la qualité de nos systèmes. Ainsi, nous saluons la démarche de l'Autorité ayant pour objectif l'adoption d'un cadre réglementaire permettant d'assurer la mise en place de pratiques de gestion saine et prudente relatives aux incidents de sécurité de l'information.

Également, nous remercions l'Autorité du dialogue entamé avec l'industrie pour échanger sur le projet de règlement. En effet, ces échanges ont permis de bien saisir l'intention derrière certaines dispositions sur lesquelles des préoccupations et questionnements ont été soulevés. Nous comprenons que la démarche de l'Autorité est guidée par la même mission que notre organisation, soit de prévenir et gérer efficacement les incidents pouvant nuire à la sécurité de nos membres et clients, à la confiance qu'ils nous accordent et à la continuité de nos opérations. Nos commentaires ci-après abondent en ce sens et visent à assurer l'atteinte des objectifs ainsi qu'une mise en place optimale du Règlement.

[1] Au 30 septembre 2023 : RG_T3_2023_FR (desjardins.com)
[2] Au 30 septembre 2023 : Fiche de l'investisseur T3 2023 vf.indd (desjardins.com)

Signalement à l'Autorité

Tout d'abord, nous comprenons que le signalement des incidents de sécurité de l'information à l'Autorité devrait se faire selon une approche fondée sur le risque et des critères propres aux institutions financières en fonction de leur taille, leur complexité et la nature de leurs activités. Nous sommes d'avis que la lecture du Règlement devrait faire référence à cette notion afin qu'il soit appliqué dans cette perspective.

En effet, nous comprenons que l'Autorité souhaite que les institutions financières divulguent les incidents majeurs, identifiés selon des critères qui leur sont propres, soit les incidents justifiant une notification à la haute direction et/ou au conseil d'administration. Or, le Règlement ne réfère nulle part à la possibilité de classer les incidents selon leur niveau d'importance ou la gravité de leur impact et, de surcroit, emploie une définition très large des incidents de sécurité sans mentionner de notions de gradation de ceux-ci.

Nous encourageons, par conséquent, l'Autorité à mieux refléter son objectif et ainsi s'assurer que le Règlement énonce des attentes basées sur les principes précédemment énoncés laissant aux institutions financières la flexibilité voulue de l'appliquer selon leurs particularités. Des précisions doivent être apportées afin de circonscrire les incidents à signaler à la haute direction et/ou au conseil d'administration de l'institution financière et donc, à l'Autorité.

De plus, le premier alinéa de l'article 5 du Règlement prévoit que l'incident doit être signalé « au plus tard 24 heures suivant cet incident ». Or, nous en déduisons que l'intention de l'Autorité serait plutôt d'assurer le signalement au plus tard dans les 24 heures suivant la notification de l'incident à la haute direction et/ou au conseil d'administration. Nous recommandons donc à l'Autorité de refléter plus précisément ses intentions à l'égard du délai de divulgation.

Politique de gestion des incidents de sécurité de l'information

Concernant l'article 3, nous comprenons que l'Autorité souhaite que la gestion et le signalement des incidents de sécurité de l'information fassent l'objet d'un cadre de gestion incluant les rôles et responsabilités, politiques et procédures à cet effet. Nous suggérons d'aligner les termes employés sur les attentes notamment énoncées à la *Ligne directrice sur la gestion du risque opérationnel* et à la *Ligne directrice sur la gestion des risques liés aux technologies de l'information* en faisant référence à un cadre de gestion plutôt qu'à une politique, ce qui assurerait la flexibilité requise aux institutions financières.

Formulaire de signalement et suivis à l'Autorité

Un encadrement harmonisé des divulgations d'incident de sécurité de l'information à l'échelle canadienne favoriserait non seulement la réduction de la charge de conformité des institutions financières, mais permettrait parallèlement aux autorités réglementaires et organismes gouvernementaux de dresser plus facilement un portrait global de la situation. De plus, afin de simplifier le processus de signalement des institutions financières leur permettant, en même temps, d'optimiser leurs pratiques opérationnelles au bénéfice de leurs membres et clients, nous suggérons à l'Autorité de s'inspirer par exemple de l'Autorité ontarienne de réglementation du secteur financier (ARSF)[3], laquelle accepte d'être avisée au moyen d'un formulaire comparable émis par une autre autorité de réglementation des services financiers afin de réduire la charge de conformité de ses assujettis.

