5.2

Réglementation et lignes directrices

5.2 RÉGLEMENTATION ET LIGNES DIRECTRICES

5.2.1 Consultation

Aucune information.

5.2.2 Publication

DÉCISION N° 2024-PDG-0043

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

Vu le pouvoir de l'Autorité des marchés financiers (l'« Autorité ») de prendre 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* (le « Règlement »), conformément aux articles 66 et 73 de la *Loi sur les agents d'évaluation du crédit*, RLRQ, c. A-8.2 (la « LAEC »), aux articles 485 et 496 de la *Loi sur les assureurs,* RLRQ, c. A-32.1 (la « LA »), aux articles 601.1 et 601.9 de la *Loi sur les coopératives de service financiers*, RLRQ, c. C-67.3 (la « LCSF »), au paragraphe *u* de l'article 43 et à l'article 45.9 de la *Loi sur les institutions de dépôts et la protection des* dépôts, RLRQ, c. I-13.2.2 (la « LIDPD ») et conformément aux articles 277 et 286 de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02 (la « LSFSE »);

Vu le pouvoir de l'Autorité prévu à la LAEC, à la LA, à la LCSF, à la LIDPD et à la LSFSE, de prendre un règlement, qui appartient exclusivement à son président-directeur général, conformément à l'article 24 de la *Loi sur l'encadrement du secteur financier*, RLRQ, c. E-6.1;

Vu la publication pour consultation au Bulletin de l'Autorité le 7 décembre 2023 [(2023) B.A.M.F., vol. 20, n° 48, section 5.2.1] du projet de Règlement accompagné de l'avis prévu à l'article 10 de la *Loi sur les règlements*, RLRQ, c. R-18.1, conformément au troisième alinéa de l'article 67 de la LAEC, au troisième alinéa de l'article 486 de la LA, au troisième alinéa de l'article 601.2 de la LCSF, au troisième alinéa de l'article 45 de la LIDPD et au troisième alinéa de l'article 278 de la LSFSE;

Vu les modifications apportées au projet de Règlement à la suite de cette consultation;

Vu l'obligation de soumettre un règlement pris en vertu des articles 66 et 73 de la LAEC, des articles 485 et 496 de la LA, des articles 601.1 et 601.9 de la LCSF, du paragraphe *u* de l'article 43 et de l'article 45.9 de LIDPD, des articles 277 et 286 de la LSFSE au ministre des Finances (le « Ministre »), qui peut l'approuver avec ou sans modification, conformément au premier alinéa de l'article 67 de la LAEC, au premier alinéa de l'article 486 de la LA, au premier alinéa de l'article 601.2 de la LCSF, au premier alinéa de l'article 45 de la LIDPD, et conformément au premier alinéa de l'article 278 de la LSFSE;

Vu le projet de Règlement présenté par la Direction principale de l'encadrement et de la résolution ainsi que la recommandation du surintendant des institutions financières de prendre le Règlement et d'autoriser sa transmission au Ministre pour approbation;

En conséquence :

L'Autorité prend 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*, dans ses versions française et

anglaise, dont les textes sont annexés à la présente décision, et en autorise la transmission au Ministre pour approbation.

Fait le 16 septembre 2024.

Yves Ouellet
Président-directeur général

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[i]

L'Autorité des marchés financiers (l'« Autorité ») publie, en version française et anglaise, le règlement suivant :

- *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*

Avis de publication

Le règlement a été pris par l'Autorité le 16 septembre 2024, a reçu l'approbation ministérielle requise et entrera en vigueur le 23 avril 2025.

L'arrêté ministériel approuvant le règlement a été publié dans la *Gazette officielle du Québec*, en date du 23 octobre 2024 et est reproduit ci-dessous.

Le 24 octobre 2024

---

[i] Diffusion autorisée par Les Publications du Québec

A.M., 2024-13

Arrêté numéro 2024-13 du ministre des Finances en date du 7 octobre 2024

Loi sur les agents d'évaluation du crédit
(chapitre A-8.2)

Loi sur les assureurs
(chapitre A-32.1)

Loi sur les coopératives de services financiers
(chapitre C-67.3)

Loi sur les institutions de dépôts et la protection des dépôts
(chapitre I-13.2.2)

Loi sur les sociétés de fiducie et les sociétés d'épargne
(chapitre S-29.02)

CONCERNANT 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

VU que l'article 66 de la Loi sur les agents d'évaluation du crédit (chapitre A-8.2) prévoit qu'en plus des autres règlements qu'elle peut prendre en vertu de cette loi, l'Autorité des marchés financiers peut, par règlement, déterminer les normes applicables aux agents d'évaluation du crédit relativement à leurs pratiques commerciales et à leurs pratiques de gestion;

