ASSEMBLÉE NATIONALE DU QUÉBEC

PREMIÈRE SESSION QUARANTE-DEUXIÈME LÉGISLATURE

Journal des débats

de la Commission permanente des finances publiques

Le jeudi 21 novembre 2019 — Vol. 45 N° 46

Consultations particulières sur la question de la fuite de données personnelles chez Desjardins

Président de l'Assemblée nationale :
M. François Paradis

2019

Abonnement annuel (TPS et TVQ en sus):

Débats de l'Assemblée	145,00 $
Débats de toutes les commissions parlementaires	500,00 $
Pour une commission parlementaire en particulier	100,00 $
Index (une session, Assemblée et commissions)	30,00 $

Achat à l'unité: prix variable selon le nombre de pages.

Règlement par chèque à l'ordre du ministre des Finances et adressé comme suit:

Assemblée nationale du Québec
Direction de la gestion immobilière et des ressources matérielles
1020, rue des Parlementaires, bureau RC.85
Québec (Québec)
G1A 1A3

Téléphone: 418 643-2754
Télécopieur: 418 643-8826

Consultation des travaux parlementaires de l'Assemblée ou des commissions parlementaires dans Internet à l'adresse suivante:
www.assnat.qc.ca

Dépôt légal: Bibliothèque nationale du Québec
ISSN 0823-0102

Commission des finances publiques

Le jeudi 21 novembre 2019 — Vol. 45 N° 46

Table des matières

Autres intervenants

M. Jean-François Simard, président
M. Mario Asselin, président suppléant

Mme Émilie Foster
Mme Marwah Rizqy
M. Gaétan Barrette
M. Jean-Bernard Émond
M. Louis-Charles Thouin
M. Gabriel Nadeau-Dubois

* M. Guy Cormier, Mouvement Desjardins
* M. Denis Berthiaume, idem
* M. Louis Morisset, AMF
* M. Patrick Déry, idem
* M. Joel Heft, Equifax Canada inc.
* M. Eric Prud'homme, ABC
* Mme Angelina Mason, idem
* Mme Marie-Claude Champoux, OPC
* M. André Allard, idem

* Témoins interrogés par les membres de la commission

Le jeudi 21 novembre 2019 — Vol. 45 N° 46

Consultations particulières sur la question de la fuite de données personnelles chez Desjardins

(Onze heures quarante-six minutes)

Le Président (M. Simard) : Chers collègues, alors, à l'ordre, s'il vous plaît! Bienvenue à toutes et à tous, aux parlementaires comme aux non-parlementaires.

Comme vous le savez, la commission est réunie afin de procéder aux consultations particulières et auditions publiques sur la question de la fuite de données personnelles chez Desjardins.

Mme la secrétaire, vous allez bien?

La Secrétaire : Oui.

Le Président (M. Simard) : Y aurait-il des remplacements ce matin?

La Secrétaire : Oui, M. le Président. Alors, M. Reid (Beauharnois) est remplacé par M. Lafrenière (Vachon); M. Derraji (Nelligan) est remplacé par Mme Rizqy (Saint-Laurent); et M. Ouellet (René-Lévesque) est remplacé par M. Gaudreault (Jonquière).

Le Président (M. Simard) : Très bien. Alors, comme nous avons, malgré nous, commencé légèrement en retard, j'aurais besoin de votre consentement afin que nous puissions poursuivre après l'heure initialement envisagée. M. le député de Robert-Baldwin.

M. Leitão : Merci, M. le Président. Bien sûr, consentement, mais c'est que je soulignais que c'est quand même ironique qu'on fasse ça puisqu'on est ici sous une procédure un peu spéciale. Mais nous allons être bons joueurs. Consentement.

Remarques préliminaires

Le Président (M. Simard) : Très bien. Merci pour ce consentement. Alors, comme vous le savez, chaque audition commence par des remarques générales, des remarques préliminaires. Alors, il y a des remarques qui sont faites de part et d'autre de cette table. Et nous allons commencer par la partie gouvernementale. M. le député de Saint-Jérôme, la parole est à vous.

M. Youri Chassin

M. Chassin : Merci, M. le Président. J'aimerais rappeler, en commençant, que, si le gouvernement a décidé d'aller de l'avant avec les audiences d'aujourd'hui, c'est en raison de l'aspect humain de la fuite de données chez Desjardins. Donc, au-delà des actions déjà entreprises par le gouvernement, si nous sommes ici, c'est pour répondre aux nombreuses questions des clients touchés, des Québécois qui ont des inquiétudes, qui veulent savoir ce qu'ils risquent et ce qui a été fait pour qu'ils soient protégés. Ce sont leurs questions, leurs histoires que nous avons tous entendues en comté, comme députés, que nous avons tous à l'esprit ce matin.

Il est important de rappeler, pour que les débats du jour puissent avoir lieu dans l'ordre... de se rappeler, donc, qu'il existe une différence fondamentale entre les dossiers de protection des dossiers... des données personnelles, pardon, dans les ministères et les organismes et la protection des données financières dans les institutions privées. La responsabilité de l'État existe dans les deux cas, mais n'est pas la même. J'insiste sur ce point parce que le mélange des genres n'aide en rien les Québécois touchés par la fuite de données.

Le premier sujet, nos ministères l'ont bien en main avec des projets de loi. Nous aurons l'occasion d'en débattre à satiété à cette occasion.

Le deuxième, c'est celui auquel on s'intéresse aujourd'hui, soit ce qui est fait en matière de protection des données financières des individus au sein d'institutions bancaires privées.

Nous sommes conscients qu'une enquête est présentement en cours et nous respectons le fait que certaines informations doivent demeurer confidentielles puisque celles-ci se déroulent toujours à l'heure actuelle. Je parle, bien sûr, de ces enquêtes, M. le Président. Nous croyons toutefois qu'il est pertinent de rencontrer les acteurs que nous avons convoqués aujourd'hui pour qu'ils nous expliquent ce qui s'est passé, les mesures en réaction à la fuite de données, mais aussi pour nous orienter sur l'encadrement gouvernemental qui pourrait contribuer à la meilleure protection des données financières des Québécois.

Encore une fois, l'ampleur des événements nous force à faire preuve d'écoute et de rigueur par respect pour tous ceux qui ont été touchés par la fuite de données. On parle de 4,2 millions de Québécois qui ont des inquiétudes légitimes et qui veulent avoir des réponses, et surtout un peu de paix d'esprit. Notre devoir de parlementaires est de représenter les

intérêts de la population québécoise à l'Assemblée nationale, et c'est ce que nous allons faire aujourd'hui en recevant Desjardins, Equifax et tous les autres groupes qui se joindront à nous tout au long de la journée. Merci, M. le Président. • *(11 h 50)* •

Le Président (M. Simard) : Merci à vous, M. le député de Saint-Jérôme. Je cède maintenant la parole au député de Vachon.

M. Ian Lafrenière

M. Lafrenière : Merci beaucoup, M. le Président. Alors, salutations aux collègues qui sont aujourd'hui présents. Je ne referai pas la genèse de tout ce qui s'est passé en cette commission pour arriver ici aujourd'hui, mais malheureusement c'est un constat qui est triste, qu'on arrive à cette façon-là de procéder, parce qu'au final ce que les citoyens veulent entendre, c'est qu'est-ce qui s'est passé. Ils veulent entendre Desjardins. Oui, il est vrai, M. le Président, que, dans le passé, on a entendu Desjardins s'exprimer, que ce soit dans les médias ou même au niveau du fédéral, mais il y a des questions que les... et je suis persuadé que mes collègues ici ont entendu beaucoup de questions des citoyens qui les ont interpelés dans leur comté, que ce soit ici...

Et aujourd'hui on va écouter Desjardins, on va interroger. Il va y avoir Equifax, l'OPC, l'association des banques canadiennes, l'AMF et José Fernandez. La SQ avait été invitée au tout début, et, étant donné que l'enquête est toujours active, ils ont décliné l'invitation, et ça, mon collègue l'a dit tout à l'heure, on en est très conscients.

Aujourd'hui, M. le Président, ce qu'on veut, c'est trouver des réponses pour les citoyens. Et je dois vous avouer que moi-même, j'ai reçu une lettre de Desjardins quand tout ça a commencé, et ça m'a insécurisé. Ça m'a insécurisé sur le coup, mais ça m'a insécurisé sur le futur, en disant : Quand est-ce que ça va arriver? Quelle journée il va y arriver quelque chose?

Et un des enjeux qu'on va devoir adresser aujourd'hui, c'est le vol d'identité aussi, vol d'identité qui a de grandes conséquences pour les citoyens. Lorsqu'on se fait voler son identité, lorsque des gens font des emprunts, font des transactions en notre nom, il y a de lourdes conséquences. Lors du débat, la semaine passée, j'en ai parlé amplement. Aujourd'hui, on a entendu une victime, Mme Aubry, qui est venue en parler, et ce sont des conséquences réelles. Je l'ai vu moi-même sur le terrain. C'est des gens qui sont dévastés, et ça reste. C'est extrêmement difficile de s'en sortir.

Alors, je pense que, comme parlementaires, aujourd'hui, on a un travail important. Le travail important qu'on a, c'est de poser les questions au nom de nos citoyens. Moi, je tends la main à mes collègues des oppositions en disant : Travaillons ensemble, posons les bonnes questions au nom de nos citoyens.

