Canadian Life & Health Insurance Association
Association canadienne des compagnies d'assurances de personnes

Mémoire sur le

PROJET DE RÈGLEMENT SUR LA GESTION ET LE SIGNALEMENT DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

présenté à

l'AUTORITÉ DES MARCHÉS FINANCIERS

20 février 2024

SOMMAIRE

L'Association canadienne des compagnies d'assurances de personnes (ACCAP) est heureuse de soumettre à l'Autorité des marchés financiers (AMF) ses observations au sujet du projet de Règlement sur la gestion et le signalement des incidents de sécurité de l'information (le « projet de Règlement »).

Dans le présent mémoire, nous formulons des commentaires clés sur chacune des parties du projet de Règlement. Nos principales recommandations sont les suivantes :

1. Les institutions financières ne devraient être tenues de signaler que les incidents de sécurité de l'information qui à la fois sont importants et touchent les personnes/activités au Québec;
2. Une souplesse devrait être accordée pour ce qui est du signalement d'incidents dans les 24 premières heures;
3. Un protocole de partage d'information sur les incidents de sécurité de l'information devrait être établi entre les autorités de réglementation canadiennes;
4. Les incidents de confidentialité qui ne sont pas considérés comme étant des incidents de sécurité de l'information ne devraient pas être visés par le projet de Règlement;
5. Les rapports sur l'évolution de la situation devraient être produits dans un délai raisonnable et à mesure que de nouveaux renseignements deviennent disponibles;
6. Le projet de Règlement ne devrait pas prévoir de sanctions pécuniaires, et
7. Un délai de mise en œuvre suffisant devrait être prévu.

Nos recommandations et d'autres observations clés sont exposées en détail ci-dessous.

À PROPOS DE NOUS

L'ACCAP est une association à adhésion libre dont les membres détiennent 99 % des affaires d'assurances vie et maladie en vigueur au Canada.

Les assureurs de personnes jouent un rôle clé dans l'économie du Québec. Ils emploient plus de 34 000 Québécois et ont versé 2,2 milliards de dollars en contribution fiscale au Québec en 2022. La vaste majorité des fournisseurs d'assurances vie et maladie sur le marché canadien sont habilités à mener des activités au Québec, et treize d'entre eux y ont leur siège social.

Les assureurs accompagnent les familles québécoises à toutes les étapes de la vie (naissance, études, voyages, retraite, maladie, décès). Notre industrie fournit à 7,3 millions de Québécois une large gamme de produits essentiels à la sécurité financière dans les bons comme dans les mauvais moments, dont l'assurance vie, les rentes et l'assurance maladie complémentaire, y compris l'assurance médicaments.

OBSERVATIONS CLÉS SUR CHACUNE DES PARTIES DU PROJET DE RÈGLEMENT

Chapitre 1 : Champ d'application et interprétation

Le champ d'application du projet de Règlement devrait être restreint au Québec

De nombreuses sociétés membres de l'ACCAP exercent leurs activités dans tout le pays, et certaines à l'échelle internationale. Les institutions financières sont donc déjà assujetties à d'autres contrôles réglementaires en ce qui concerne le signalement des incidents de sécurité de l'information. Il est important d'éviter le double emploi entre les attentes réglementaires, car cela pourrait créer de la disparité parmi ces attentes. Cela pourrait également être lourd à satisfaire pour les sociétés, au moment où celles-ci devraient s'appliquer à gérer la situation engendrée par un incident. Par exemple, le Préavis sur le signalement des incidents liés à la technologie et à la cybersécurité (« le Préavis ») du Bureau du surintendant des institutions financières (BSIF) porte sur les impacts sur le système financier canadien. Par conséquent, nous recommandons que le projet de Règlement vise uniquement les incidents qui touchent les personnes résidant au Québec ou les activités qui y sont exercées.

La définition d'incident de sécurité de l'information doit être clarifiée

En ce qui concerne les définitions figurant dans le projet de Règlement, nous préconisons l'harmonisation la plus complète possible entre les autorités de réglementation, particulièrement avec l'Autorité ontarienne de réglementation des services financiers (ARSF) et le BSIF qui ont déjà leur propre définition.