VU que le premier alinéa de l'article 67 de cette loi prévoit que tout règlement pris en vertu de la présente loi par l'Autorité des marchés financiers est approuvé, avec ou sans modification, par le ministre des Finances;

VU que les troisième et quatrième alinéas de cet article prévoient qu'un projet de règlement est publié au Bulletin de l'Autorité des marchés financiers, que l'avis prévu à l'article 10 de la Loi sur les règlements (chapitre R-18.1) y est joint et qu'un projet de règlement ne peut être soumis pour approbation avant l'expiration d'un délai de 30 jours à compter de sa publication;

VU que le cinquième alinéa de cet article prévoit qu'un tel règlement entre en vigueur à la date de sa publication à la *Gazette officielle du Québec* ou à une date ultérieure qu'il indique, qu'il est aussi publié au Bulletin de l'Autorité des marchés financiers et qu'en cas de différence entre le règlement publié au Bulletin de l'Autorité des marchés financiers et celui publié à la *Gazette officielle du Québec*, ce dernier prévaut;

VU que l'article 73 de cette loi prévoit qu'un règlement pris en vertu de cette loi peut prévoir qu'un manquement à l'une de ses dispositions peut donner lieu à une sanction administrative pécuniaire et que ce règlement peut prévoir des conditions d'application de la sanction et déterminer les montants ou leur mode de calcul, lesquels peuvent notamment varier selon la gravité du manquement, sans toutefois excéder les montants maximaux prévus à l'article 72 de cette loi;

VU que l'article 485 de la Loi sur les assureurs (chapitre A-32.1) prévoit qu'en plus des autres règlements qu'elle peut prendre en vertu de cette loi, l'Autorité des marchés financiers peut, par règlement, déterminer les normes applicables aux assureurs autorisés relativement à leurs pratiques commerciales et à leurs pratiques de gestion et aux fédérations de sociétés mutuelles relativement à leurs pratiques de gestion;

VU que le premier alinéa de l'article 486 de cette loi prévoit que tout règlement pris en vertu de la présente loi par l'Autorité des marchés financiers est approuvé, avec ou sans modification, par le ministre des Finances;

VU que les troisième et quatrième alinéas de cet article prévoient qu'un projet de règlement est publié au Bulletin de l'Autorité des marchés financiers, que l'avis prévu à l'article 10 de la Loi sur les règlements (chapitre R-18.1) y est joint et qu'un projet de règlement ne peut être soumis pour approbation avant l'expiration d'un délai de 30 jours à compter de sa publication;

VU que le cinquième alinéa de cet article prévoit qu'un tel règlement entre en vigueur à la date de sa publication à la *Gazette officielle du Québec* ou à une date ultérieure qu'il indique. Il est aussi publié au Bulletin de l'Autorité des marchés financiers. En cas de différence entre le règlement publié au Bulletin de l'Autorité des marchés financiers et celui publié à la *Gazette officielle du Québec*, ce dernier prévaut;

VU que l'article 496 de cette loi prévoit que l'Autorité des marchés financiers peut, dans un règlement pris en vertu de cette loi, prévoir qu'un manquement à l'une de ses dispositions peut donner lieu à une sanction administrative pécuniaire et que ce règlement peut prévoir des conditions d'application de la sanction et déterminer les montants ou leur mode de calcul, lesquels peuvent notamment varier selon la gravité du manquement, sans toutefois excéder les montants maximums prévus à l'article 494;

VU que l'article 601.1 de la Loi sur les coopératives de services financiers (chapitre C-67.3) prévoit que l'Autorité des marchés financiers peut, par règlement, déterminer les

normes applicables aux coopératives de services financiers relativement à leurs pratiques commerciales et à leurs pratiques de gestion;

VU que le premier alinéa de l'article 601.2 de cette loi prévoit que tout règlement pris en vertu de l'article 601.1 par l'Autorité des marchés financiers est approuvé, avec ou sans modification, par le ministre des Finances;

VU que les troisième et quatrième alinéas de cet article prévoient qu'un projet de règlement est publié au Bulletin de l'Autorité des marchés financiers, que l'avis prévu à l'article 10 de la Loi sur les règlements (chapitre R-18.1) y est joint et qu'un projet de règlement ne peut être soumis pour approbation avant l'expiration d'un délai de 30 jours à compter de sa publication;