Et je veux aussi rassurer les gens qui nous écoutent en disant : C'est le début, ce n'est pas la fin. Alors, oui, aujourd'hui, il y a une journée où on va pouvoir poser des questions. Mais, parallèlement à ça, notre gouvernement est déjà dans l'action, et il y aura des projets de loi qui vont être déposés incessamment. Et, comme vous le savez, M. le Président, lorsqu'il y a un dépôt de projet de loi, il y a une possibilité de convoquer des groupes pour les entendre, et ça sera fait aussi.

Alors, trois projets de loi distincts, autant d'occasions d'entendre des gens. Alors, je veux rassurer les oppositions en disant : Aujourd'hui, oui, on entend six groupes, mais, dans le futur, il y en aura d'autres. Travaillons ensemble pour le bien-être des gens qui nous écoutent. Merci, M. le Président.

Le Président (M. Simard) : Merci à vous, M. le député de Vachon. Je cède maintenant la parole au député de Robert-Baldwin et porte-parole de l'opposition officielle. Cher collègue.

M. Carlos J. Leitão

M. Leitão : Très bien. Merci beaucoup, M. le Président. Alors, nous aussi, nous allons participer activement à cette commission. Nous allons faire notre travail. Je dois quand même nous rappeler à nous tous que nous sommes ici dans un exercice qui nous a été imposé par le leader du gouvernement, un exercice imposé et qui est beaucoup plus restreint que ce que nous aurions souhaité faire.

Permettez-moi, M. le Président, parce que c'est important, de rappeler un peu la chronologie des événements. Le 20 juin 2019, Desjardins a annoncé publiquement la fuite de données. Le 21 juin, le collègue député de Laurier-Dorion avait demandé une séance de... un mandat d'initiative dans une autre commission parlementaire. Le 9 juillet, M. le Président, le député de René-Lévesque avait adressé une demande de mandat d'initiative à la Commission des finances publiques. Le 9 juillet. Le 28 août, nous avons eu finalement une séance de travail d'à peine 30 minutes, où on n'a pas réussi à s'entendre. Le 3 septembre, on a finalement eu une séance qui a duré un peu plus de temps.

Et finalement on a procédé au vote. On avait une liste d'une douzaine de groupes. On n'a pas été capable de faire approuver cette liste, et donc la motion a été rejetée, M. le Président. Donc, si nous nous trouvons ici aujourd'hui, c'est en conséquence de cela. Le 1er novembre, on apprend que ce sont tous les membres de Desjardins qui ont été touchés par cette fuite. Et, ce jour-là aussi, moi, j'avais déposé, ainsi que le député de René-Lévesque, une autre demande de mandat d'initiative. Et c'est à ce moment-là que le gouvernement a court-circuité les procédures, ce qu'il peut faire avec l'article 146, en imposant cette commission avec un nombre très restreint de participants.

Nous voulons entendre Desjardins, et c'est très bien, on va poser des questions, ainsi qu'Equifax, AMF et les autres. Mais, comme le député de Vachon a mentionné, on parle ici de la protection des données personnelles, le vol d'identité. Ça demande une commission parlementaire beaucoup plus large que cela, et nous souhaitons que cela se fasse. Ça aurait pu être fait sur deux ou trois jours. Ça n'aurait pas entravé les travaux parlementaires.

Donc, nous allons participer à cette session, très bien. Comme le député de Vachon a mentionné, c'est le début et pas la fin. Mais nous souhaitons que la continuation se fasse ici, dans cette Assemblée, dans cette commission, qu'on puisse entendre tous les experts. L'enjeu va bien au-delà de Desjardins. L'enjeu concerne la protection des données privées de tous les Québécois dans des organismes privés et publics. Il faut faire la lumière sur tous ces enjeux-là. Merci, M. le Président.

Le Président (M. Simard) : Merci à vous, M. le député de Robert-Baldwin. M. le député de Rosemont, vous avez exactement 2 min 40 s.

Une voix : ...

Le Président (M. Simard) : Bien oui, une minute, cher collègue. Je m'excuse. Ce sera plus tard que vous aurez 2 min 40 s. Désolé.

M. Vincent Marissal

M. Marissal : O.K. Merci. Bien, bienvenue, chers collègues. Finalement, je dirais, tout ça pour ça. Je veux rassurer le député de Vachon. On est ici pour les mêmes raisons. On n'a juste pas pris le même chemin pour se rendre, et c'est malheureux. Je veux remercier le député de Robert-Baldwin d'avoir fait un excellent exposé, parce que je n'aurai pas le temps de le faire en une minute.

C'est quand même ironique, tant d'efforts si longtemps pour arriver ici avec si peu de temps dans un dossier aussi important. Il paraît qu'on vit de petites victoires dans l'opposition, mais, si tant est que celle-ci est une victoire, elle a un goût franchement amer. On n'a pas aimé, personne, en tout cas, de ce côté-ci de la table, je pense que je parle au nom de mes collègues, la façon dont ça s'est fait. On a l'impression désagréable de s'être fait rentrer ça dans la gorge un peu de force. Et d'entendre ce qui a été dit en plus tôt ce matin au salon bleu, franchement, c'est ajouter l'insulte à l'injure. Visiblement, certains collègues du gouvernement n'ont pas la même mémoire que nous de la façon dont ça s'est passé.

Cela dit, on est contents. Puis on est contents que Desjardins puisse finalement témoigner et on va faire ça avec professionnalisme et rigueur. Merci, M. le Président.

Le Président (M. Simard) : Merci, cher collègue. M. le député de Jonquière.

M. Sylvain Gaudreault

M. Gaudreault : Oui, merci, M. le Président. Comme 4,2 millions de membres de Desjardins, je suis également touché par cette fuite de données personnelles extrêmement préoccupante. Nous avons demandé, le 9 juillet dernier, cette commission. Alors, aujourd'hui, on se retrouve avec un sentiment de trop peu, trop tard. Mais on va le faire quand même avec toute l'énergie que vous nous connaissez et toute la rigueur que vous nous connaissez également pour comprendre ce qui s'est passé et porter un jugement, mais surtout essayer de trouver des solutions.

Parmi les solutions qu'on cherchera à trouver, moi, je veux surtout comprendre les limites réelles du droit québécois versus les compétences fédérales en protection des données personnelles. Alors, là-dessus, je pense qu'on a un chantier à examiner de façon très, très serrée... et de bien comprendre ce qui s'est passé.

Par ailleurs, bien, j'ai hâte d'entendre également les explications de Desjardins, d'Equifax, de l'Autorité des marchés financiers, de l'Office de la protection du consommateur, les banquiers, également, et les experts, que nous aurions préféré pouvoir contre-vérifier, l'expert qu'on va recevoir, avec d'autres types d'experts dans le domaine. Merci.

Auditions

Le Président (M. Simard) : Merci à vous, cher collègue. Alors, nous procédons maintenant à la seconde étape de ces auditions en débutant, donc, nos échanges et nos présentations. Alors, M. Cormier, bienvenue parmi nous. Auriez-vous d'abord, pour les fins de nos travaux, l'amabilité de vous présenter ainsi que de présenter les personnes qui vous accompagnent?

Mouvement Desjardins

M. Cormier (Guy) : Alors, Guy Cormier, président et chef de la direction du Mouvement Desjardins. Bonjour, tout le monde. À ma droite, Isabelle Garon, qui est vice-présidente, Bureau du président, Coopération et Soutien aux administrateurs, à ma gauche, Denis Berthiaume, qui est premier vice-président exécutif et chef de l'exploitation du Mouvement Desjardins, et, à sa gauche, M. Yvan-Pierre Grimard, qui est vice-président, Affaires institutionnelles et gouvernementales, au Mouvement Desjardins.

• *(12 heures)* •

Le Président (M. Simard) : Nous vous écoutons, et vous disposez d'une période de 10 minutes.

M. Cormier (Guy) : Bien, alors, écoutez, merci beaucoup, M. le Président de la Commission des finances publiques. Mesdames messieurs, membres de la commission, bonjour à toutes et à tous.

Desjardins comprend très bien la préoccupation des Québécois concernant le vol de données et de renseignements personnels qui est survenu chez nous. On entend participer très activement à la mise en place de solutions visant une

meilleure protection des renseignements personnels et la mise en place d'une véritable identité numérique. Je tiens à vous rassurer d'entrée de jeu que vous avez notre plus entière collaboration aujourd'hui.

Le 1er novembre dernier, 24 heures après un appel de la Sûreté du Québec, j'ai informé nos membres publiquement que l'enquête policière tendait à démontrer que l'ensemble des membres particuliers de Desjardins étaient touchés par la fuite de renseignements. Je rappelle, là, ici, là, qu'il ne s'agit pas d'un nouveau délit. C'est toujours la même enquête sur le même délit commis à l'interne par le même employé malveillant qui a agi seul.

Depuis juillet, tous les membres chez Desjardins bénéficient dorénavant d'une protection, la Protection membres Desjardins, une protection automatique et permanente en cas de fraude et de vol d'identité, une protection qui est unique au Canada. Ce même jour, le 1er novembre, on avait prévu prononcer, puis on l'a quand même annoncé, là, l'extension de ce programme de protection. Ce sera tous nos membres chez Desjardins qui vont dorénavant bénéficier, sans frais, d'un service de surveillance de crédit d'Equifax. Ils vont recevoir, au cours des prochaines semaines, un code d'activation. Ils pourront s'inscrire directement à Equifax.