La définition d'incident de sécurité de l'information donnée à l'article 2 est très large. Il importe que la définition soit claire et qu'elle évite les critères vagues, lesquels rendraient la conformité difficile pour les institutions financières. En outre, une définition claire est nécessaire pour que les institutions financières comprennent les attentes quant au type d'incidents à signaler. Par exemple, l'on ne sait pas exactement s'il est attendu des institutions financières qu'elles signalent les incidents « non prouvés » qui pourraient « éventuellement » avoir un impact sur les clients (incidents avérés par opposition à soupçonnés) ou les tentatives qui ont été stoppées (attaques ayant réussi ou également celles qui ont échoué). Nous présentons ci-dessous des éléments spécifiques de la définition qui pourraient être clarifiés.

Premièrement, il n'est pas indiqué clairement si la définition d'incident de sécurité de l'information prévoit un seuil d'importance relative. De nos discussions avec l'AMF, nous comprenons que seuls les incidents avérés, de grande envergure et qui ont réussi seraient à signaler. Nous recommandons de clarifier cet élément dans le projet de Règlement.

Il devrait appartenir à chaque institution financière de déterminer ce qui constitue un incident « important » en fonction de l'impact sur ses activités, ses opérations et les consommateurs.

Deuxièmement, ce qui est entendu par « atteinte » dans la définition n'est pas clair. Nous recommandons de retirer la mention d'« atteinte » ou de définir le terme dans le projet de Règlement. L'AMF pourrait harmoniser cette définition avec celles qu'appliquent d'autres organismes de réglementation, dont le BSIF dans le Préavis sur le signalement des incidents liés à la technologie et à la cybersécurité.

Chapitre 2 : Gestion des incidents de sécurité de l'information

Section I : Politique de gestion des incidents de sécurité de l'information

Les exigences relatives aux politiques de gestion des incidents de sécurité de l'information devraient être proportionnées

L'article 3 du projet de Règlement énonce ce que doit comporter la politique de l'institution financière en matière de gestion des incidents de sécurité de l'information. Cette approche est trop contraignante. Les institutions financières devraient avoir la souplesse voulue pour déterminer ce qui est inclus dans leurs politiques et leurs procédures de gestion des incidents de sécurité de l'information, en fonction de leur taille ainsi que de la nature et la complexité de leurs activités.

En outre, il se peut que des institutions financières aient déjà en place des politiques et des procédures de gestion des incidents de sécurité de l'information contenues dans d'autres politiques (sur la gestion de la continuité des activités, p. ex.). Il ne devrait pas être attendu des institutions financières qu'elles élaborent une politique autonome pour la gestion des incidents de sécurité de l'information.

Enfin, l'exigence selon laquelle la politique doit inclure une procédure de signalement des incidents à « toute autre partie prenante » est très large. Nous recommandons qu'il soit clairement indiqué dans le projet de Règlement que les institutions financières doivent signaler un incident uniquement aux parties prenantes pour lesquelles l'incident est important et si la loi l'exige.

La surveillance à l'égard des tiers devrait être raisonnable

L'article 3 exige que les institutions financières se dotent de procédures et de mécanismes permettant de détecter et d'évaluer les incidents de sécurité de l'information ainsi que d'y répondre lorsque ces incidents surviennent au sein d'une tierce partie à qui l'institution a confié l'exercice de toute partie d'une activité. Tel qu'elle est rédigée, cette disposition engloberait tous les incidents ayant un impact sur le tiers, même ceux qui n'ont pas d'incidence sur l'institution financière dans l'exercice de l'activité qui lui a été confiée.

Nous recommandons que le projet de Règlement se restreigne aux « fournisseurs de services » à qui a été confié l'exercice de toute partie d'une activité de l'institution financière. Il faudrait également modifier le projet de Règlement de manière à ce qu'il vise uniquement les incidents de grande envergure qui touchent l'institution financière et ses activités. Nous recommandons en outre qu'il soit précisé que la responsabilité de l'institution financière n'exonère pas les fournisseurs de services de leur propre responsabilité et de l'obligation de reddition de comptes s'y rattachant.

Section II : Signalement à l'Autorité des marchés financiers

Une souplesse devrait être accordée pour ce qui est du signalement des incidents dans les 24 premières heures

Il faudrait clarifier à quel moment débute le délai de 24 heures. Il peut y avoir des cas où un incident s'est produit, mais l'institution financière n'en a pas été informée. Nous recommandons de modifier le projet de Règlement pour préciser de signaler à l'Autorité tout incident (ajout en caractères gras) « au plus tard 24 heures suivant **le moment où l'incident est confirmé et les dirigeants ou, selon le cas, les gestionnaires en sont informés** ».