VU que le cinquième alinéa de cet article prévoit qu'un tel règlement entre en vigueur à la date de sa publication à la *Gazette officielle du Québec* ou à une date ultérieure qu'il indique, qu'il est aussi publié au Bulletin de l'Autorité des marchés financiers et qu'en cas de différence entre le règlement publié au Bulletin de l'Autorité des marchés financiers et celui publié à la *Gazette officielle du Québec*, ce dernier prévaut;

VU que l'article 601.9 de cette loi prévoit que le ministre des Finances ou l'Autorité des marchés financiers peut, dans un règlement pris en vertu de la cette loi, prévoir qu'un manquement à l'une de ses dispositions peut donner lieu à une sanction administrative pécuniaire et que ce règlement peut prévoir des conditions d'application de la sanction et déterminer les montants ou leur mode de calcul, lesquels peuvent notamment varier selon la gravité du manquement, sans toutefois excéder les montants maximums prévus par l'article 601.7;

VU que le paragraphe *u* de l'article 43 de la Loi sur les institutions de dépôts et la protection des dépôts (chapitre I-13.2.2) prévoit qu'en outre des pouvoirs de réglementation qui lui sont conférés par cette loi, l'Autorité des marchés financiers peut faire des règlements pour déterminer les normes applicables aux institutions de dépôts autorisées relativement à leurs pratiques commerciales et à leurs pratiques de gestion;

VU que le premier alinéa de l'article 45 de cette loi prévoit qu'un règlement pris par l'Autorité des marchés financiers en application de cette loi est soumis à l'approbation du ministre des Finances, qui peut l'approuver avec ou sans modification;

VU que le troisième alinéa de cet article prévoit qu'un projet de règlement visé au premier alinéa de cet article ne peut être soumis pour approbation avant l'expiration d'un délai de 30 jours à compter de sa publication et qu'il entre en vigueur à la date de sa publication à la *Gazette officielle du Québec* ou à toute autre date ultérieure qui y est déterminée;

VU que l'article 45.9 de cette loi prévoit que l'Autorité des marchés financiers peut, dans un règlement pris en vertu de cette loi, prévoir qu'un manquement à l'une de ses dispositions peut donner lieu à une sanction administrative pécuniaire et que ce règlement peut prévoir des conditions d'application de la sanction et déterminer les montants ou leur mode de calcul, lesquels peuvent notamment varier selon la gravité du manquement, sans toutefois excéder les montants maximums prévus à l'article 45.7;

VU que l'article 277 de la Loi sur les sociétés de fiducie et les sociétés d'épargne (chapitre S-29.02) prévoit qu'en plus des autres règlements qu'elle peut prendre en vertu de cette loi, l'Autorité des marchés financiers peut, par règlement, déterminer les normes applicables aux sociétés de fiducie autorisées relativement à leurs pratiques commerciales et leurs pratiques de gestion;

VU que le premier alinéa de l'article 278 de cette loi prévoit que tout règlement pris en vertu de cette loi par l'Autorité des marchés financiers est approuvé, avec ou sans modification, par le ministre des Finances;

VU que les troisième et quatrième alinéas de cet article prévoient qu'un projet de règlement est publié au Bulletin de l'Autorité des marchés financiers, que l'avis prévu à l'article 10 de la Loi sur les règlements (chapitre R-18.1) y est joint et qu'un projet de règlement ne peut être soumis pour approbation avant l'expiration d'un délai de 30 jours à compter de sa publication;

VU que le cinquième alinéa de cet article prévoit qu'un tel règlement entre en vigueur à la date de sa publication à la *Gazette officielle du Québec* ou à une date ultérieure qu'il indique, qu'il est aussi publié au Bulletin de l'Autorité des marchés financiers et qu'en cas de différence entre le règlement publié au Bulletin et celui publié à la *Gazette officielle du Québec*, ce dernier prévaut;

VU que l'article 286 de cette loi prévoit que l'Autorité des marchés financiers peut, dans un règlement pris en vertu de cette loi, prévoir qu'un manquement à l'une des dispositions peut donner lieu à une sanction administrative pécuniaire et que ce règlement peut prévoir des conditions d'application de la sanction et déterminer les montants ou leur mode de calcul, lesquels peuvent notamment varier selon la gravité du manquement, sans toutefois excéder les montants maximums prévus à l'article 284;

VU que le 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 a été publié au Bulletin de l'Autorité des marchés financiers, volume 20, n° 48 du 7 décembre 2023;

VU que l'Autorité des marchés financiers a adopté le 16 septembre 2024, par la décision n° 2024-PDG-0043, 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;

VU qu'il y a lieu d'approuver ce règlement sans modification;

EN CONSÉQUENCE, le ministre des Finances approuve sans modification 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, dont le texte est annexé au présent arrêté.