Depuis juin, chez Desjardins, on a travaillé d'arrache-pied. On a congédié l'employé fautif. On a développé des nouvelles protections sans égal au Canada. Et, dans un temps record, on a mobilisé l'organisation, traité jusqu'à 125 000 appels par jour. Et aujourd'hui c'est plus de 41 % des membres, là, qui se sont inscrits sur Equifax, ce qui constitue un résultat sans précédent à travers le monde. On a posé des questions à l'interne. On en pose encore. Et on a continué à faire évoluer nos procédures. On a agi en tout temps dans l'intérêt de nos membres.

Desjardins, c'est la plus grande institution financière du Québec et le premier groupe coopératif financier en Amérique du Nord. C'est 312 milliards d'actifs, 23 milliards de capitalisation, 45 000 employés et près de 120 ans de partenariat avec les Québécois. Desjardins a été classé par Bloomberg parmi les institutions financières les plus solides à travers le monde. Desjardins est reconnu par les conventions internationales comme une institution financière d'importance systémique. On est encadrés par l'Autorité des marchés financiers du Québec, qui applique à Desjardins les mêmes exigences que le Bureau du Surintendant des institutions financières applique aux banques canadiennes. On est soumis aux mêmes agréments internationaux de conformité que les banques. On est évalués par les mêmes agences de notation. On est soumis aux mêmes règles d'audit trimestriel.

À chaque année, le Mouvement Desjardins investit 70 millions de dollars en sécurité informatique et en cybersécurité. Nos processus sont constamment en évolution. Et, je le rappelle, là, dans l'affaire qui nous préoccupe, là, nos systèmes n'ont jamais, jamais été compromis. La fraude interne, c'est la bête noire de toute organisation, comme c'est arrivé chez Marriott, comme c'est arrivé chez Disney, comme c'est arrivé chez Sephora, comme c'est arrivé à Revenu Québec, et même dans le dossier de santé Québec.

Au début du mois, le commissaire à la vie privée du Canada a révélé que 28 millions de Canadiens, 28 millions de Canadiens, avaient été touchés par des fuites de données dans la dernière année, découlant de 680 déclarations volontaires. 28 millions en un an. Si on enlève à peu près les 4 millions de Desjardins puis les 6 millions de Capital One, là, il reste 18 millions de Canadiens dont les données ont été volées. C'est qui, les autres organisations? C'est qui qui a agi avec autant de transparence et le même sens du devoir que Desjardins a démontré dans les derniers mois? J'ai fait cinq conférences de presse. J'ai accordé des dizaines d'entrevues. Puis j'en suis à ma deuxième commission parlementaire. Et loin de moi, ici, là, l'idée de jeter la pierre à d'autres entreprises qui ont été victimes de fraude interne, mais, au contraire, ce que ça démontre, c'est qu'il faut se retrousser les manches, actuellement, là, pour chercher des solutions ensemble.

Ce qui s'est produit chez Desjardins, c'est très sérieux, et on a agi en conséquence. Mais, si on veut rendre réellement justice aux membres de Desjardins, là, et, plus largement, aux citoyens du Québec et du Canada, on doit élargir notre regard tous ensemble parce qu'il y a eu de nombreux cas avant Desjardins, il y a eu des cas depuis le 20 juin puis il va continuer malheureusement d'avoir des cas dans le futur encore. Le vol de données, c'est un fléau mondial.

Chaque année, la multinationale québécoise CGI discute avec 5 500 de ses clients à travers le monde. En 2019, au cours de ses échanges, 20 % de ses clients ont indiqué n'avoir aucun plan pour améliorer la sécurité des données personnelles qu'ils gèrent et un autre 20 % a indiqué qu'elles souhaitaient investir dans ce domaine, mais ne savaient tout simplement pas avec quelles balises elles devaient le faire. La conclusion de ces échanges, c'est qu'à part les pays de l'Union européenne la grande majorité des pays de l'OCDE tarde trop à réagir à cet enjeu, la protection des renseignements personnels.

Le retentissement de ce qui est arrivé chez Desjardins, là, c'est un éveil brutal qu'on ne doit certainement pas gaspiller. Je nous enjoins tous à voir au-delà de la situation de Desjardins puis à se poser les vraies questions. Et, chez Desjardins, on a formé un groupe de travail à l'interne auquel j'ai donné un mandat très clair pour nos membres et les consommateurs : Constituez un guide des meilleures pratiques à des fins de sensibilisation et d'éducation. Les meilleurs systèmes vont toujours nécessiter la vigilance des consommateurs.

Pour les entreprises, constituer un guide de sensibilisation et de prévention de la fraude — on a, chez Desjardins, 360 000 entreprises qui font affaire avec nous et qui gèrent chacune des données sur leurs clients — puis, pour les gouvernements et les institutions, rassembler des informations et ouvrir un réel dialogue sur la notion d'identité numérique... Nous rendrons, d'ailleurs, public, disponible à tous, un rapport sur nos travaux au premier trimestre de 2020.

Et, dans le cadre de ce troisième volet là, sur le volet gouvernemental et institutionnel, là, sur l'identité numérique, j'ai rencontré, la semaine dernière, Joni Brennan, qui est la présidente du DIACC, Digital Identity & Authentification Council of Canada. Desjardins est membre fondateur de ce conseil, qui est destiné à la promotion et à la préparation d'un système canadien d'identité numérique et qui participe à des discussions au niveau international.

Et, ce matin, je suis heureux de vous annoncer devant la commission que Desjardins sera et est l'instigateur de la mise sur pied d'une nouvelle branche francophone du DIACC ici, au Québec, que l'on va dorénavant appeler le forum de l'identité numérique. Depuis le 20 juin, il y a plusieurs organisations au Québec qui ont manifesté leur volonté de travailler avec Desjardins pour chercher des solutions. Ce forum, il est ouvert à toutes les parties prenantes et transcende toute

forme de concurrence ou de corporatisme dans la société. L'enjeu, il est stratégique, il est économique puis il est social. Avec ce forum, ce qu'on veut essentiellement, c'est coaliser les acteurs, documenter ce qu'il se fait ailleurs à travers le monde, identifier des pistes de solutions qui seraient adaptées à la réalité québécoise puis aider le gouvernement dans ses prises de décision. Et j'invite, d'ailleurs, le gouvernement du Québec à se joindre à ce forum.

On est à l'ère du numérique. Les données sont désormais considérées comme des ressources dans la société. Elles sont à la base de toutes les innovations technologiques que l'on connaît. Il ne s'agit pas d'arrêter ce mouvement-là actuellement, là, mais il faut l'encadrer de la bonne façon. Actuellement, on s'enregistre sur différents réseaux avec des documents gouvernementaux qui ont été conçus pour d'autres fins à une autre époque. On a construit, là, autour de ça, depuis les dernières années, là, un paquet de parapluies informatiques pour protéger ça, mais ce n'est pas optimal.

Actuellement, les consommateurs, les citoyens sèment leurs données personnelles un peu partout au gouvernement, dans plusieurs ministères, chez leur employeur, à la caisse, à la banque, dans les municipalités, chez leur fournisseur Internet, chez Hydro-Québec et dans de nombreux, nombreux commerces. On multiplie les expositions. On multiplie les risques. Il faut redonner à chaque personne le contrôle de ses données. Il faut redonner du sens. Il faut construire une véritable identité numérique au Québec et au Canada.

Le gouvernement a annoncé son intention de légiférer. La législation fait évidemment partie de la solution, mais avec doigté. On ne peut pas cadenasser les données. Il faut réunir confidentialité, sécurité et fluidité. Il faut tirer les bonnes leçons de ce qui s'est passé chez Desjardins et ailleurs et travailler ensemble dans l'intérêt des citoyens et dans l'intérêt de notre économie.

Merci beaucoup. On est prêts à répondre à vos questions.

Le Président (M. Simard) : Très bien. Merci, M. Cormier. Alors, merci pour cet exposé. Avant de céder la parole à mes collègues, simplement vous rappeler que plusieurs d'entre eux veulent s'adresser à vous, et, afin de maximiser notre temps, je nous invite à des réponses à la fois complètes, mais néanmoins synthétiques. Ceci étant dit, M. le député de Saint-Jérôme, à vous la parole.

M. Chassin : Merci, M. le Président. Merci, M. Cormier, pour cette présentation. Bienvenue.

Vous êtes une institution d'une importance capitale dans l'économie québécoise. Je dirais même que Desjardins habite en partie l'imaginaire des Québécois, ce qui explique sans doute le retentissement du vol de données qu'on a connu. Bon, évidemment, la fuite de données chez Desjardins, vous en avez été victime. Il y a 4,2 millions de Québécois qui en ont été victimes. Ça soulève de nombreuses questions. Je vais en poser, certains de mes collègues aussi. Je vous prierais de garder vos réponses assez courtes et concises, autant que faire se peut.

J'aimerais comprendre un élément. Évidemment, vous en parliez dans votre présentation, c'est un employé mal intentionné qui, chez vous, a mis la main sur ces données. Est-ce que vous pouvez nous donner un sens des catégories de travailleurs, d'employés de Desjardins qui ont accès à ces données, sachant que... J'imagine que, par exemple, un directeur a accès à ces données-là. Quelqu'un qui fait de l'entretien au sein d'une caisse populaire n'a pas accès. Entre les deux, quelle serait la proportion des catégories d'emploi qui ont accès aux données?