Il faut bien comprendre que l'institution financière doit s'attacher à cerner et à gérer l'incident dans les 24 premières heures et qu'elle pourrait ne pas encore avoir en main toute l'information devant figurer dans le rapport. Nous recommandons qu'il soit uniquement attendu des institutions financières qu'elles fournissent l'information disponible dans les 24 premières heures. Si des détails précis ne sont pas connus au moment où l'institution financière remplit le rapport d'incident, il serait indiqué que

l'information n'est pas encore disponible. À mesure que des renseignements deviennent disponibles, l'institution financière pourra les communiquer promptement.

Comme nous l'avons mentionné plus haut, il devrait uniquement être attendu des institutions financières qu'elles signalent les incidents importants ou de grande envergure. Chaque institution financière devrait pouvoir déterminer ce qui constitue un incident « important » en fonction de l'impact sur ses activités, ses opérations et les consommateurs.

La formule « ayant un risque d'occasionner des répercussions négatives » est également vague. Il faudrait clarifier ce qui est entendu par cela.

Enfin, il ne faudrait pas que les institutions financières soient dissuadées de signaler des incidents aux autorités chargées de l'application de la loi. À cet effet, elles ne devraient pas être tenues de signaler à l'AMF un incident qui a été signalé à un organisme d'application de la loi si l'incident n'atteint pas le seuil de signalement à l'AMF. Dans certains cas, il se peut que l'institution financière soit empêchée de signaler un incident qui a déjà été signalé à d'autres organismes d'application de la loi (des lois à l'international, par exemple, peuvent empêcher le partage de l'information). L'attente devrait être que les institutions financières déclarent les incidents seulement « dans la mesure permise par la loi ».

Un protocole de partage d'information sur les incidents de sécurité de l'information devrait être établi entre les autorités de réglementation

Nous préconisons une plus grande collaboration et un meilleur échange d'information entre l'AMF et les autres organismes de réglementation. Le projet de Règlement prévoit que tout incident de sécurité de l'information signalé à un organisme de réglementation, comme le BSIF, doit également être signalé à l'AMF. Cela double le travail et fait peser une charge indue sur les sociétés, et pourrait entraîner des retards inutiles dans la gestion d'incident.

Comme nous l'avons indiqué plus haut, nous recommandons que le projet de Règlement vise uniquement les incidents qui touchent les personnes résidant au Québec ou les activités qui y sont exercées.

La désignation par exemple d'une autorité principale chargée de recevoir les rapports d'incidents et de diffuser l'information aux autres organismes de réglementation assurerait que ces organismes obtiennent l'information qu'ils requièrent tout en réduisant au minimum les exigences de signalement imposées aux assureurs. Ces derniers pourraient ainsi consacrer le plus de temps possible à la gestion des incidents de sécurité de l'information.

Les incidents de confidentialité qui ne sont pas considérés comme étant des incidents de sécurité de l'information ne devraient pas être à signaler

L'article 6 exige qu'une institution financière qui signale un « incident de confidentialité » à la Commission d'accès à l'information le signale au même moment à l'AMF. Cela crée de la redondance quant au signalement et à la surveillance de ce type d'incidents.

Compte tenu de l'évolution de la législation, dont la mise en œuvre des nouvelles exigences de la *Loi sur la protection des renseignements personnels dans le secteur privé* au Québec, nous estimons qu'il ne devrait pas être attendu de l'institution financière qu'elle signale à l'AMF un incident de confidentialité si cet incident n'atteint pas le seuil de signalement à l'AMF.

Voici des exemples à examiner de situations qui, selon nous, devraient être exclues de la visée du projet de Règlement :

- À la suite d'une erreur humaine, une demande de règlement d'assurance est sauvegardée dans le mauvais fichier et l'assureur envoie une communication renfermant des renseignements d'identification personnelle au mauvais destinataire;
- Lors du traitement d'une demande de règlement, l'institution financière envoie une demande de renseignements ou des lettres au mauvais médecin ou employeur; et
- Un employé non autorisé accède par erreur à des renseignements personnels.

