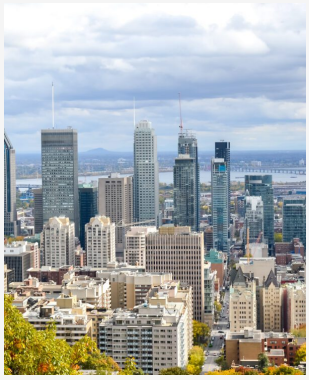
OSLER

Le nouveau régime de signalement des incidents de sécurité de l'information de l'AMF du Québec : ce que les institutions financières doivent savoir



3 DÉCEMBRE 2024 12 MIN DE LECTURE

Expertises Connexes

- Cybersécurité et intervention en cas d'incident lié à la sécurité
- Réglementation des services financiers
- Respect de la vie privée et gestion de l'information
- Services financiers

Auteurs(trice): Éloïse Gratton, Ad. E., François Joli-Coeur, Justin P'ng, CIPP/C/US, Marguerite Rolland

Le 23 octobre 2024, l'Autorité des marchés financiers du Québec (l'AMF) a publié 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* [PDF] (Règlement de l'AMF). À partir du 23 avril 2025, des obligations de gestion et de signalement des incidents de sécurité de l'information pour certaines institutions financières et agents d'évaluation de crédit entreront en vigueur. Notons qu'un bon nombre de ces exigences sont conformes aux attentes de l'AMF énoncées dans sa Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications.

Le présent article décrit les principales obligations du règlement de l'AMF et les compare à deux régimes de signalement existants : le Préavis de Signalement des incidents liés à la technologie et à la cybersécurité du Bureau du surintendant des institutions financières (Préavis du BSIF), et le *Règlement sur les incidents de confidentialité* (Règlement sur le secteur privé) de la *Loi sur la protection des renseignements personnels dans le secteur privé du* Québec (LPRPSP).

Champ d'application

Le Règlement de l'AMF s'applique aux assureurs[1], fédérations et caisses[2], institutions de dépôt[3], sociétés de fiducie[4], et agents d'évaluation du crédit[5] exerçant leurs activités au Québec (collectivement, les Institutions Financières). En raison de leurs activités au Québec, ces organisations sont généralement assujetties au Règlement sur le secteur privé[6], et certaines de ces organisations ou leurs activités sont réglementées en tant qu'institutions financières fédérales (IFF) assujetties au Préavis du BSIF. Comme nous l'expliquons ci-dessous, les organisations soumises à ces deux autres régimes de signalement devraient être bien placées pour se conformer au Règlement de l'AMF étant donné son chevauchement avec ces régimes existants.

Le Règlement de l'AMF s'applique aux « incidents de sécurité de l'information » qui sont

définis comme « une atteinte à la disponibilité, à l'intégrité ou à la confidentialité des systèmes d'information ou aux informations qu'ils contiennent »[7]. En revanche, le Préavis du BSIF s'applique à un « incident lié à la technologie ou à la cybersécurité » qui est « un incident qui a ou pourrait avoir des conséquences sur les activités d'une IFF, y compris sur les plans de la confidentialité, de l'intégrité ou de la disponibilité de ses systèmes ou de ses renseignements »[8]. La LPRPSP s'applique plus étroitement aux « incidents de confidentialité » qui concernent l'accès, l'utilisation ou la communication non autorisés d'un renseignement personnel, ainsi que la perte ou toute autre atteinte à la protection des renseignements personnels[9].

Seuil de signalement

En vertu du Règlement de l'AMF, un incident de sécurité de l'information doit être signalé à l'AMF lorsqu'il a été (1) signalé aux dirigeants ou aux gestionnaires de l'Institution Financière et qu'il a « un risque d'occasionner des répercussions négatives », ou (2) signalé ou qui fait l'objet d'un avis à un organisme de réglementation, à une personne ou à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, ou, contractuellement, est chargé de dédommager le préjudice qui aurait pu être causé par cet incident. De plus, un incident de confidentialité signalé à la Commission d'accès à l'information (CAI) doit également faire l'objet d'un signalement à l'AMF[10].

Un incident qui atteint ce seuil est susceptible d'atteindre également le seuil prévu par le Préavis du BSIF, qui définit un incident à signaler comme un incident pouvant répondre à l'un de seize critères, y compris des répercussions sur les opérations, l'infrastructure, les systèmes ou les données de l'IFF[11]. De même, le Préavis du BSIF inclut les incidents qui sont signalés à d'autres « autres organismes de surveillance ou de réglementation canadiens ou étrangers » comme un élément déclencheur du signalement d'un incident au BSIF[12]. En revanche, le seuil de signalement prévu par la LPRPSP n'exige la déclaration d'un incident à la CAI que s'il existe un risque de préjudice sérieux pour les personnes concernées[13].