M. Cormier (Guy) : Bien, essentiellement... Je vais y aller rapidement. Denis, tu auras peut-être des questions d'exploitation.

Mais essentiellement, sur 45 000 employés, il y a des employés qui ont accès à des données, là. Vous pensez à votre caissière dans votre caisse, là, elle regarde son écran, elle a de l'information sur vous, là. Le planificateur financier, il a de l'information sur vous. Le directeur de comptes aux entreprises, il a de l'information sur votre entreprise. Alors, c'est balisé, c'est encadré. Il n'y a personne chez Desjardins qui ouvre son ordinateur, là, puis qui a accès à toutes les données de tous les membres, tous les clients, le matin, instantanément, sur son système, là. Il y a d'importantes mesures de sécurité qui sont mises de l'avant.

Mais, une fois que j'ai dit ça, il y a quelques employés, quelques dizaines d'employés, qui ont accès à beaucoup plus d'informations pour différentes raisons. Pensez à tout ce qui touche la lutte au blanchiment d'argent. La lutte au blanchiment d'argent, on a des obligations légales et réglementaires de transmettre de l'information. On peut penser à la sécurité. On peut penser au marketing. Et, à ce moment-là, il y a des mesures qui encadrent le nombre de données que les gens ont accès.
• *(12 h 10)* •

M. Chassin : Est-ce que vous pourriez nous donner une proportion approximative?

M. Cormier (Guy) : Sur 45 000 employés, là, on parle de quoi, Denis, quelques dizaines?

M. Berthiaume (Denis) : Quelques centaines, là.

M. Cormier (Guy) : Quelques centaines d'employés sur 45 000 employés qui ont accès à un peu plus d'informations.

M. Chassin : Et donc c'est là où il y a des contrôles de sécurité plus serrés, j'imagine, compte tenu de cet accès-là?

M. Cormier (Guy) : Il y a des contrôles de sécurité partout. Il y a des contrôles de sécurité face à nos caissières. Il y a des contrôles de sécurité face à nos planificateurs financiers. Il y a des contrôles de sécurité par rapport à tous nos employés. Et, en fonction du type d'information qu'ils peuvent avoir accès, bien, les contrôles de sécurité sont modulés en conséquence. Mais tout le monde a des contrôles de sécurité.

M. Chassin : Et donc vous avez rajouté des contrôles de sécurité aussi par la suite. Dans l'état actuel des choses, est-ce que... par exemple, des contrôles de sécurité même avant l'embauche?

M. Cormier (Guy) : Denis, peut-être, tu peux y aller là-dessus.

M. Berthiaume (Denis) : ...peut-être compléter. Écoutez, un, première des choses, il y a tout un système de gestion des accès et des identités qui sont présents. Alors, il y a un principe de base : à 45 000 employés, les employés ont accès au système strictement de ce qui est requis dans le cadre de leur travail. Donc, ça, ça existe. Évidemment, après ça...

M. Chassin : Mais, avant l'embauche, est-ce que...

M. Berthiaume (Denis) : Avant l'embauche, il y a des enquêtes de sécurité qui sont menées.

M. Chassin : D'accord.

M. Berthiaume (Denis) : Puis, pour ce qu'on appelle des comptes à hauts privilèges, c'est poussé encore plus loin, donc c'est avant l'embauche. Et il y a également des mesures additionnelles.

M. Chassin : Merci. Il y a, donc, des données qui ont été volées, qui, évidemment, contiennent un certain nombre d'éléments qui sont bons longtemps, que ce soit la date de naissance ou le numéro d'assurance sociale. Est-ce que vous pourriez nous donner un sens de combien de temps ces données pourraient être éventuellement utilisées contre le détenteur des données?

M. Cormier (Guy) : Bien, écoutez... Denis, tu veux-tu y aller? Je pourrai compléter.

M. Berthiaume (Denis) : Mais je peux y aller, puis vous pourrez compléter, M. le Président.

Un élément qui est important, évidemment, la durée de vie des données. Il y a des données, effectivement, qui ne bougent pas, qui ne sont pas mobiles, mais, strictement avec un numéro d'assurance sociale et avec une date de naissance, bien, oui, ce qu'on peut observer, c'est que les gens peuvent se servir de ça. Effectivement, quand c'est rendu à l'extérieur, c'est rendu à l'extérieur. Toutefois, il y a une durée de vie à certaines données. Donc, pour fins d'authentification, les mécanismes d'authentification sont beaucoup plus larges que strictement demander une date de naissance et un numéro d'assurance sociale. Alors, par d'autres mécanismes d'authentification, questions de sécurité ou différents modes de fonctionnement au niveau de la sécurité, eh bien, on vise, dans le fond, à périmer, en quelque part, ces données-là dans tout le processus d'authentification de nos membres.

M. Chassin : D'accord.

M. Cormier (Guy) : Et, très rapidement, c'est pour ça qu'on a lancé la Protection membres Desjardins. Le 15 juillet, quand on a lancé la Protection membres Desjardins, c'est, justement, pour protéger ce type de risque là. Aujourd'hui, tous les membres chez Desjardins bénéficient de cette protection-là. Dans un an, dans deux ans, dans 10 ans, dans 50 ans, dans 75 ans, tant qu'ils sont membres chez Desjardins, ils ont accès à... S'il y a une transaction frauduleuse dans leur compte — ou non autorisée — on les rembourse. S'ils ont malheureusement un réel vol d'identité, ils appellent chez Desjardins. Gratuitement, on a des spécialistes, avocats, spécialistes, psychologues, s'il le faut, qui peuvent les accompagner. Puis, troisièmement, s'ils ont des dépenses personnelles, on rembourse jusqu'à 50 000 $. C'est pour gérer ce risque-là qu'on a mis cette protection-là.

M. Chassin : Question : Est-ce que vous avez eu, avant les faits, des indications à l'interne qu'il y aurait des risques de sécurité sur les données personnelles?

M. Cormier (Guy) : Bien, essentiellement, là, régulièrement, à chaque année, on investit 70 millions de dollars par année. On investit 70 millions de dollars par année dans nos différentes mesures de sécurité. Et on a un plan annuel dans lequel on décide parfois : O.K., on alloue notre argent où?

M. Chassin : Vous êtes conscients des failles possibles.

M. Cormier (Guy) : La fraude interne, les attaques externes, les demandes de rançon, la cybersécurité. On parle avec des spécialistes universitaires. On parle avec des spécialistes internationaux. On se fait accompagner par des firmes externes. On parle aux autres institutions financières. On parle à l'environnement pour voir qu'est-ce qui se passe, actuellement, dans le marché et on investit.

Alors, parfois, effectivement, les gens disent : Ah! attention, de ce temps-ci, il y a beaucoup d'hameçonnage par rapport à tel nouveau type de fraude. O.K., on ajuste nos mesures de... procédures de sécurité. C'est un jeu de chat et souris, ça, là. Aujourd'hui, pendant que je vous parle, là, il y a probablement des gens qui écoutent ce que je vais dire pour essayer d'attaquer Desjardins et d'autres institutions financières prochainement.

M. Chassin : Et on ne voudrait pas ça.

M. Cormier (Guy) : Alors, c'est ça, la réalité.

M. Chassin : Merci, M. Cormier. Mes collègues vont continuer.

Le Président (M. Simard) : Tout à fait. Merci à vous, M. le député de Saint-Jérôme. Mme la députée de Charlevoix—Côte-de-Beaupré.

Mme Foster : Bonjour. Merci beaucoup d'être ici aujourd'hui.

Je commencerais par une mise en situation. On va prendre un cas fictif, Louise. Louise fait partie des 4,2 millions d'abonnés chez vous qui ont été victimes de vol de données. En juin dernier, elle ouvre le bulletin de nouvelles, elle apprend qu'il y a eu une fuite massive de données chez Desjardins. Elle s'inquiète. Elle se demande si elle va recevoir la lettre, si elle fera partie des clients touchés. Finalement, quelques semaines plus tard, elle reçoit la lettre. Elle fait partie des clients qui sont touchés dans la première vague.

Dans la lettre, on lui dit essentiellement : Voici, si vous voulez une surveillance de crédit, vous devez vous inscrire à Equifax. Elle appelle chez Equifax, c'est long, c'est long. Elle appelle deux fois, trois fois, parce qu'il y a une heure d'attente à chaque fois, puis elle travaille comme tout le monde. Donc, à un moment donné, elle ne peut pas juste faire ça dans sa vie. Par la suite, elle finit par rejoindre Equifax, a sa surveillance de crédit, mais, au final, elle se dit : C'est lourd, c'est lourd. Est-ce que je reste membre chez Desjardins? Ça, c'est la première question. Elle décide de rester membre, mais elle se pose des questions, sans compter le fait qu'on lui répond en anglais chez Equifax. Ça, c'est une autre chose.

Suite à ça, moi, j'ai quelques questions. Je vais vous les poser en rafale à partir de cette mise en situation là, parce que vous comprenez que, du point de vue du citoyen, je vais essayer de vous les poser, les questions, mais du point de vue du citoyen, tel qu'ils ont vécu la situation. Je vais poser les quelques questions en rafale, mais je vous demanderais d'attendre à la fin. Peut-être les prendre en note puis me les répondre en rafale également. Ce serait apprécié.