Le 7 octobre 2024

Le ministre des Finances,
ERIC GIRARD

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

Loi sur les agents d'évaluation du crédit
(chapitre A-8.2, a. 66 et 73).

Loi sur les assureurs
(chapitre A-32.1, a. 485 et 496).

Loi sur les coopératives de services financiers
(chapitre C-67.3, a. 601.1 et 601.9).

Loi sur les institutions de dépôts et la protection des dépôts
(chapitre I-13.2.2, a. 43, par. *u* et a. 45.9).

Loi sur les sociétés de fiducie et les sociétés d'épargne
(chapitre S-29.02, a. 277 et 286).

CHAPITRE I
CHAMP D'APPLICATION ET INTERPRÉTATION

1. Le présent règlement s'applique aux institutions financières suivantes :

1° un assureur autorisé en vertu de la Loi sur les assureurs (chapitre A-32.1) et une fédération de sociétés mutuelles visée par cette loi;

2° une fédération et une caisse qui n'est pas membre d'une fédération visées à la Loi sur les coopératives de services financiers (chapitre C-67.3);

3° une institution de dépôts autorisée en vertu de la Loi sur les institutions de dépôts et la protection des dépôts (chapitre I-13.2.2);

4° une société de fiducie autorisée en vertu de la Loi sur les sociétés de fiducie et les sociétés d'épargne (chapitre S-29.02).

Il s'applique également à un agent d'évaluation du crédit désigné en vertu de la Loi sur les agents d'évaluation du crédit (chapitre A-8.2).

2. Pour l'application du présent règlement, on entend par « incident de sécurité de l'information » une atteinte à la disponibilité, à l'intégrité ou à la confidentialité des systèmes d'information ou aux informations qu'ils contiennent.

CHAPITRE II
GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

SECTION I
POLITIQUE DE GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

3. Une institution financière ou un agent d'évaluation du crédit doit établir et mettre en œuvre une politique de gestion des incidents de sécurité de l'information qui comporte, notamment, des procédures et des mécanismes permettant de détecter, d'évaluer et de répondre aux incidents de sécurité de l'information pouvant survenir au sein de l'institution, d'une caisse membre d'une fédération, de l'agent d'évaluation du crédit, ou d'un tiers à qui cette institution, cette caisse ou cet agent a confié l'exercice de toute partie d'une activité, dans la mesure où l'incident affecte l'activité qui lui a été confiée.

La politique de gestion des incidents de sécurité de l'information comporte également une procédure de signalement des incidents de sécurité de l'information aux dirigeants ou, selon le cas, aux gestionnaires de l'institution financière ou de l'agent d'évaluation du crédit, y compris une procédure de signalement à ceux-ci lorsque cet incident survient au sein d'une caisse membre d'une fédération ou d'un tiers visé au premier alinéa.

En outre, la politique doit prévoir une procédure de signalement à toute autre partie prenante, notamment aux clients, aux tiers à qui cette institution ou cet agent a confié l'exercice de toute partie d'une activité, aux consommateurs, à l'Autorité des marchés financiers de même qu'aux autres organismes de réglementation.

4. Une institution financière ou un agent d'évaluation du crédit doit désigner, par écrit, un de ses dirigeants ou, 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.

SECTION II
SIGNALEMENT À L'AUTORITÉ DES MARCHÉS FINANCIERS

5. Une institution financière ou un agent d'évaluation du crédit doit aviser l'Autorité de tout incident de sécurité de l'information ayant un risque d'occasionner des répercussions négatives qui a été signalé à ses dirigeants ou, selon le cas, à ses gestionnaires au plus tard 24 heures suivant le moment auquel il a été signalé.

L'institution financière ou l'agent d'évaluation du crédit doit aussi aviser l'Autorité, dans ce même délai, de tout incident de sécurité de l'information qui a été 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.

6. Une institution financière ou un agent d'évaluation du crédit doit, lorsqu'il avise la Commission d'accès à l'information, instituée par l'article 103 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1), d'un incident de confidentialité visé au deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1), aviser au même moment l'Autorité.

7. Une institution financière ou un agent d'évaluation du crédit avise l'Autorité d'un incident de sécurité de l'information en remplissant le formulaire disponible sur le site Web de l'Autorité.

8. Une institution financière ou un agent d'évaluation du crédit doit aviser l'Autorité de l'évolution de la situation au plus tard 3 jours suivant l'avis qui lui a été donné en vertu de l'article 5 et au plus tard tous les 3 jours suivant l'avis précédent jusqu'à la transmission à l'Autorité d'un avis confirmant que l'incident est maîtrisé et que les activités ont repris leur cours normal.