De plus, conformément aux recommandations[4] proposées par le Conseil de stabilité financière (CSF/FSB), nous encourageons l'Autorité à travailler vers une plus grande convergence des rapports sur les incidents liés à la sécurité de l'information. Cette convergence pourrait notamment prendre la forme d'un protocole de partage d'informations entre les différentes autorités réglementaires permettant ainsi aux assujettis exerçant des activités à travers de multiples juridictions d'effectuer leur divulgation à leur régulateur principal sachant que ce dernier assurera les suivis avec les autres régulateurs concernés.

Par ailleurs, en ce qui concerne l'obligation d'aviser l'Autorité de l'évolution de la situation « au plus tard tous les 3 jours suivant l'avis précédent », nous considérons que cette obligation devrait être plus flexible. En effet, la gestion et la résolution des incidents de sécurité de l'information étant une priorité pour les institutions financières, la transmission de nouvelles informations ne devrait se faire que lorsqu'elles sont disponibles, et ce, jusqu'à la clôture de l'incident. Préconisant la transparence envers nos régulateurs, nous jugeons que la divulgation d'avis subséquents serait plus pertinente si elle est effectuée en fonction des développements de la situation plutôt que sur une périodicité de trois jours.

À cet effet, nous référons l'Autorité aux exigences de signalements subséquents du Bureau du surintendant des institutions financières[5] qui préconise un suivi à mesure que les renseignements deviennent disponibles, tout en se réservant le droit d'exiger au besoin une fréquence de divulgation plus rapprochée.

---

[3] Ligne directrice Gestion des risques liés aux technologies de l'information (« TI ») : « Afin de réduire la charge de travail des entités ou des personnes réglementées qui doivent soumettre plusieurs rapports d'incident, l'ARSF acceptera également d'être avisée au moyen d'un formulaire comparable émis par une autre autorité de réglementation des services financiers», https://www.fsrao.ca/fr/reglementation/lignes-directrices/gestion-des-risques-lies-aux-technologies-de-linformation-ti

[4] « Recommendation 2 : Explore greater convergence of CIR frameworks Financial authorities should continue to explore ways to align their CIR regimes with other relevant authorities, on a cross-border and cross-sectoral basis, to minimise potential fragmentation and improve interoperability. » p.16, https://www.fsb.org/wp-content/uploads/P130423-1.pdf

[5] Préavis : Signalement des incidents liés à la technologie et à la cybersécurité (BSIF, 13 août 2021)

Disposition finale

Finalement, nous avançons qu'un délai d'implantation minimal de douze (12) mois faciliterait l'atteinte des objectifs du Règlement de façon optimale considérant que des rehaussements seront nécessaires afin de pleinement intégrer les nouvelles exigences à notre cadre de gestion interne.

Au nom du Mouvement Desjardins, nous vous remercions pour cette occasion de partager nos commentaires sur ce projet.

Pour toute information additionnelle, n'hésitez pas à communiquer avec les soussignés.

Veuillez agréer, Monsieur, nos salutations les plus distinguées.

La directrice principale Relations réglementaires,

Giuseppina Marra, CPA auditrice, IAS.A

c.c.
M^me^ Marie-Andrée Alain, v.-p. et chef de la conformité et protection des renseignements personnels, Mouvement
M^me^ Véronique Bégnoche, v.-p. Stratégies, gouvernance et conseils en sécurité, Mouvement
M. Pierre-Alexandre Braeken, v.-p. et chef de la gestion des risques technologiques et des cyberrisques, Mouvement
M. Jonathan Dumont-Veillette, v.-p. Risques opérationnels, Mouvement
M. Daniel Alvarez, v.-p. Risques, Gouvernance et performance technologiques, Mouvement