Premièrement, l'erreur ne vient pas du citoyen, elle vient d'un employé chez Desjardins, tout ça, mais ultimement la responsabilité est quand même sur Desjardins, du vol de données. Alors, pourquoi mettre le singe sur l'épaule du consommateur en ce qui concerne le service de la surveillance du crédit? C'est long, c'est fastidieux. Ça a connu des ratés, ça a été compliqué. Pourquoi mettre le singe sur le dos du client? Il y en a 4,2 millions comme ça.

Également, est-ce que vous vous êtes assurés avec Equifax, avant d'accorder ce contrat-là de protection, de surveillance, qu'ils avaient les capacités pour faire face à cette surveillance? Parce que, je comprends, les choses se sont faites vite, mais le service en français a connu des ratés et le système informatique également. La capacité était, bon, plus ou moins suffisante pour répondre à la demande dans les premiers mois.

Également, pour ceux qui ne seront pas capables de s'inscrire au service avant le 1er janvier 2020, parce que la première vague, là, on nous dit... Moi-même, j'ai reçu cette lettre-là. Je faisais partie de la première vague. On nous dit : À partir du 1er janvier 2020, bien, si vous ne vous êtes pas inscrit, c'est comme un vide. Qu'est-ce qu'il arrive? Parce qu'ultimement, je le rappelle, ce n'est pas la faute du client, ce qui est arrivé.

Également, Equifax elle-même a été victime d'une fuite de données massive en 2017. Donc, quelle est la limite de votre responsabilité sur les données de vos membres que vous avez référés à Equifax si une fuite du genre se reproduit chez eux?

Finalement, je fais référence à quelque chose que vous avez dit tout à l'heure et que vous avez dit également lorsque vous êtes allé au Parlement fédéral devant une commission. Vous avez mentionné que la Protection membres Desjardins, qui couvre la protection des actifs, d'accompagnement en cas d'utilisation frauduleuse des renseignements personnels et de remboursement de frais pour des démarches de restauration d'identité... Donc là, on est hors de la surveillance de crédit, on est dans l'autre protection que vous offrez. Vous dites — j'ai accroché un peu : C'est permanent tant qu'on reste client chez vous. Donc, qu'est-ce qu'il arrive si quelqu'un, suite à tout ça, décide : Moi, je ne veux plus de compte chez Desjardins? Est-ce que cette protection-là est permanente? Mais est-ce qu'elle l'est vraiment? Parce que vous avez encore mentionné tout à l'heure : Tant que la personne demeure membre chez nous... Alors, voilà. Merci.

M. Cormier (Guy) : Écoutez, quelques éléments de réponse.

Premièrement, moi, là, avant le 20 juin, là, il arrive une fuite de renseignements, là, il y a deux entreprises au Canada qui offrent ce service-là, deux, pas trois, pas quatre, pas cinq, pas 10, deux : Equifax, 70 % de part de marché, et TransUnion, 30 %. Alors là, l'eau rentre dans le sous-sol, là, puis il y a deux camions qui passent sur la rue, là, pas deux, pas trois, pas quatre, cinq, deux camions. Je peux attendre des semaines et des semaines ou je dis : Je travaille avec Equifax. On s'est assis avec Equifax. On a pris le temps de regarder, dans un court délai, quelles étaient les protections. C'est une firme internationale qui a fait ça à plein d'autres endroits.

Alors, on a fait les vérifications, puis ils nous ont dit : Oui, on est en mesure d'accompagner adéquatement. Puis, en moyenne, c'est 5 % à 10 % des gens qui sont victimes d'une fuite qui s'inscrivent. Là, on leur a dit : O.K., parfait, mais, si c'est plus, êtes-vous capable d'accompagner tout ça? Oui, on va travailler avec eux comme tels. Évidemment, au début, là, il y a eu des enjeux que vous avez mentionnés. Mais rapidement Equifax s'est assis avec nous, puis on a cherché des solutions. Puis Equifax, je dois dire, a fait preuve d'ouverture. Ils ont augmenté leur capacité de leur site Internet. Ils ont augmenté leurs ressources en français. Là, on le voit depuis le 1er novembre, la qualité de la prise en charge est très différente comme telle.

Mais, je le répète, et ça, je pense que c'est un élément que les gouvernements devraient regarder, il y a deux firmes de bureau de crédit au Canada, deux. Alors, à un moment donné, les institutions financières travaillent avec les entreprises avec lesquelles elles ont le droit de travailler au Canada. Ça, c'est la première chose.

La deuxième chose, c'est probablement tout ce qui touche au niveau de... pas capable de s'inscrire d'août à décembre par rapport à la... chez Desjardins. Bien, c'est qu'on laisse cinq à six mois, puis les gens nous disent, chez Equifax, même chez TransUnion, que, généralement, les gens qui veulent s'inscrire, bien, s'inscrivent au début. Après quatre, cinq, six mois, bien, déjà, s'il reste 60 %, 65 % des gens qui ne sont pas activés, s'ils ne l'ont pas activé en juillet, en août, en septembre, en octobre, en novembre, bien, pourquoi après cinq, six mois, là, quand tous les médias en ont parlé? Alors, les gens nous disent : C'est rarement tout le monde qui s'inscrit au service de protection.

Pourquoi on a lancé la Protection membres Desjardins? C'est parce qu'effectivement on voyait que ce n'étaient pas tous les membres chez Desjardins qui s'inscrivaient puis on se disait : Qu'est-ce qu'on fait s'il y en a juste 10 %, 20 %, 30 % puis que les autres ne le sont pas? Quelle est notre responsabilité, comme entreprise, comme coopérative? Et c'est là qu'on s'est dit : Il faut lancer une protection additionnelle. On a lancé la Protection membres Desjardins, c'est vrai, exclusivement pour nos membres. Il faut être membre de la coopérative parce que quelqu'un qui décide de quitter sa coopérative, bien, pourquoi les autres membres devraient soutenir cette protection-là pour 20, 30, 40 ans quand eux ont décidé de prendre la décision de rester dans la coopérative, alors que les autres ont décidé de quitter? La protection, elle est permanente tant que vous êtes membre de la coop. C'est un peu le sens de ce qu'on a voulu amener.

• *(12 h 20)* •

Mme Foster : ...reste encore un peu de temps?

Le Président (M. Simard) : Oui, oui, oui. Il vous reste 2 min 50 s.

Mme Foster : On parle quand même d'une situation exceptionnelle. De dire que la personne qui décide de ne plus être membre chez vous perd cette protection-là quand l'erreur qui a été commise au départ ne le concerne pas, mais concerne Desjardins, c'est un peu particulier.

M. Cormier (Guy) : La dame ou l'homme qui a ça peut quitter Desjardins, et on va quand même lui offrir une protection de cinq ans avec Equifax, payée par Desjardins. Alors, même si elle a quitté Desjardins, là, depuis le mois d'août ou septembre, Desjardins continue de lui payer une protection Equifax pour les cinq prochaines années en cas de vol d'identité. Moi, je pense qu'on prend nos responsabilités, là.

Le Président (M. Simard) : Je sais que le député de Vachon souhaitait également intervenir. Cher collègue, à vous la parole. Il vous reste 2 min 11 s.

M. Lafrenière : Merci beaucoup. Merci pour la présentation. Je ne me trompe pas en disant que vous êtes dans un système coopératif. Donc, il y a plusieurs caisses. Il y a combien de caisses au total?

M. Cormier (Guy) : Aujourd'hui, on est à 212 caisses.

M. Lafrenière : 212 caisses. Est-ce que je me trompe aussi en disant que chacune de ces caisses-là a une banque de données, c'est-à-dire, quand moi, je me présente pour ouvrir un compte, la caisse où je me présente à une base de données avec mes informations?

M. Cormier (Guy) : Je pense, c'est centralisé. Denis?

M. Berthiaume (Denis) : C'est un système central. C'est des accès qui sont donnés aux caisses, caisse par caisse, mais c'est un système central. On fonctionne avec des systèmes centraux.

M. Lafrenière : Donc, il y a un système central, mais, dans la caisse, il n'y a aucune copie de mes informations personnelles qui se retrouvent là.

M. Cormier (Guy) : Ah! bien non, c'est sûr qu'il y a des données. Il y a des données papier, là. Il y a des demandes de crédit. Il y a des cartes de signature. Il y a ces éléments-là.

M. Lafrenière : Ma prochaine question... Puis vous l'avez dit, hein, quand vous vous êtes présentés au fédéral, vous avez dit que c'est un problème qui était majeur, là, la petite bête noire avec nos fraudeurs internes. Je suis d'accord avec vous. Je veux savoir quelle journalisation vous faites pour les interrogations qui se font de vos employés dans les systèmes, à savoir moi, j'ai eu accès aux dossiers de tant de clients en temps réel. Est-ce qu'il y a une journalisation qui se fait chez vous?

M. Cormier (Guy) : Bien, Denis, tu veux-tu y aller sur ça?

M. Lafrenière : Puis, je m'excuse, j'y vais rapidement parce qu'on est serrés dans le temps.

M. Cormier (Guy) : Oui, oui, tout à fait, tout à fait, vas-y, Denis, là, sur les mesures de sécurité.

M. Berthiaume (Denis) : Bon, écoutez, là, évidemment, là, quand on parle de nos mesures de sécurité à l'interne, la journalisation, chez Desjardins, il s'en fait, de la journalisation. Maintenant, il faut le voir comme un outil. Ce n'est

pas un bâton magique, la journalisation, là. C'est un outil dans le coffret à outils de toutes sortes de mesures de sécurité qu'on met. Dans l'encadrement, il y a de la journalisation.