Principales obligations

Signalement initial à l'AMF

En vertu du Règlement de l'AMF, les Institutions Financières doivent signaler les incidents de sécurité de l'information à l'AMF dans les 24 heures suivant le signalement de l'incident à l'interne aux dirigeants ou gestionnaires de l'institution ou à l'externe selon les critères susmentionnés[14]. De même, en vertu du Préavis du BSIF, les IFF doivent signaler un incident lié à la technologie ou à la cybersécurité à la Division du risque lié aux technologies du BSIF dans les 24 heures suivant l'incident ou plus tôt si possible[15]. Toutefois, en vertu du Règlement sur le secteur privé, les incidents de confidentialité doivent être signalés « avec diligence » à la CAI[16].

Avis des développements

Le Règlement de l'AMF exige que les Institutions Financières informent l'AMF de l'évolution de l'incident tous les trois jours à compter de la notification initiale jusqu'à ce qu'un avis de résolution de l'incident soit soumis (sauf pour les incidents de confidentialité signalés à la CAI)[17]. Cette exigence diffère du Préavis du BSIF, qui attend des IFF qu'elles « fassent périodiquement le point (...) à mesure que de nouveaux renseignements deviennent disponibles », avec un exemple de mise à jour quotidienne[18]. Le Règlement sur le secteur

privé exige seulement que certains développements soient notifiés à la CAI « avec diligence »[19].

Forme et contenu du signalement

Selon le Règlement de l'AMF, les Institutions Financières doivent signaler un incident à l'AMF en remplissant un formulaire disponible sur le site web de l'AMF (qui n'est pas encore disponible)[20]. Le Préavis du BSIF exige également que les IFF signalent un incident en remplissant un formulaire disponible sur le site web du BSIF et en le transmettant à la Division du risque lié aux technologies du BSIF[21]. D'une manière générale, le formulaire de signalement prévu par le Préavis du BSIF exige que les IFF fournissent

- des renseignements sur l'incident et les personnes à contacter
- l'emplacement/site et les secteurs d'activité touchés, (iii) une description de l'incident et des risques connexes
- le niveau de priorité de l'incident
- les renseignements sur les notifications internes et externes de l'incident[22]

Enfin, le Règlement sur le secteur privé exige un avis écrit à la CAI, mais n'impose pas l'utilisation du formulaire [PDF] qu'elle met à la disposition du public[23]. L'avis peut être envoyé par la poste ou par courriel. Le Règlement sur le secteur privé exige que les renseignements suivants soient inclus dans un avis d'incident :

- le nom et le numéro d'entreprise au Québec de l'organisation ainsi que le nom et les coordonnées d'un représentant
- une description des renseignements personnels visés par l'incident ainsi que des circonstances et de la cause de l'incident
- la date ou la période où l'incident a eu lieu ou et le moment où l'organisation a pris connaissance de l'incident
- le nombre de personnes concernées par l'incident et le nombre de celles qui résident au Québec
- une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées
- les renseignements relatifs à la notification des personnes dont les renseignements personnels sont concernés par l'incident
- les mesures d'atténuation et de réduction des risques que l'organisation a prises après l'incident ou qu'elle a l'intention de prendre, y compris les délais de mise en œuvre
- si un autre organisme exerçant des responsabilités semblables à celles de la CAI a été avisé de l'incident[24]

Rapport final d'incident

Dans les 30 jours suivant la transmission à l'AMF de l'avis confirmant qu'un incident est maîtrisé, l'Institution Financière doit également envoyer à l'AMF un rapport qui

- identifie la source et le type d'incident
- fournit une évaluation de la récurrence potentielle de l'incident
- décrit les mesures prises pour réduire la probabilité que de nouveaux incidents de même nature ne se produisent[25]

Le Préavis du BSIF exige également ce type de rapport post-incident, mais il ne doit contenir que l'examen postérieur à l'incident de l'IFF après l'incident et les leçons apprises de l'expérience[26]. Le Règlement sur le secteur privé et la LPRPSP n'imposent pas de rapport post-incident.

Registre des incidents

Le Règlement de l'AMF exige que les Institutions Financières tiennent à jour un registre de sécurité de l'information contenant les informations suivantes :

- la date et l'heure de l'incident
- la localisation de l'incident
- la nature de l'incident
- une description détaillée de l'incident, incluant une évaluation de la récurrence potentielle de l'incident
- tout préjudice engendré par l'incident
- tout tiers concerné par l'incident
- les actions prises
- l'acceptation ou non du risque résiduel et les justificatifs afférents
- les actions prévues
- la date de clôture de l'incident[27]

Le Règlement sur le secteur privé exige la tenue d'un registre des incidents de confidentialité dont le contenu est essentiellement similaire, à quelques différences près[28]. En revanche, le Préavis du BSIF n'exige pas qu'une IFF tienne un registre des incidents, et la ligne directrice du BSIF sur la Gestion du risque lié aux technologies et du cyberrisque ne le recommande pas non plus comme pratique exemplaire.