9. Une institution financière ou un agent d'évaluation du crédit transmet à l'Autorité un rapport dans un délai de 30 jours suivant la transmission à l'Autorité de l'avis confirmant qu'un incident est maîtrisé et que les activités ont repris leur cours normal. Le rapport contient, notamment, les éléments suivants :

1° l'identification de la source et du type d'incident;

2° l'appréciation de l'institution financière ou de l'agent d'évaluation du crédit quant à la récurrence potentielle de l'incident;

3° les moyens pris pour réduire la probabilité que de nouveaux incidents de même nature ne se produisent.

SECTION III
REGISTRE DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

10. Une institution financière ou un agent d'évaluation du crédit doit tenir à jour un registre des incidents de sécurité de l'information qui comprend, pour chaque incident :

1° la date et l'heure de celui-ci;

2° sa localisation;

3° sa nature;

4° une description détaillée de celui-ci, incluant les renseignements contenus au paragraphe 2° de l'article 9;

5° les préjudices engendrés par celui-ci;

6° les tiers concernés par l'incident;

7° les actions prises;

8° l'acceptation ou non du risque résiduel et les justificatifs afférents;

9° les actions prévues;

10° la date de sa clôture.

11. Une institution financière ou un agent d'évaluation du crédit doit conserver les renseignements consignés au registre de manière sécurisée et confidentielle, afin d'en maintenir l'intégrité pour une période minimale de 5 ans à compter de la date du rapport visé à l'article 9.

CHAPITRE III
SANCTIONS ADMINISTRATIVES PÉCUNIAIRES

12. Une sanction administrative pécuniaire d'un montant de 250 $ dans le cas d'une personne physique ou de 1 000 $ dans les autres cas peut être imposée à une institution financière ou à un agent d'évaluation du crédit visé à l'article 1 :

1° qui, en contravention à l'article 4, n'a pas désigné, par écrit, un de ses dirigeants ou, selon le cas, un de ses gestionnaires, responsable de surveiller la gestion et le signalement des incidents de sécurité de l'information;

2° qui, en contravention de l'article 5, n'a pas avisé l'Autorité d'un incident au plus tard 24 heures suivant le moment auquel il a été signalé à ses dirigeants ou, selon le cas, à ses gestionnaires;

3° qui, en contravention à l'article 6, n'a pas avisé l'Autorité au moment où un avis est transmis à la Commission d'accès à l'information;

4° qui, en contravention à l'article 8, n'a pas avisé l'Autorité de l'évolution de la situation, au plus tard 3 jours suivant l'avis visé à l'article 5 et au plus tard tous les 3 jours suivant l'avis précédent, jusqu'à la transmission d'un avis confirmant que l'incident est maîtrisé et que les activités ont repris leur cours normal.

13. Une sanction administrative pécuniaire d'un montant de 500 $ dans le cas d'une personne physique ou de 2 500 $ dans les autres cas peut être imposée à une institution financière ou à un agent d'évaluation du crédit visé à l'article 1 :

1° qui, en contravention à l'article 3, n'établit pas ou ne met pas en œuvre une politique de gestion des incidents de sécurité de l'information;

2° qui, en contravention à l'article 10, ne tient pas à jour un registre des incidents de sécurité de l'information;

3° qui, en contravention à l'article 11, ne conserve pas les renseignements au registre des incidents de sécurité de l'information pour une période minimale de 5 ans à compter de la date du rapport visé à l'article 9.

CHAPITRE IV
DISPOSITION FINALE

14. Le présent règlement entre en vigueur le (*indiquer ici la date qui suit de 6 mois la date de la publication du présent règlement à la Gazette officielle du Québec*).

84264

M.O., 2024-13

Order number 2024-13 of the Minister of Finance, 7 October 2024

Credit Assessment Agents Act
(chapter A-8.2)

Insurers Act
(chapter A-32.1)

Act respecting financial services cooperatives
(chapter C-67.3)

Deposit Institutions and Deposit Protection Act
(chapter I-13.2.2)

Trust Companies and Savings Companies Act
(chapter S-29.02)

CONCERNING the Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents

WHEREAS section 66 of the Credit Assessment Agents Act (chapter A-8.2) stipulates that, in addition to the other regulations it may make under this Act, the *Autorité des marches financiers* may, by regulation, determine the standards that apply to credit assessment agents as regards their commercial practices and management practices;

WHEREAS the first paragraph of section 67 of the said Act stipulates that a regulation made under this Act by the *Autorité des marches financiers* is approved by the Minister of Finance with or without amendment;