Nous recommandons que les incidents de confidentialité qui ne sont pas considérés comme étant des incidents de sécurité de l'information soient exclus de la visée du projet de Règlement et qu'il soit plutôt fait référence aux lois existantes sur la protection de la vie privée pour les incidents relatifs à des atteintes à la confidentialité. C'est l'approche qu'utilise l'ARSF, laquelle exige que les entités et les personnes réglementées se conforment aux exigences en place relativement aux risques liés aux technologies de l'information (TI) et à la protection des renseignements personnels (p. ex., la *Loi sur la protection des renseignements personnels et les documents électroniques*).

Par conséquent, nous recommandons de modifier le projet de Règlement comme suit (ajout en caractères gras) : « […] sur la protection des renseignements personnels dans le secteur privé **qui est considéré comme étant un incident de sécurité de l'information pour l'application du présent règlement**, le signaler au même moment à l'Autorité ».

Permettre aux institutions financières d'examiner le formulaire de signalement d'incident de sécurité de l'information avant qu'il ne soit finalisé

L'article 7 du projet de Règlement énonce qu'une institution financière doit signaler à l'Autorité un incident de sécurité de l'information en remplissant le formulaire disponible sur le site Web de l'Autorité. Nous demandons que ce formulaire soit mis à la disposition des institutions financières aux fins d'examen et de commentaire avant d'être finalisé.

Comme nous l'avons indiqué plus haut, de nombreux membres de l'ACCAP exercent des activités et fournissent des services aux consommateurs dans tout le pays. Il se peut que ces entités soient déjà assujetties à des exigences de signalement par d'autres organismes de réglementation canadiens. Le fait d'avoir en place des attentes différentes d'une province à l'autre, et au niveau fédéral, sera très lourd pour les sociétés. Cela est particulièrement vrai lorsque le signalement doit être fait dans un délai court. Les assureurs doivent se concentrer sur la gestion de l'incident, et les tout premiers jours sont critiques.

Nous recommandons que l'AMF adopte une approche similaire à celle de l'ARSF, dont la ligne directrice précise ce qui suit : « 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. »

Enfin, nous recommandons qu'il soit clairement indiqué dans le projet de Règlement que toute information transmise à l'AMF demeure confidentielle, car des renseignements sensibles pourraient être inclus dans les rapports. Cela engloberait toute information échangée entre les autorités de réglementation et les organismes d'application de la loi.

Les rapports sur l'évolution de la situation devraient être fournis dans un délai raisonnable et à mesure que de nouveaux renseignements deviennent disponibles

Il est attendu dans le projet de Règlement que les institutions financières avisent l'AMF de l'évolution de la situation au plus tard trois jours suivant l'avis initial, et au plus tard tous les trois jours par la suite, jusqu'à la clôture de l'incident.

Cette exigence est très contraignante pour les sociétés. Comme nous l'avons indiqué précédemment, les institutions financières devraient s'employer à comprendre et à gérer l'incident sans se préoccuper de faire rapport tous les trois jours, surtout si aucun renseignement nouveau important n'est disponible. Nous recommandons plutôt que les institutions financières communiquent toute nouvelle information à l'AMF dans un délai raisonnable et à mesure qu'elle devient disponible, ce qui est conforme à l'approche adoptée par d'autres autorités de réglementation.

Si l'AMF décide de maintenir l'exigence de fournir des rapports sur l'évolution de la situation tous les trois jours, le projet de Règlement devrait être modifié pour préciser qu'il s'agit de trois jours ouvrables. En effet, si certaines unités au sein de l'institution financière travailleront en dehors des heures ouvrables afin d'atténuer et de résoudre l'incident, d'autres, comme celles chargées de faire rapport, continueraient à observer les heures ouvrables normales.

Nous souhaitons également voir clarifié ce qui est considéré comme la « clôture de l'incident de sécurité de l'information ». Nous recommandons la cohérence avec les autres autorités de réglementation sur ce point et sur le délai pour faire rapport. Par exemple, le Préavis du BSIF précise : « Une fois l'incident maîtrisé, les activités reprises et le dossier clos, l'IFF doit rendre compte au BSIF de son examen postérieur à l'incident et des leçons apprises. »

En outre, le rapport post-incident exigé à l'article 10 est suffisant pour aviser que l'incident est sous contrôle. L'envoi d'un second avis confirmant que les activités ont repris leur cours normal, exigé à l'article 9, est redondant. Cela est sous-entendu une fois l'incident clos.

