3115, chemin Harvester, bureau 201
Burlington (Ontario) L7N 3N8

20 février 2024

Me Philippe Lebel
Secrétaire et directeur général du secrétariat et des affaires juridiques
Autorité des marchés financiers
Place de la Cité, tour Cominar
2640, boulevard Laurier, 3ième étage
Québec (Québec) G1V 5C1
Télécopieur : 418-525-9512
Courrier électronique : consultation-en-cours@lautorite.qc.ca

Me Lebel,

Veuillez accepter le présent document à titre d'observations de Trans Union du Canada, Inc. (« **TransUnion** ») soumises à l'Autorité des marchés financiers (« **AMF** ») en réponse à la publication pour consultation 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* (« **Projet de règlement** »).

Nous aborderons ci-dessous notre compréhension du Projet de règlement à la suite de son examen et de notre rencontre avec les représentants de l'AMF le 31 janvier dernier.

A. PORTÉE DE LA DÉFINITION D'« INCIDENT DE SÉCURITÉ »

Durant la rencontre de présentation du Projet de règlement, nous avons demandé une clarification de la définition d'incident de sécurité de l'information à l'article 2. Il a été alors confirmé que la définition vise à se distinguer de celle d'incident de confidentialité en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c. P-39.1 (« **Loi sur le secteur privé** »). Non seulement celle-ci vise l'inclusion de ce type d'incident mais va également au-delà de cette catégorie en exigeant, par exemple, que les incidents de sécurité touchant des informations telles que des secrets commerciaux ou professionnels soient divulgués.

Nous souhaitons souligner un dédoublement du régime applicable en la matière, puisque les attaques fructueuses contre des systèmes d'informations contenant des renseignements personnels sont automatiquement des incidents devant être signalés à la Commission d'accès à l'information (« **CAI** ») en vertu de la Loi sur le secteur privé et du règlement en découlant.

Nous vous soumettons qu'un régime législatif complet couvre ce type d'incident et que le législateur a dévolu tous les pouvoirs nécessaires à sa gestion à un régulateur expert en la matière. De ce fait, nous sommes d'avis que la portée du Projet de règlement devrait être réduite en conséquence.

B. DÉSIGNATION DU RESPONSABLE

Afin de permettre aux institutions financières et agents d'évaluation du crédit (« AÉC ») une reddition de comptes plus flexible autant aux gestionnaires qu'aux officiers, nous suggérons de modifier l'article 4 en ajoutant cette possibilité.

Par exemple:

> *4. Une institution financière ou un agent d'évaluation du crédit doit désigner, par écrit, un de ses dirigeants ou gestionnaires et, dans le cas d'une coopérative de services financiers, un de ses gestionnaires, responsable de surveiller la gestion et le signalement des incidents de sécurité de l'information.*
>
> *4. A financial institution or a credit assessment agent must assign, in writing, responsibility for monitoring the management and reporting of information security incidents to one of its officers or managers, and in the case of a financial services cooperative, to one of its managers."*

C. SIGNALEMENT DES INCIDENTS DANS LES 24 HEURES

L'article 5 du Projet de règlement prescrit le signalement des incidents de sécurité dans un délai fixe de 24 heures, soit « *au plus tard 24 heures suivant cet incident* ».

Nous soulignons d'abord qu'aucun autre régulateur au Canada n'exige un signalement dans les 24 heures suivant un incident de sécurité. D'un point de vue pratique, le respect de l'obligation de signalement à l'intérieur d'un délai de 24 heures suivant un incident ne serait pas forcément réalisable puisque cela ne prendrait pas en compte des réalités opérationnelles auxquelles font face les entreprises qui subissent de tels incidents. L'évaluation et la catégorisation d'une situation comme un étant un incident à signaler, par exemple, sont des exercices qui peuvent substantiellement se développer et évoluer au-delà des premières 24 heures de la survenance d'un incident.

Suivant la rencontre avec vos représentants, il a été mentionné que TransUnion avait la latitude de déterminer les critères de catégorisation des incidents de sécurité et que le Projet de règlement vise les incidents d'une importance et d'une gravité telles qu'ils sont signalés à la haute direction d'une entité visée.

Malgré la clarification à l'effet que l'AMF désire être informée des incidents majeurs et que le délai de 24 heures ne commence à courir qu'à partir du signalement interne d'une entité à sa haute direction, il semble encore une fois que le texte proposé au Projet de règlement s'écarte de l'intention de l'AMF dans l'application de cette obligation.

Afin de donner aux entités visées la flexibilité et la latitude nécessaires pour assurer une réponse efficace aux incidents de sécurité, nous suggérons de modifier le texte de l'article 5 en retirant la référence d'« *au plus tard 24 heures suivant cet incident* » ou de la remplacer par des termes plus flexibles tels que *« dès que possible après le signalement de l'incident à la haute direction ».* Un ajustement correspondant est suggéré pour l'article 13(2) du Projet de règlement.