WHEREAS the third and fourth paragraphs of the said section stipulate that a draft of a regulation must be published in the *Bulletin de l'Autorité des marches financiers* with the notice required under section 10 of the Regulations Act (chapter R-18.1) and that the draft of the regulation may not be submitted for approval before 30 days have elapsed since the publication of the draft;

WHEREAS the fifth paragraph of the said section stipulates that a regulation under this section comes into force on the date of its publication in the *Gazette officielle du Québec* or on any later date specified in it, that it must also be published in the *Bulletin de l'Autorité des marches financiers* and that, if the regulation published in the *Bulletin de l'Autorité des marches financiers* differs from the one published in the *Gazette officielle du Québec*, the latter prevails;

WHEREAS section 73 de of the said Act stipulates that a regulation made under this Act may specify that a failure to comply with the regulation may give rise to a monetary administrative penalty, that the regulation may define the conditions for applying the penalty and set forth the amounts or the methods for determining them and that the amounts may vary according to the seriousness of the failure to comply, without exceeding the maximum amounts provided for in section 72;

WHEREAS section 485 of the Insurers Act (chapter A-32.1) stipulates that, in addition to other regulations that it may make under this Act, the *Autorité des marches financiers* may, by regulation, determine the standards applicable to authorized insurers in relation to their commercial practices and their management practices and to federations of mutual companies in relation to their management practices;

WHEREAS the first paragraph of section 486 of the said Act stipulates that a regulation made under this Act by the *Autorité des marches financiers* is approved by the Minister of Finance with or without amendment;

WHEREAS the third and fourth paragraphs of the said section stipulate that a draft of a regulation must be published in the *Bulletin de l'Autorité des marches financiers* with the notice required under section 10 of the Regulations Act (chapter R-18.1) and that the draft of the regulation may not be submitted for approval and the regulation may not be made before 30 days have elapsed since the publication of the draft;

WHEREAS the fifth paragraph of the said section stipulates that a regulation under this section comes into force on the date of its publication in the *Gazette officielle du Québec* or on any later date specified in it, that it must also be published in the *Bulletin de l'Autorité des marches financiers* and that, if the regulation published in the *Bulletin de l'Autorité des marches financiers* differs from the one published in the *Gazette officielle du Québec*, the latter prevails;

WHEREAS section 496 of the said Act stipulates that the *Autorité des marches financiers* may, in a regulation made under this Act, specify that a failure to comply with the regulation may give rise to a monetary administrative penalty, that the regulation may define the conditions for applying the penalty and set forth the amounts or the methods for determining them and that the amounts may vary according to the seriousness of the failure to comply, without exceeding the maximum amounts provided for in section 494;

WHEREAS section 601.1 of the Act respecting financial services cooperatives (chapter C-67.3) stipulates that the *Autorité des marches financiers* may, by regulation, determine the standards applicable to financial services cooperatives in relation to their business and management practices;

WHEREAS the first paragraph of section 601.2 of the said Act stipulates that a regulation made under section 601.1 by the *Autorité des marches financiers* is approved by the Minister of Finance with or without amendment;

WHEREAS the third and fourth paragraphs of the said section stipulate that a draft of a regulation must be published in the *Bulletin de l'Autorité des marches financiers* with the notice required under section 10 of the Regulations Act (chapter R-18.1) and that the draft of the regulation may not be submitted for approval and the regulation may not be made before 30 days have elapsed since the publication of the draft;

WHEREAS the fifth paragraph of the said section stipulates that a regulation under this section comes into force on the date of its publication in the *Gazette officielle du Québec* or on any later date specified in it, that it must also be published in the *Bulletin de l'Autorité des marches financiers* and that, if the regulation published in the *Bulletin de l'Autorité des marches financiers* differs from the one published in the *Gazette officielle du Québec*, the latter prevails;

WHEREAS section 601.9 of the said Act stipulates that the *Autorité des marches financiers* may, in a regulation made under this Act, specify that a failure to comply with the regulation may give rise to a monetary administrative penalty, that the regulation may define the conditions for applying the penalty and set forth the amounts or the methods for determining them and that the amounts may vary according to the seriousness of the failure to comply, without exceeding the maximum amounts provided for in section 601.7;

WHEREAS the paragraph *u* of section 43 of the Deposit Institutions and Deposit Protection Act (chapter I-13.2.2) stipulates that, in addition to the regulatory powers assigned to it by this Act, the *Autorité des marches financiers* may make regulations for determining the standards applicable to authorized deposit institutions in relation to their commercial practices and their management practices;

WHEREAS the first paragraph of section 45 of the said Act stipulates that a regulation of the *Autorité des marches financiers* under this Act must be submitted for approval to the Minister of Finance, who may approve it with or without amendment;