Correction de la numérotation dans la version française du projet de Règlement

Le chapitre II du projet de Règlement est divisé en sections. Dans la version française, la section II est manquante (le texte saute de la section I à la section III). Il faudrait corriger la numérotation dans la version définitive du Règlement.

Section III : Registre des incidents de sécurité de l'information

Les institutions financières devraient avoir la souplesse voulue pour élaborer leur propre registre des incidents de sécurité de l'information

L'article 11 du projet de Règlement exige qu'une institution financière tienne à jour un registre des incidents de sécurité de l'information à des fins internes. Il précise ce que doit comprendre ce registre. Étant donné que le registre doit servir à des fins internes, les institutions financières devraient à notre avis avoir la souplesse voulue pour déterminer ce qui doit y être versé. Pour cette raison, nous recommandons que le projet de Règlement suive une approche fondée sur des principes, sans prescrire les renseignements devant figurer au registre.

Le projet de Règlement exige que l'institution financière conserve le registre pendant une période minimale de sept ans à compter de la date du rapport. Ce délai est plus long que d'autres périodes de conservation prévues par des législations similaires. Par exemple, le Règlement sur les incidents de confidentialité du Québec exige que les renseignements au registre des incidents de confidentialité soient tenus à jour et conservés pendant cinq ans seulement. Nous recommandons que le projet de Règlement s'harmonise avec d'autres législations similaires.

Chapitre III : Sanctions administratives pécuniaires

Le projet de Règlement ne devrait pas prévoir de sanctions pécuniaires

Le chapitre III énonce les sanctions pécuniaires imposées aux institutions financières qui ne répondent pas aux attentes énoncées dans le projet de Règlement.

Les cyberincidents sont imprévisibles, ne font pas partie du cours normal des affaires et ne sont généralement pas dus à la négligence ou à de mauvaises pratiques commerciales. Dans la plupart des cas, l'institution financière en est victime. L'imposition de sanctions n'est pas une pratique courante pour les incidents de sécurité de l'information et l'AMF serait la première autorité au Canada à y recourir. Nous ne pensons pas que cela soit approprié.

Nous recommandons que l'AMF adopte une approche similaire à celles d'autres autorités de réglementation en matière de conformité. Par exemple, le Préavis du BSIF sur le signalement des incidents liés à la technologie et à la cybersécurité précise que « si l'IFF omet de signaler un incident […], elle s'expose à une surveillance accrue, notamment des activités de suivi renforcées, à son inscription à la liste de surveillance ou à son classement à un stade d'intervention ». En vertu de la ligne

directrice de l'ARSF, « la non-conformité à ces lignes directrices peut avoir une incidence sur l'aptitude d'un titulaire de permis individuel au moment du renouvellement ». À notre avis, l'une ou l'autre de ces approches serait appropriée.

Enfin, il est énoncé dans le projet de Règlement que l'institution financière qui ne transmet pas à l'AMF un signalement au moment où un avis est transmis à la Commission d'accès à l'information se verrait imposer une sanction pécuniaire. Comme nous l'avons recommandé plus haut, ce type d'incidents, qui ne sont pas considérés comme étant des incidents de sécurité de l'information, devraient être exclus de la visée du projet de Règlement.

Chapitre IV : Disposition finale

Un délai de mise en œuvre suffisant devrait être accordé aux sociétés

Nous recommandons qu'un délai de deux ans soit accordé pour la mise en œuvre du Règlement, car certaines sociétés devront adapter leurs processus internes existants et pourraient devoir embaucher du personnel pour répondre aux nouvelles exigences. Nous demandons également que la période de transition soit clairement définie lorsque le Règlement définitif sera publié.

CONCLUSION

Nous vous remercions de nous avoir donné l'occasion de formuler des commentaires concernant le projet de Règlement sur la gestion et le signalement des incidents de sécurité de l'information. Si vous avez des questions ou souhaitez en discuter davantage, n'hésitez pas à communiquer avec Lyne Duhaime, présidente, ACCAP-Québec, et vice-présidente principale, Politiques et réglementation des marchés, à l'adresse lduhaime@clhia.ca.

Canadian Life & Health Insurance Association
Association canadienne des compagnies d'assurances de personnes

1001, boul. de Maisonneuve Ouest,
bureau 630
Montréal (Québec)
H3A 3C8
514-845-9004
info@clhia.ca