M. Lafrenière : Parfait, ce qui m'amène à l'autre question, la préembauche. Vous faites une enquête de sécurité de vos employés qui vont se présenter chez vous?

M. Berthiaume (Denis) : Tout à fait, oui.

M. Lafrenière : Pendant l'emploi, est-ce que vous refaites une enquête?

M. Berthiaume (Denis) : Pour les comptes, évidemment, il y a des catégories d'emploi où, effectivement, les mesures de sécurité, les enquêtes sont beaucoup plus régulières.

M. Lafrenière : Vous comprenez où je veux vous amener quand je vous dis ça? C'est parce qu'un employé qui est rentré chez vous avec un dossier parfait, après quatre, cinq, six ans, problème financier quelconque, décide d'être malveillant pour le crime organisé ou quoi que ce soit, est-ce qu'il y a un drapeau qui va s'allumer automatiquement chez vous s'il n'y a pas de vérification qui se fait?

M. Berthiaume (Denis) : Dans nos comptes d'accès à hauts privilèges, il y a des enquêtes.

M. Lafrenière : Donc, c'est certain que ce n'est pas tout le monde. Merci.

Le Président (M. Simard) : Merci à vous, M. le député de Vachon. Vous êtes parfaitement dans votre temps. Je cède maintenant la parole à notre collègue la députée de Saint-Laurent. Madame.

Mme Rizqy : Merci beaucoup. Bienvenue parmi nous. D'emblée, on vous a proposé d'être assermentés, chose à laquelle vous avez dit que vous ne souhaitez pas demander une assermentation pour pouvoir répondre à nos questions.

On va continuer sur l'employé. Mes questions vont être très précises. Je ne parlerai pas de façon générale. On parle vraiment du dossier qui nous concerne, la fuite de données. L'employé en question avait combien d'années de service chez vous?

M. Cormier (Guy) : Écoutez, il y a une enquête policière en cours actuellement, là. C'est un employé qui travaille depuis longtemps, mais on a des... Il y a des recours collectifs contre Desjardins puis il y a des enquêtes policières. Alors, il y a des réponses qu'on va tout faire pour vous donner, là, mais je peux vous dire que c'est plusieurs années. Mais on a des avis qui nous disent d'être très prudents dans ce qu'on va exprimer publiquement.

Mme Rizqy : Comprenez-moi bien, je ne demanderai aucune donnée nominative qui pourrait révéler l'identité de la personne.

M. Cormier (Guy) : Plusieurs années, plusieurs années.

Mme Rizqy : Et l'employé en question, est-ce qu'il était dans un programme de marketing, de fidélisation de clients?

M. Cormier (Guy) : C'est un employé qui travaillait dans... qui avait accès à des bases de données chez Desjardins. Ça peut être au marketing, à la sécurité, aux ressources humaines, dans le blanchiment d'argent, mais c'est quelqu'un qui travaillait dans nos bases de données.

Mme Rizqy : Si vous souhaitez ne pas répondre à une question, vous pouvez le dire tout simplement. Est-ce que l'employé en question était, lorsqu'il est parti avec des données, dans un programme de journalisation ou pas?

M. Cormier (Guy) : Je ne sais pas s'il était...

M. Berthiaume (Denis) : Regardez, là, on tombe dans... Encore une fois, je réitère, là, on est dans une enquête, présentement, policière. Alors, on va être très, très prudents sur ce qu'on va déclarer ici à cette commission.

Mme Rizqy : Je ne pense pas qu'il y ait quoi que ce soit ici qui peut brimer l'enquête policière lorsqu'on demande une question sur la journalisation des données. Oui, il peut y avoir quelque chose par rapport au recours collectif, j'en suis. Est-ce que vous demandez le huis clos?

M. Berthiaume (Denis) : Je ne demande pas de huis clos.

Mme Rizqy : Si je vous dis que l'employé en question, il n'était pas dans un programme de journalisation, est-ce que ça, ça peut être vrai?

M. Berthiaume (Denis) : Regardez, je vous réitère qu'il y a des mécanismes de sécurité qui existent. La journalisation, c'est un des mécanismes de sécurité qui est utilisé chez Desjardins.

Mme Rizqy : L'employé en question...

M. Berthiaume (David) : Je ne veux pas commenter sur l'employé en question. Il y a des enquêtes en cours.

Mme Rizqy : O.K. À quel moment vous avez décidé, avec le Service de police de Laval... à savoir qui allait récupérer le matériel volé chez l'employé? Quelle date?

M. Cormier (Guy) : C'est Desjardins. Ce n'est pas avec le Service de police de Laval que ces démarches-là ont été faites, là. C'est, dans le fond, au moment où le Service de police de Laval nous a informés que, dans le cadre de l'une de leurs enquêtes, qui n'est pas reliée à Desjardins, en passant, là, qu'eux pensaient qu'il pourrait y avoir de l'information de Desjardins qui circule à l'extérieur de Desjardins. Donc, on était à la fin du mois de mai, à peu près, là.

Mme Rizqy : Et, à ce moment-là, vous avez pris une décision d'aller récupérer le matériel volé chez l'employé?

M. Cormier (Guy) : À ce moment-là, on a pris des décisions de protéger l'information qu'on avait chez nos membres comme tels.

Mme Rizqy : Est-ce qu'à ce moment-là, à quelque part dans votre service juridique, quelqu'un vous a informé que, si vous allez récupérer les données chez l'employé en question, il pourrait compromettre l'enquête criminelle parce que vous pouvez avoir compromis la preuve dans un procès futur? Est-ce que vous avez eu ce questionnement avec le service de police?

M. Cormier (Guy) : La décision que j'ai eu à prendre comme président de Desjardins, c'est : Est-ce que je protège les membres ou je protège l'enquête policière? J'ai décidé de protéger mes membres.

Mme Rizqy : Et aujourd'hui est-ce que ça fait en sorte qu'on n'est pas en mesure d'aller plus loin dans l'enquête criminelle?

M. Cormier (Guy) : Ce n'est pas ce que les policiers nous disent.

Mme Rizqy : D'accord. Et, par rapport toujours à l'employé en question, tantôt, vous avez dit qu'il avait agi seul. Est-ce que vous êtes certains qu'il a agi seul? Parce qu'on entend aussi qu'INTERPOL court après d'autres personnes.

M. Cormier (Guy) : Aujourd'hui, le Service de police de Laval, la Sûreté du Québec et nos propres enquêtes nous indiquent tous que c'est un employé qui a agi seul. On va laisser l'enquête poursuivre... Puis moi aussi, j'ai hâte de voir ce que la Sûreté du Québec et le Service de police de Laval vont poursuivre comme enquête. Mais aujourd'hui, l'information qu'on a en date d'aujourd'hui, à ma connaissance, c'est un seul employé.

Mme Rizqy : En décembre 2018, est-ce que vous étiez au courant qu'il y avait déjà une brèche?

M. Cormier (Guy) : Non. En décembre 2018, là, si vous référez à ce qui a pu être véhiculé, Desjardins a régulièrement transmis de l'information aux corps policiers parce qu'on avait trouvé qu'il y avait des transactions frauduleuses dans certains comptes. Ce qu'on fait, là, à chaque semaine, régulièrement, c'est par rapport à la lutte au blanchiment d'argent ou à des situations comme ça. On a transmis de l'information au Service de police de Laval sans savoir vers où ça nous mènerait.

Mme Rizqy : Mais vous saviez qu'il y avait déjà une brèche en décembre 2018 ou pas?

M. Berthiaume (Denis) : Moi, je réitère, là, ce qui a été fait en décembre 2018. Quand il y a des actions frauduleuses qui se passent, quand on pense qu'il y a un risque de fraude, automatiquement, on amène le dossier vers les autorités policières rapidement, quand on pense qu'il y a un acte criminel qui peut être commis. Par la suite, ça a pris un certain temps, il y a eu du travail conjoint avec nos équipes d'enquête interne, avec les policiers de Laval. Et c'est le 22 mai que les policiers de Laval nous sont revenus avec la donnée qui, là, pointait vers une fuite. Avant ça, on n'avait pas d'indication à l'interne.

Mme Rizqy : Mais, en décembre 2018, vous aviez déjà des lumières assez suffisantes pour appeler le Service de police de Laval, non?

M. Berthiaume (Denis) : Non. C'est un cas de fraude. Encore une fois, là, c'est une transaction qui nous apparaît suspecte qui a amené à une déclaration. Il y en a, là, régulièrement, des transactions qui nous apparaissent suspectes, qu'on amène vers les corps policiers, et là eux vont démarrer une enquête. C'est comme ça que ça s'est passé.

M. Cormier (Guy) : ...quelqu'un qui dépose un chèque, dans un compte, dans une caisse.

Mme Rizqy : Je comprends parfaitement, mais je suis vraiment dans le cas de l'employé malveillant. Dans le cas de l'employé malveillant, est-ce que c'est lui aussi que vous avez identifié en 2018?

M. Cormier (Guy) : Il n'y a pas de lien.

Mme Rizqy : Il n'y a pas de lien? D'accord.

