BAC
Bureau d'assurance du Canada

PAR COURRIEL SEULEMENT
consultation-en-cours@lautorite.qc.ca

Le 13 février 2025

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

Objet : Consultation sur le nouveau formulaire de l'Autorité des marchés financiers pour le signalement des incidents de sécurité de l'information

Le Bureau d'assurance du Canada (ci-après « BAC ») remercie l'Autorité des marchés financiers (ci-après « Autorité ») de l'opportunité qui lui est donnée de prendre part à la consultation sur le nouveau formulaire pour le signalement des incidents de sécurité de l'information.

Nous désirons également vous remercier d'avoir rencontré les membres du groupe de travail du BAC sur les incidents de sécurité de l'information le 16 janvier 2025. À l'occasion de cette rencontre, l'Autorité a précisé qu'un Guide d'application et de mise en œuvre sera prochainement mis à la disposition des assureurs. Nous saluons cette initiative qui contribuera à faciliter la mise en conformité des institutions.

De plus, nous remercions l'Autorité pour les précisions apportées lors de cette rencontre quant au champ d'application du règlement. Nous comprenons que seuls les incidents majeurs rapportés à la haute direction de l'institution financière doivent obligatoirement être signalés à l'Autorité. Ainsi, il appartient à chaque institution d'établir, dans sa procédure de signalement (article 3 al. 2 du règlement), les critères visant à déterminer s'il s'agit d'un incident risquant d'occasionner des répercussions négatives qui doit être rapporté et, le cas échéant, à qui.

Les recommandations énoncées ci-après visent l'atteinte d'un équilibre entre l'allègement du fardeau administratif des assureurs, la protection des consommateurs et l'intégrité du secteur financier québécois.

Informations décrivant ce qui s'est ou qui se produit relatif au présent incident

- Nos de référence d'incidents reliés : La divulgation des autres incidents devrait être limitée à ceux ayant déjà été divulgués à l'Autorité, vu leur matérialité et de leur gravité.

- Description de l'incident : Les autres sections du formulaire permettent de fournir une panoplie de détails. Nous suggérons de limiter cette section à une description sommaire de l'incident, afin d'éviter la duplication d'Informations. Au surplus, une section « Information supplémentaire », à la fin du formulaire, permet aux assureurs de fournir des détails additionnels, si nécessaire.

- Type d'incident : Nous constatons que l'énumération comporte à la fois des types et des causes d'incident. Par exemple, l'erreur humaine (une cause) pourrait entraîner plusieurs types d'incidents. Le BAC recommande de distinguer les types et les causes et de ne conserver que les types d'incidents dans cette section. À titre indicatif, le Bureau du surintendant des institutions financières (ci-après « BSIF ») a prévu une section intitulée « Catégorie d'incident », où le répondant doit sélectionner l'incident technologique ou le cyberincident. Par la suite, la section « Type d'incident » permet de sélectionner une option parmi plusieurs. Nous recommandons à l'Autorité d'adopter une approche similaire à celle du BSIF, dans un esprit d'harmonisation et de cohérence.

- Protection de renseignements personnels : Le BAC reconnaît la pertinence de la troisième option de choix, à savoir « Incertain au moment présent ». Nous recommandons d'ajouter ce choix de réponse à tous les champs/choix de réponse, car il pourrait arriver qu'un assureur ne dispose pas de l'information requise au moment de remplir le formulaire.

- Date et heure de l'occurrence de l'incident : Prévoir un champ de réponse permettant d'inscrire une période approximative ou plusieurs périodes distinctes, le cas échéant. En réalité, il pourrait y avoir plusieurs occurrences d'un même incident. Le formulaire devrait refléter cette réalité. Cette modification serait aussi plus cohérente et distinguerait cette question de la précédente, exigeant la divulgation de la date et de l'heure de la détection de l'incident (ou de la première fois où il est rapporté dans l'organisation).

- Statut de l'incident : Le formulaire du BSIF indique que certains champs doivent obligatoirement être complétés alors que d'autres semblent être optionnels. Il est mentionné dans le formulaire de l'Autorité que : « Pour qu'un incident puisse être fermé, tous les champs d'information obligatoires et requis par le règlement, incluant le rapport post-mortem, doivent avoir été remplis et transmis par le biais du présent formulaire. ». Le BAC recommande à l'Autorité d'identifier clairement les champs obligatoires et requis par le règlement, en y ajoutant un astérisque (*) ou autre signe graphique.

- Date et heure de la maîtrise de l'incident/Date et heure de la clôture (ou fermeture de l'incident) : Les assureurs se questionnent sur la pertinence de préciser l'heure de la maîtrise et de la clôture de l'incident. En effet, cette information est très souvent difficile à identifier et n'apporterait pas de valeur ajoutée réelle au processus de surveillance de l'Autorité.