Politique de gestion des incidents de sécurité de l'information

En vertu du Règlement de l'AMF, les Institutions Financières sont tenues de mettre en œuvre une politique de gestion des incidents qui comprend des procédures et des mécanismes de détection, d'évaluation et de réponse aux incidents de sécurité de l'information, et de signalement de ces incidents aux dirigeants ou gestionnaires de l'Institution Financière et à

tout autre intervenant (y compris les clients, les fournisseurs de services, les consommateurs, l'AMF elle-même et d'autres organismes chargés à l'application de la loi)[29].

Le Règlement de l'AMF exige également que la responsabilité de la gestion des incidents et de l'établissement de rapports soit confiée par écrit à un responsable ou à un gestionnaire désigné[30]. Alors que le Préavis du BSIF ne prévoit pas d'exigences concernant les politiques de gestion des incidents et la responsabilité y afférente, la ligne directrice du BSIF sur la Gestion du risque lié aux technologies et du cyberrisque contient des recommandations comparables, bien qu'elles soient facultatives. Enfin, si les obligations de gouvernance prévues par le Règlement sur le secteur privé et la LPRPSP sont moins prescriptives, elles requièrent toujours, de manière générale, l'établissement et la mise en œuvre de politiques et de pratiques de gouvernance qui garantissent la protection des renseignements personnels, et exigent la désignation d'un responsable de la protection de la vie privée[31].

Recommandations et mesures de mise en conformité

La préparation à la mise en conformité avec le Règlement de l'AMF diffère selon le type d'Institution Financière dont relève l'organisation. Dans les deux cas, les organisations doivent être conscientes que des sanctions administratives pécuniaires pouvant aller de 250 à 2 500 dollars canadiens peuvent être imposées en cas de non-respect du Règlement de l'AMF, en fonction du type d'infraction[32].

Les IFF déjà présentes au Québec

Les IFF qui exercent déjà des activités au Québec et qui sont déjà en mesure de se conformer au Préavis du BSIF, à la LPRPSP et au Règlement sur le secteur privé sont en grande partie en mesure de se conformer au Règlement de l'AMF. Collectivement, les deux autres régimes de signalement se chevauchent en grande partie avec le Règlement de l'AMF. Toutefois, il est conseillé d'examiner les programmes de conformité et les ententes conclues avec les fournisseurs de services afin d'identifier et de combler toute lacune dans les procédures de conformité.

Institutions Financières non réglementées par le BSIF

Les organisations qui ne sont pas réglementées par le BSIF (et qui ne sont donc pas assujetties au Préavis du BSIF) devront peut-être déployer des efforts de conformité plus importants. Bien que ces organisations devraient déjà être en mesure de se conformer au Règlement sur le secteur privé en raison de leurs activités au Québec, les exigences du Règlement sur le secteur privé sont moins spécifiques et prescriptives que celles contenues dans le Règlement de l'AMF. Par conséquent, ces organisations devront adapter leurs programmes de conformité et leurs ententes conclues avec les fournisseurs de services afin de refléter les exigences du règlement de l'AMF.

---

[1] Les assureurs agréés en vertu de la *Loi sur les assureurs* et les fédérations de sociétés mutuelles visées par cette loi.

[2] Fédérations et caisses populaires non-membres d'une fédération visée à la *Loi sur les coopératives de services financiers*.

[3] Institutions de dépôt autorisées en vertu de la *Loi sur les institutions de dépôts et la*

protection des dépôts.

[4] Les sociétés fiduciaires autorisées en vertu de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*.

[5] Les agents d'évaluation du crédit désignés en vertu de la *Loi sur les agents d'évaluation du crédit*.

[6] Règlement relatif au secteur privé, article 1.

[7] Règlement de l'AMF, article 2.

[8] Préavis du BSIF, « Portée et définition ».

[9] LPRPSP, article 3.6.

[10] Règlement de l'AMF, articles 5 et 6.

[11] Préavis du BSIF, « Critères de signalement ».

[12] Préavis du BSIF, « Critères de signalement ».

[13] LPRPSP, articles 3.5 para 2, 3.7.

[14] Règlement de l'AMF, article 5.

[15] Préavis du BSIF, « Exigences de signalement initial ».

[16] LPRPSP, article 3.5, paragraphe 2.

[17] Règlement de l'AMF, article 8.

[18] Préavis du BSIF, « Exigences de signalement subséquent ».

[19] Règlement de l'AMF, article 4.

[20] Règlement de l'AMF, article 7.

[21] Préavis du BSIF, « Exigences de signalement initial ».

[22] Voir le formulaire de déclaration d'incident technologique et cybernétique du BSIF [PDF].

[23] Règlement sur le secteur privé, article 3.

[24] Règlement sur le secteur privé, article 3.

[25] Règlement de l'AMF, article 9.

[26] Préavis du BSIF, « Exigences de signalement subséquent ».

[27] Règlement de l'AMF, article 10.

[28] Règlement sur le secteur privé, article 7.

[29] Règlement de l'AMF, article 3.

[30] Règlement de l'AMF, article 4.

[31] ARPPIPS, articles 3.1 para 2, 3.2.

[32] Règlement de l'AMF, articles 12-13.