M. Cormier (Guy) : Il n'y a pas de lien du tout, du tout. Il n'y a aucun lien. L'information qu'on a, c'est que, nous, là, comme on fait dans plein d'autres transactions, on avise un corps policier qu'il y a une transaction qui nous paraît bizarre, susceptible d'être peut-être criminelle, dans un compte. On envoie ça, parfois c'est au fédéral, parfois c'est à la Sûreté du Québec. C'est ça qui s'est passé.

• *(12 h 30)* •

Mme Rizqy : O.K., parfait. Et, au niveau de votre gestion de risque, est-ce que c'est par la suite que... Lorsque vous avez réalisé qu'effectivement ça touchait énormément de monde — initialement, vous avez été informés que c'était environ deux millions de personnes — au niveau du risque, étiez-vous suffisamment assurés pour ce risque ou, à partir du mois de juillet, vous avez fait des appels dans certaines compagnies d'assurance pour être assurés davantage?

Et, là-dessus, ça m'amène à la question suivante, parce que... Est-ce que vous avez géré le risque en fonction aussi des pénalités? En ce moment, quand je regarde les lois désuètes, c'est autour de 10 000 $ maximum, 100 000 $ pour une récidive. Est-ce que vous êtes suffisamment assurés pour ce type de fraude?

M. Cormier (Guy) : Bien, écoutez, on est une institution financière qui a des réassureurs pour plein de types de situations. Parfois, c'est la fraude. On est un assureur de dommages. Quand il y a des inondations, on indemnise, mais, à partir d'un certain niveau, c'est un réassureur qui indemnise. Donc, ça fait partie de nos activités courantes en termes de risque, donc ça fait partie de nos mesures de risque. On a des réassureurs. Parfois, on prend les risques nous-mêmes. Dans ce cas-ci, là, on a mis une provision de 70 millions dans notre deuxième trimestre, 40 millions pour la Protection membres Desjardins, 30 millions pour le service d'Equifax et quelques frais juridiques. Et, en date d'aujourd'hui, on n'a pas changé cette provision-là au troisième trimestre.

Le Président (M. Simard) : Merci. M. le député de Robert-Baldwin.

M. Leitão : Merci beaucoup, M. le Président. Alors, M. Cormier, M. Berthiaume, bonjour, merci d'être là. J'ai une question très précise qui est venue d'un citoyen, qui me l'a adressée et qui m'a demandé de vous la poser, donc je le fais. Depuis le début de cet événement, on est sous l'impression ou, en tout cas, ce citoyen est sous l'impression que les données qui ont été volées, c'est identification personnelle, nom, adresse, date de naissance, etc. La question qui se pose, et que je me pose aussi, et que je vous la pose : Est-ce que les soldes des comptes ont aussi été volés? Donc, l'information qui circule inclut non seulement nom, adresse, date de naissance, etc., mais aussi le solde en dépôt?

M. Berthiaume (Denis) : Il y a certains éléments de détention qui faisaient partie de la fuite, donc, oui. La réponse, c'est oui. En même temps, je réitère qu'il n'y avait pas de numéro de compte, il n'y avait pas de question de sécurité et il n'y avait pas de numéro d'identification personnel qui ont fuité. Il y avait certains éléments de détention, oui.

M. Leitão : Merci, merci pour la réponse. Et donc c'est là la question à laquelle on doit venir, poursuivant ce que le député de Vachon avait mentionné tantôt, donc le vol d'identité. Le vol d'identité, alors, devient encore plus dangereux dans ce cas-ci, puisqu'on a non seulement les noms, adresses, etc., des personnes, dates de naissance, mais aussi si cette personne a potentiellement un actif intéressant à son compte ou pas. Donc ça, ça permet au voleur de peut-être mieux cibler d'éventuelles opérations frauduleuses.

Maintenant, ce que je trouve important et que beaucoup de citoyens nous posent la question, et je ne sais pas si vous pouvez répondre, c'est : Qu'est-ce qui se passe maintenant? Donc, il y a des personnes, 4,4 millions de Québécois qui ont vu leurs données personnelles maintenant se trouver on ne sait pas trop où. L'enquête nous dira où ça se trouve. Maintenant, qu'est-ce qui se passe? Il y a les mesures de protection que vous avez mises en place, très bien, mais, en termes de protection de leurs actifs, protection de leur identité, comment vous voyez la suite des choses?

M. Cormier (Guy) : Bien, je vous dirais trois choses. La première, c'est qu'avec la mise sur pied de la Protection membres Desjardins le message que je passe aux membres chez Desjardins, c'est que Desjardins va vous prendre en charge si vous êtes victime, malheureusement, d'un vol d'identité. Et les gens, ils n'ont qu'à communiquer chez Desjardins. Si c'est dans vos comptes chez Desjardins, on vous rembourse, et, si vous êtes malheureusement victime d'un vol d'identité, nous sommes la seule institution financière qui vous accompagne comme on le fait, au Canada, avec des spécialistes, avec des remboursements jusqu'à 50 000 $ si vous avez des dépenses personnelles, puis avec un accompagnement très, très personnalisé. Donc, ça, c'est la première chose qui est importante pour rassurer les membres.

La deuxième chose, bien, c'est qu'il faut en discuter maintenant en tant que société. Moi, je pense que c'est anormal, encore, qu'en 2020 on s'identifie avec des permis de conduire, des numéros d'assurance sociale, des numéros de carte d'assurance maladie. Il y a des pays dans le monde qui ont pris une avance importante sur le Québec et le Canada par rapport à la protection des renseignements personnels. C'est un fléau, là, on le voit, il y a 28 millions de Canadiens qui ont été victimes de ça. Alors, je pense que ce qu'il faut faire maintenant, c'est une vraie, véritable réflexion de société pour aller plus loin.

Le Président (M. Simard) : Merci. M. le député de La Pinière, il vous resterait à peine 30 secondes.

M. Barrette : M. le Président, M. Cormier, M. Berthiaume, dans toute l'industrie où il y a des grandes banques de données, là, les banques, là, vous tous et toutes, là, aujourd'hui, dans votre industrie, on réclame des gouvernements qu'ils

interviennent pour resserrer les règles. Avez-vous une opinion là-dessus? Manifestement, les règles actuelles n'ont pas marché. Alors, je vous demande deux choses : Étiez-vous à date? Et, si les règles actuelles ne fonctionnent pas, qu'est-ce que vous recommandez au gouvernement? C'est ça, l'enjeu, là, ici, là.

Le Président (M. Simard) : Merci, M. le député de La Pinière. Alors, nous cédons maintenant la parole au député de Rosemont pour une période de 2 min 40 s. Cher collègue.

M. Marissal : Oui, en effet. Merci. Je coupe...

(Panne de son)

M. Marissal : Pardon?

Une voix : ...

M. Marissal : Merci. Je coupe court aux salutations. Ce n'est pas par manque de politesse, c'est par manque de temps. Ça, je le dis souvent. J'aimerais ça, mieux comprendre, parce qu'il y a quelque chose qui me mystifie. Fin 2008, vous indiquez à la police que vous avez identifié quelque chose de possiblement croche, 2018, fin 2018. Six mois plus tard, c'est la police qui vous dit qu'il y a eu effectivement un problème de l'ordre que vous mentionnez, mais c'est pire encore. Comment ça se fait, là, je vais faire court, comment ça se fait que, pendant six mois, vous n'aviez pas compris, vous ne vous étiez pas aperçus que vous vous étiez fait voler quatre millions de dossiers dans vos propres fichiers? Ça me... Je ne la pogne pas.

M. Cormier (Guy) : Bien, la réponse est simple. À chaque jour, on envoie plein d'informations à lutte au blanchiment d'argent, aux corps policiers, sur des transactions qui nous apparaissent douteuses. C'est des millions de transactions qu'il y a chez Desjardins dans une semaine, des millions, des milliards dans une année. Il y en a plein qu'on doit même, réglementairement parlant, déclarer à des autorités gouvernementales. Après chacune de ces transactions-là, notre travail à nous, ce n'est pas de les investiguer, c'est le travail de la police ou des autorités réglementaires. C'est notre règlement de faire ça.

M. Marissal : ...fait voler dans vos propres fichiers, là. Il y a eu un vol chez vous, puis vous ne le saviez pas.

M. Cormier (Guy) : Bien, au mois de décembre, là, on en... Aujourd'hui, probablement qu'il y a des gens chez Desjardins qui envoient de l'information à des corps policiers, aujourd'hui, là, aujourd'hui, pendant qu'on se parle. Est-ce que c'est un vol chez Desjardins? Je n'en ai aucune idée. C'est après que la police nous dit : Ah! bien, nous, on a... dans le cadre d'une enquête, puis ça aurait même pu venir d'une autre enquête, dire : On a trouvé de l'information reliée à Desjardins. Je comprends le lien qu'on essaie de faire, mais la réalité, là, c'est qu'aujourd'hui on envoie probablement de l'information à Ottawa sur la lutte au blanchiment d'argent, par rapport au terrorisme, par rapport à la cybercriminalité. Mais on ne met pas, nous, nos efforts à enquêter ça individuellement, on laisse les policiers faire leur...

(Panne de son)

M. Berthiaume (Denis) : Peut-être un élément, si vous permettez...

M. Marissal : Rapidement, s'il vous plaît.

M. Berthiaume (Denis) : Juste un élément rapidement, là. Décembre, c'était une transaction. Il n'y a pas eu de connexion possible à faire entre ça puis le fait qu'il y avait de la donnée qui était sortie, là. C'étaient deux choses.