WHEREAS the third paragraph of the said section stipulates that a draft of a regulation referred to in the first paragraph may not be submitted for approval and the regulation may not be made before the expiry of 30 days after the publication of the draft regulation and that the regulation comes into force on the date of its publication in the *Gazette officielle du Québec* or on any later date determined in the regulation;

WHEREAS section 45.9 of the said Act stipulates that the *Autorité des marches financiers* may, in a regulation made under this Act, specify that a failure to comply with the regulation may give rise to a monetary administrative penalty, that the regulation may define the conditions for applying the penalty and set forth the amounts or the methods for determining them and that the amounts may vary according to the seriousness of the failure to comply, without exceeding the maximum amounts provided for in section 45.7;

WHEREAS section 277 of the Trust Companies and Savings Companies Act (chapter S-29.02) stipulates that in addition to other regulations that it may make under this Act, the *Autorité des marches financiers* may, by regulation, determine the standards applicable to authorized trust companies in relation to their commercial and management practices;

WHEREAS the first paragraph of section 278 of the said Act stipulates that a regulation made under this Act by the *Autorité des marches financiers* is approved by the Minister of Finance with or without amendment;

WHEREAS the third and fourth paragraphs of the said section stipulate that a draft of a regulation must be published in the *Bulletin de l'Autorité des marches financiers* with the notice required under section 10 of the Regulations Act (chapter R-18.1) and that the draft of the regulation may not be submitted for approval and the regulation may not be made before 30 days have elapsed since the publication of the draft;

WHEREAS the fifth paragraph of the said section stipulates that a regulation under this section comes into force on the date of its publication in the *Gazette officielle du Québec* or on any later date specified in it, that it must also be published in the *Bulletin de l'Autorité des marches financiers* and that, if the regulation published

in the *Bulletin de l'Autorité des marches financiers* differs from the one published in the Gazette officielle du Québec, the latter prevails;

WHEREAS section 286 of the said Act stipulates that the *Autorité des marches financiers* may, in a regulation made under this Act, specify that a failure to comply with the regulation may give rise to a monetary administrative penalty, that the regulation may define the conditions for applying the penalty and set forth the amounts or the methods for determining them and that the amounts may vary according to the seriousness of the failure to comply, without exceeding the maximum amounts provided for in section 284;

WHEREAS the draft Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents was published in the *Bulletin de l'Autorité des marchés financiers*, volume 20, no. 48 of December 7, 2023;

WHEREAS the *Autorité des marches financiers* made, on September 16, 2024, by the decision no. 2024-PDG-0043, Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents;

WHEREAS there is cause to approve this regulation without amendment;

CONSEQUENTLY, the Minister of Finance approves without amendment Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents appended hereto.

October 7, 2024

ERIC GIRARD
Minister of Finance

Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents

Credit Assessment Agents Act
(chapter A-8.2, ss. 66 and 73).

Insurers Act
(chapter A-32.1, ss. 485 and 496).

Act respecting financial services cooperatives
(chapter C-67.3, ss. 601.1 and 601.9).

Deposit Institutions and Deposit Protection Act
(chapter I-13.2.2, s. 43, par. *u* and s. 45.9).

Trust Companies and Savings Companies Act
(chapter S-29.02, ss. 277 and 286).

CHAPTER I
SCOPE AND INTERPRETATION

1. This Regulation applies to the following financial institutions:

(1) insurers authorized under the Insurers Act (chapter A-32.1) and federations of mutual companies that are subject thereto;

(2) federations and credit unions not members of a federation that are subject to the Act respecting financial services cooperatives (chapter C-67.3);

(3) deposit institutions authorized under the Deposit Institutions and Deposit Protection Act (chapter I-13.2.2); and

(4) trust companies authorized under the Trust Companies and Savings Companies Act (chapter S-29.02).

This Regulation also applies to credit assessment agents designated under the Credit Assessment Agents Act (chapter A-8.2).

2. For purposes of this Regulation, "information security incident" means an attack on the availability, integrity or confidentiality of information systems or the information they contain.

CHAPTER II
MANAGEMENT OF INFORMATION SECURITY INCIDENTS

DIVISION I
INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

3. A financial institution or a credit assessment agent must develop and implement an information security incident management policy that includes, without limitation, procedures and mechanisms for detecting, assessing and responding to information security incidents that may occur within the institution, a credit union that is a member of a federation, the credit assessment agent, or a third party to which such institution, credit unition that is a member of a federation, or credit assessment agent has entrusted the performance of any part of an activity, if the incident affects the activity entrusted to such third party.

