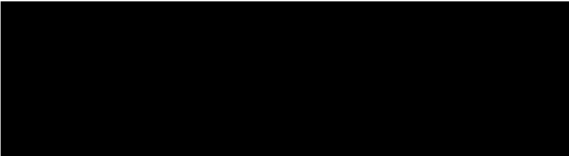




Le 31 mars 2016

PAR COURRIEL



La présente fait suite à votre demande d'accès à l'information reçue par courriel le 1^{er} mars 2016 et pour laquelle je vous ai transmis un accusé réception le 2 mars 2016. Votre demande est ainsi libellée :

« Les rapports, bilans ou documents en lien avec des virus ou autres logiciels malveillants ayant infecté le réseau informatique de votre institution en 2013, 2014 et 2015. »

En réponse à votre demande, voici les informations demandées.

Virus

Tous les postes de travail et les serveurs de la Caisse sont protégés par des logiciels antivirus. La détection des virus est journalisée et la disponibilité des mises à jour est vérifiée plusieurs fois par jour.

Les virus détectés sont contenus et nettoyés automatiquement par le système antivirus que la Caisse a mis en place. Aucun virus n'a affecté le réseau informatique de la Caisse pour toutes les années visées par votre demande.

Autres logiciels malveillants

En ce qui a trait aux incidents reliés à des cryptologiciels (type de logiciels malveillants), nous vous informons que deux incidents ont été répertoriés sur des postes spécifiques : l'un en 2014 et l'autre en 2015. Ces incidents ont été pris en charge rapidement et aucune perte de données n'a été enregistrée. Dans les deux cas, il s'agissait de deux nouveaux virus qui ne pouvaient être détectés par notre système antivirus.

Pour les autres logiciels malveillants, nous vous informons qu'un incident a été détecté en 2013, lequel faisait suite à une intervention volontaire survenue lors de tests d'intrusion annuels que la Caisse effectue pour s'assurer de la robustesse et de la sécurité de son

[REDACTED]

réseau. Puisque les équipes d'opérations de la Caisse n'étaient pas informées de la tenue de ces tests, ils ont immédiatement détecté cet incident et pris les mesures appropriées.

La sécurité informatique est une préoccupation constante pour la Caisse. C'est pourquoi des copies de sécurité sont prises plusieurs fois par jour par la Caisse pour éviter les perturbations dues à ce type d'incidents. Par ailleurs, lorsque la Caisse détecte un nouveau virus, nous avisons les éditeurs de nos logiciels antivirus afin que ces nouveaux virus soient ajoutés aux mesures de sécurité que nous avons mises en place.

Nous considérons que la présente répond entièrement à votre demande d'accès à l'information.

En terminant, pour votre information, nous vous faisons part de la teneur de l'article 135 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* :

«135. Une personne dont la demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels peut demander à la Commission de réviser cette décision.

Une personne qui a fait une demande en vertu de la présente loi peut demander à la Commission de réviser toute décision du responsable sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur l'application de l'article 9 ou sur les frais exigibles.

Ces demandes doivent être faites dans les trente jours qui suivent la date de la décision ou de l'expiration du délai accordé par la présente loi au responsable pour répondre à une demande. La Commission peut toutefois, pour un motif raisonnable, relever le requérant du défaut de respecter ce délai.»

Veillez agréer, [REDACTED] mes salutations distinguées.

[REDACTED]
Ginette Depelteau
Vice-présidente principale,
Conformité et investissement responsable et
Responsable de l'accès à l'information
et de la protection des renseignements personnels