- Acteurs : Le BAC reconnaît sans équivoque que la transparence est de mise et que l'Autorité doit disposer des informations nécessaires pour assurer un suivi des incidents de sécurité de l'information. Cependant, dans un souci de protection des renseignements personnels, nous nous questionnons sur la nécessité, dans le cadre de ce processus, de divulguer les noms des employés. La mention de l'unité administrative à laquelle ils sont rattachés nous apparaît suffire à l'atteinte de l'objectif recherché.

Aussi, il y aurait lieu d'élargir la définition des acteurs en permettant d'inscrire les noms des comités internes impliqués, sans en énumérer nécessairement les membres.

- Date et heure des signalements aux parties prenantes prévues au règlement/Organismes ou autorités financières ou non financières informées : Nous remarquons que les organismes de règlementation sont compris à la section « parties prenantes prévues au règlement ». Le Règlement mentionne d'ailleurs, à l'article 3 : « (…) à l'Autorité des marchés financiers de même qu'aux autres organismes de réglementation ». La question suivante exige quant à elle de nommer « tout autre organisme financier ou non financier informé de cet incident ». Afin de faciliter la divulgation de l'information requise et d'éviter toute confusion, le BAC recommande de clarifier les expressions « organismes de réglementation » et « autre organisme financier », d'autant plus que dans le deuxième cas, tous les exemples fournis renvoient à des organismes manifestement non financiers.

Informations décrivant selon l'institution les répercussions ou préjudices engendrés, estimés ou appréhendés de l'incident signalé

- Clientèles affectées et volumétrie : Le BAC recommande de limiter l'obligation de divulgation de la nature et de la volumétrie des clientèles à celles intéressant l'Autorité. Ce faisant, nous suggérons la modification suivante « ~~notamment~~ au Québec ». Deuxièmement, nous vous soumettons qu'il serait pertinent de préciser la portée de l'expression « transactions mises en jeu », car elle est imprécise et trop subjective. Enfin, nous souhaitons porter à votre attention que la répartition géographique est une information pouvant être difficile à déterminer et qu'elle risque, dans certains cas, d'être approximative.

- Impacts financiers/Impacts opérationnels/impacts réputationnels/Impacts légaux et règlementaires : L'échelle proposée par l'Autorité (inconnus/faibles/modérés/importants/majeurs) devrait comporter une description des caractéristiques propres à ces différents paliers, afin d'assister les assureurs dans l'identification du degré concret des impacts engendrés par l'incident de sécurité. Cette précision serait d'autant plus utile si l'Autorité entend utiliser universellement son échelle. En effet, toutes les institutions n'utilisent pas les mêmes échelles et devront donc effectuer des analyses et des comparaisons pour déterminer le degré d'impact correspondant aux choix proposés dans le formulaire.

Autres informations

- Enseignements tirés et mesures correctives à venir/Risques résiduels :

  À la suite d'un incident de sécurité, les assureurs prennent immédiatement les moyens requis pour éviter qu'un incident similaire ne se reproduise. D'autres actions sont prises subséquemment sur un long continuum. Ainsi, il peut être difficile pour un assureur de rendre compte, dans les 30 jours de la maîtrise d'un incident, de toutes les mesures correctives envisagées, de les détailler et de fixer les dates d'achèvement estimées de chacune d'elles.

Quant aux risques résiduels, le BAC s'interroge quant au niveau de détails attendu. En effet, il est épineux pour les assureurs de se commettre sur la récurrence potentielle d'un incident de sécurité, dans la mesure où les développements technologiques et les techniques imaginés par les pirates informatiques ou « hackers » sont impossibles à prévoir.

Le BAC profite de cette occasion pour rappeler qu'un « Cadre pour une norme unique de signalement des cyberincidents » a été élaboré par le BAC national. Son objectif premier est d'harmoniser et de simplifier le processus de signalement des incidents au BSIF et aux organismes de réglementation provinciaux. La mise en œuvre de l'idée développée par l'industrie de l'assurance de dommages, soit de permettre la transmission du formulaire de signalement du BSIF aux autorités réglementaires des autres provinces, aurait été une bonne occasion d'harmoniser et d'alléger les pratiques.

Vous remerciant à l'avance de l'attention que vous accorderez aux présentes, veuillez agréer Me Lebel, l'expression de nos meilleurs sentiments.

[redacted]

Johanne Lamanque
Vice-présidente, Québec
Bureau d'assurance du Canada
jlamanque@bac-quebec.qc.ca
514 288-1563, [redacted]

c. c. : Hélène Samson, Directrice de l'encadrement prudentiel et des simulations
(helene.samson@lautorite.qc.ca)
Isabelle Déry, Conseillère experte – Réglementation des institutions financières et agents d'évaluation du crédit
(isabelle.dery@lautorite.qc.ca)
Luc Verreault, Conseiller expert – Risques non-financiers
(luc.verreault@lautorite.qc.ca)

JL/cg