The information security incident management policy shall also contain a procedure for the reporting of information security incidents to the officers or, where applicable, the managers of the financial institution or the credit assessment agent, including a procedure for the reporting of such incidents thereto when they occur within a credit union that is a member of a federation or a third party referred to in the first paragraph.

Furthermore, the policy must include a procedure for the reporting of incidents to any other stakeholders, including clients, third parties to which the institution or agent has entrusted the performance of any part of an activity, consumers, the Autorité des marchés financiers, and any other regulatory bodies.

4. A financial institution or a credit assessment must assign, in writing, responsibility for monitoring the management and reporting of information security incidents to one of its officers or, in the case of a financial services cooperative, one of its managers.

DIVISION II
REPORTING TO THE AUTORITÉ DES MARCHÉS FINANCIERS

5. Where an information security incident with potentially adverse impacts is reported to the officers or, where applicable, the managers of a financial institution or a credit assessment agent, the financial institution or the credit assessment agent must, not later than 24 hours from the time the incident is so reported, notify the Authority of the incident.

The financial institution or the credit assessment agent must, within that same period, also notify the Authority of any information security incident that has been reported or been the subject of a notice to a regulatory body, a person or a body responsible under law for the prevention, detection or repression of crime or statutory offences or contractually responsible for providing compensation for injury that may have been caused by the incident.

6. Where a financial institution or a credit assessment agent notifies the Commission d'accès à l'information, established under section 103 of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1), of a confidentiality incident referred to in paragraph 2 of section 3.5 of the Act respecting the protection of personal information in the private sector (chapter P-39.1), it must notify the Authority of the incident at the same time.

7. A financial institution or a credit assessment agent shall notify the Authority of an information security incident by completing the form available on the Authority's website.

8. A financial institution or a credit assessment agent must notify the Authority of developments in the situation not later than three days after notice is given to the Authority pursuant to section 5 and not later than every three days thereafter, until a notice is sent to the Authority confirming that the incident is under control and that operations have returned to normal.

9. A financial institution or a credit assessment agent shall send a report to the Authority within 30 days following the date the notice is sent to the Authority confirming that the incident is under control and that operations have returned to normal. The report shall, in particular:

(1) identify the source of the incident and the type of incident;

(2) provide the financial institution's or credit assessment agent's assessment regarding a potential recurrence of the incident; and

(3) describe the actions taken to reduce the likelihood of incidents of a similar nature occurring in the future.

DIVISION III
INFORMATION SECURITY INCIDENT REGISTER

10. A financial institution or a credit assessment agent must maintain a current information security incident register that shall include, for each incident:

(1) the date and time of the incident;

(2) the location of the incident;

(3) the nature of the incident;

(4) a detailed description of the incident, including the information specified in subparagraph 2 of section 9;

(5) any injury caused by the incident;

(6) any third parties involved in the incident;

(7) actions taken;

(8) whether the residual risk is accepted or not accepted and the rationale for accepting or not accepting it;

(9) planned actions; and

(10) the incident close date.

11. A financial institution or a credit assessment agent must keep the information recorded in the register in a secure and confidential manner so as to maintain the information's integrity for a minimum period of five years from the date of the report referred to in section 9.

CHAPTER III
MONETARY ADMINISTRATIVE PENALTIES

12. A monetary administrative penalty of $250 in the case of a natural person and $1,000 in any other case may be imposed on a financial institution or a credit assessment agent contemplated in section 1 that:

(1) in contravention of section 4, fails to assign, in writing, responsibility for monitoring the management and reporting of information security incidents to one of its officers or, where applicable, one of its managers;

(2) in contravention of section 5, fails to notify the Authority of an incident not later than 24 hours after the time the incident is reported to its officers or, where applicable, its managers;

(3) in contravention of section 6, when notifying the Commission d'accès à l'information of an incident, fails to notify the Authority of the incident at the same time; or

(4) in contravention of section 8, fails to notify the Authority of developments in the situation not later than three days following the notice referred to in section 7 and not later than every three days thereafter, until a notice is sent to the Authority confirming that the incident is under control and operations have returned to normal.

13. A monetary administrative penalty of $500 in the case of a natural person and $2,500 in any other case may be imposed on a financial institution or a credit assessment agent referred to in section 1 that:

(1) in contravention of section 3, fails to develop or implement an information security incident management policy;

(2) in contravention of section 10, fails to maintain a current information security incident register; or

(3) in contravention of section 11, fails to keep the information in the information security incident register for a minimum period of five years from the date of the report contemplated in section 9.

CHAPTER IV
FINAL PROVISION

14. This Regulation comes into force on (*indicate the date that is six months after the date of its publication in the Gazette officielle du Québec*).

107061