D. SIGNALEMENT À D'AUTRES ORGANISMES

Bien que l'AMF ait manifesté la volonté d'être informée des incidents de sécurité touchant des informations confidentielles relatives aux secrets commerciaux ou au secret professionnel, le retrait du deuxième paragraphe de l'article 5 du Projet de règlement nous apparaît nécessaire.

Le maintien de cette obligation d'aviser l'AMF pourrait entraîner une violation de la confidentialité d'une entente et/ou du secret professionnel de l'avocat, notamment dans les situations où une entité contacterait son assureur ou une firme spécialisée en réponse aux incidents de cybersécurité. Nous croyons qu'une telle obligation de signalement, qui entraine la divulgation de renseignements détaillés sur des contrats entre entreprises. est injustifiée en contexte de réponse à un incident de sécurité et va au-delà du mandat de l'AMF de surveiller les pratiques de gestion des AÉC.

E. SIGNALEMENT SIMULTANÉ À LA CAI ET À L'AMF

L'article 6 du Projet de règlement indique qu'un incident signalé à la CAI doit être divulgué « au même moment à l'Autorité ». Toujours dans un esprit de flexibilité et de capacité opérationnelle, nous suggérons de remplacer l'exigence d'un signalement simultané par une formulation de type « *le signaler le même jour à l'Autorité* ». Un ajustement correspondant est suggéré pour l'article 13(3) du Projet de règlement.

F. PRÉJUDICES ENGENDRÉS PAR L'INCIDENT ET ACCEPTATION DU RISQUE

La règlementation canadienne en matière d'incidents touchant des renseignements personnels est formulée afin de viser le signalement du potentiel de risque de préjudice sérieux et non le risque lui-même. Il n'est pas possible d'affirmer avec une certitude absolue la nature et l'étendue des risques possibles, ceux-ci pouvant se manifester des années après la survenance d'un incident. La même réflexion s'applique quant à une description et une justification de l'acceptation de risques résiduels. Pour ces raisons, les paragraphes (5) et (8) de l'article 11 du Projet de règlement devraient être retirés.

G. MANQUE D'INTEROPÉRABILITÉ AVEC LE RÉGIME ACTUEL

Le signalement des incidents de confidentialité est couvert par la Loi sur le secteur privé. En visant le signalement des incidents de sécurité, qui est une catégorie beaucoup plus vaste, l'AMF touche de façon incidente aux incidents de confidentialité. Nous partageons nos inquiétudes quant au constat que le Projet de règlement avance un deuxième ensemble de normes, créé uniquement pour l'AMF et exigeant un niveau de conformité allant au-delà des exigences de la CAI qui a présentement le mandat législatif de surveiller les incidents de confidentialité.

Les articles 5, 8 à 10 et 12 du Projet de règlement accentuent le manque d'interopérabilité entre ce régime parallèle proposé et les requis législatifs en place. Nous croyons que les exigences supplémentaires propres à l'AMF n'apporteront pas de valeur ajoutée ou d'avantage significatif pour les consommateurs et ne feront qu'alourdir la gestion des incidents de sécurité/de confidentialité.

Le Projet de règlement, si adopté, devrait à notre avis refléter ou, à tout le moins, s'aligner sur les exigences de la CAI qui sont imposées par la loi.

En vertu des pouvoirs qui lui sont conférés par la Loi, l'AMF supervise les activités des AÉC afin:

1) de s'assurer que les droits des consommateurs soient respectés conformément à la manière prescrite par la Loi; et

2) d'établir des normes et attentes concernant les pratiques commerciales et de gestion et de s'assurer que ces attentes soient respectées.

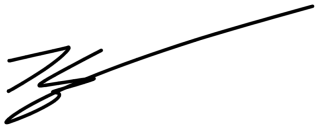
Les lignes directrices applicables aux AÉC détaillent et définissent les attentes et principes en matière de pratiques commerciales et de gestion. Les lignes directrices indiquent d'emblée que l'AMF cherche à atteindre cet objectif au moyen d'une « *approche basée sur des principes* » qui « *confère ainsi aux AÉC la latitude nécessaire leur permettant de déterminer les stratégies, politiques, procédures et processus, ainsi que de voir à leur application en regard de la nature, de la taille et de la complexité de leurs activités* ».

Nous pensons qu'une approche fondée sur des principes qui définit les résultats souhaités au moyen d'orientations offre aux AÉC la flexibilité nécessaire pour obtenir des résultats optimaux pour les consommateurs et pour concevoir des solutions d'atténuation des risques. L'ajout des obligations prévues au Projet de règlement aux attentes énoncées aux lignes directrices viendrait contrecarrer l'approche basée sur les principes en imposant des exigences règlementaires exorbitantes et prescriptives.

Conclusion

Nous vous remercions de nous avoir donné l'occasion de soumettre nos commentaires sur le Projet de règlement. Nous serions heureux de poursuivre la discussion si des renseignements ou précisions supplémentaires vous étaient nécessaires.

Sincèrement,



Thiên-Kim Nguyen, CIPP/C
Conseillère juridique

TRANS UNION DU CANADA, INC.