M. Marissal : Mon point, c'est qu'il y a quelqu'un qui rentre dans votre système, un employé, il remplit quatre clés USB, il part avec le stock, vous ne le savez pas.

M. Cormier (Guy) : Fraude interne. La fraude interne, c'est la fraude... Parlez à tous les spécialistes aujourd'hui, ils vont tous vous le dire : la fraude interne, c'est la plus difficile à contrer. C'est arrivé chez Revenu Québec, c'est arrivé dans le système de santé, c'est arrivé dans plein d'organisations. 680 entreprises au Canada ont déclaré une fuite de renseignements personnels. Alors, je comprends qu'on peut vouloir faire porter le bonnet d'âne à Desjardins, là, mais Desjardins a été transparent, a été clair et a été... a fait preuve de franchise dans ce dossier-là, et je pense que là il faut juste aussi prendre le recul de se dire : L'enjeu est beaucoup plus grand que strictement Desjardins.

Le Président (M. Simard) : Très bien. Merci, M. Cormier. Je cède maintenant la parole au député de Jonquière.

M. Gaudreault : Oui. On aimerait bien parler à beaucoup de spécialistes, mais malheureusement on va en recevoir juste un aujourd'hui, là. Ce n'est pas qu'on n'en a pas demandé.

Moi, je veux juste essayer de comprendre, là, comment un employé, la personne suspecte, là, peut avoir eu accès à 4,2 millions de données. Lui, dans sa tâche, là, il avait libre accès à tout ou il était dédié à un secteur en particulier?

Alors, ça, c'est ma première question. Et, complémentairement à ça, comment ça se fait que son patron n'a pas fait un «double check», là, sur le travail qu'il faisait?

M. Berthiaume (Denis) : Bon. La première des choses, là, c'est sûr que la personne qui a commis l'acte malveillant, c'est un spécialiste des données, ce n'était pas... c'est un spécialiste des données qui a trouvé une façon de déjouer les mécanismes de sécurité qu'on avait en place. Il ne s'est pas levé le matin en ayant accès à l'ensemble de ça, il a déjoué les paramètres de sécurité afin de se donner ces accès-là puis éventuellement exfiltrer ces données-là. Alors, c'est ce qui s'est passé.

M. Gaudreault : Bon. Et il n'y a jamais personne qui s'est aperçu qu'il avait trouvé le moyen de déjouer. Donc, la question qu'on se pose — puis je fais du pouce sur la question non répondue du député de La Pinière : Comment on fait, là, pour empêcher ce déjouement, de déjouer ces données-là? C'est quoi qui vous manque, là, dans les lois présentement pour que nous, là, on puisse corriger ça puis agir pour empêcher un futur suspect ou un futur employé de chez vous ou ailleurs de procéder de la même manière? C'est quoi, la première chose qu'on devrait faire pour empêcher que ça arrive?

M. Berthiaume (Denis) : Bien, la première des choses que je peux vous dire, c'est que le stratagème qui a été utilisé, là, Desjardins a pris ses responsabilités. C'est sûr que le stratagème, il ne reviendra pas. Ça, c'est très, très clair.

M. Gaudreault : Mais ma question, c'est nous, là, d'un point de vue législatif et parlementaire.

M. Cormier (Guy) : Bien, je pense qu'essentiellement, là, il y a une autorité des marchés financiers qui encadre très bien le Mouvement Desjardins, qui met les mesures en place puis qui met les mêmes mesures que pour toutes les autres institutions financières canadiennes. Donc, je ne pense pas que c'est strictement...

• *(12 h 40)* •

M. Gaudreault : Donc, ne rien changer...

M. Cormier (Guy) : Ce n'est pas qu'il n'y a rien à changer, je pense qu'il faut vraiment se questionner sur la quantité d'information qu'on demande parfois à des citoyens pour faire des transactions ou pour faire... pour utiliser des données. Exemple, est-ce que, quand on a besoin de faire une transaction avec une institution financière, on a besoin de toutes ces informations-là comme telles? Parfois, ça vient par la lutte au blanchiment d'argent, on va nous demander : Va chercher cette information-là pour confirmer telle donnée. O.K., on a cette information-là. Est-ce que c'est celle-là qu'on avait besoin? On aurait pu en prendre une autre comme telle. Je pense qu'il faut se questionner sur certaines mesures qu'on met de l'avant pour voir la quantité d'information qu'une institution financière a besoin par rapport... pour opérer.

M. Gaudreault : Oui, mais, moi, là, comme membre de Desjardins, là, je veux dire, quand j'appelle, on me demande mon numéro de carte de crédit, mon code crypté en arrière, mon numéro de téléphone...

Le Président (M. Simard) : Très bien.

M. Gaudreault : ...on demande le nom de jeune fille de ma mère, je veux dire, il faut qu'on le trouve, là, la solution, alors...

Le Président (M. Simard) : Merci beaucoup. Merci beaucoup. Donc, cela conclut nos échanges. Madame, messieurs, merci d'être venus parmi nous.

Et, afin de faire place à l'AMF, nous allons suspendre temporairement nos travaux.

(Suspension de la séance à 12 h 41)

(Reprise à 12 h 45)

Le Président (M. Simard) : Alors, chers amis, merci d'avoir fait diligence. Représentants de l'AMF, bienvenue. Auriez-vous l'amabilité de vous présenter? Et vous savez que vous disposez d'une période de 10 minutes.

Autorité des marchés financiers (AMF)

M. Morisset (Louis) : Parfait. Alors, merci, M. le Président. Alors, mon nom est Louis Morisset, je suis le président-directeur général de l'Autorité des marchés financiers. Je suis accompagné aujourd'hui, à ma gauche, de mon collègue Patrick Déry, surintendant de l'encadrement de la solvabilité et, à ma droite, de ma collègue Gouro Sall Diagne, directrice principale de la surveillance des institutions de dépôt.

Alors, nous sommes ici aujourd'hui pour vous éclairer sur le type d'intervention que nous menons en continu auprès des institutions financières et sur celles que nous avons menées plus précisément dans le dossier du vol de données chez Desjardins avant et depuis le 20 juin dernier. Je vous exposerai nos principales conclusions à l'heure actuelle ainsi que les prochaines étapes que nous entrevoyons dans ce dossier, étant entendu que je ne pourrai révéler certaines informations spécifiques concernant le dossier en raison de la confidentialité des travaux de surveillance de l'autorité.

L'un des rôles confiés à l'autorité est celui de régulateur prudentiel des institutions financières qui sont autorisées, en vertu de nos lois, à faire affaire au Québec. L'autorité exerce, à l'égard du Mouvement Desjardins notamment, un rôle similaire à celui joué auprès des banques par le BSIF, le Bureau du Surintendant des institutions financières, au niveau fédéral. L'objectif principal d'un encadrement prudentiel est de favoriser rehaussement en continu de la solidité des institutions financières afin qu'elles soient en mesure d'honorer tous les engagements pris envers les consommateurs malgré la matérialisation possible de risques importants auxquels elles sont exposées. C'est ce que le législateur nous demande de faire par notre mandat d'encadrement de la solvabilité des institutions financières.

Et bien que l'application de la Loi sur la protection des renseignements personnels dans le secteur privé ne relève pas de l'Autorité des marchés financiers, nous nous intéressons à tout ce qui pourrait ébranler les institutions financières, leur réputation, et ultimement leur solvabilité. L'autorité effectue ainsi une vigie en continu des principaux risques susceptibles d'affecter la solvabilité des institutions financières. Ces risques peuvent prendre plusieurs formes telles qu'une nouvelle crise financière, une catastrophe naturelle importante, ou encore un incident opérationnel majeur, par exemple, un vol de renseignements personnels, sujet dont nous discutons aujourd'hui. Nous intégrons les résultats de cette vigie à nos activités d'encadrement de même que dans la priorisation et l'allocation de nos ressources dédiées à la surveillance des institutions financières. L'autorité reconnaît que les institutions financières sont des entreprises privées en situation de concurrence et qu'elles doivent prendre des risques raisonnables. Dans ce contexte, l'autorité tient les conseils d'administration et la haute direction responsables de la viabilité de leurs institutions. Dit autrement, notre rôle n'est pas de gérer les institutions à leur place.

Ce que je souhaite souligner d'entrée de jeu, d'abord, depuis la crise financière de 2007-2008, beaucoup de travaux ont été menés, au Québec et au niveau fédéral, pour rehausser la surveillance et les attentes à l'endroit des institutions financières, et cela même si nos institutions ont été beaucoup moins touchées par cette crise qu'ailleurs dans le monde. De plus, l'encadrement du secteur financier au Canada fait l'objet d'une évaluation en profondeur par le FMI, le Fonds monétaire international, tous les cinq ans. C'est un exercice rigoureux auquel l'autorité a été à nouveau soumise tout récemment, au même titre que le BSIF et d'autres agences fédérales ou provinciales. Le dernier rapport d'évaluation du FMI, qui a été rendu public le 24 juin dernier, conclut que les pratiques déployées par l'autorité et le BSIF sont similaires et globalement conformes aux meilleures pratiques internationales. Je tenais donc à vous réitérer aujourd'hui que nous prenons notre mission très au sérieux et que nous nous efforçons de ne déployer, au Québec, rien de moins que les meilleures pratiques au monde, à l'aune desquelles, d'ailleurs, nous sommes évalués régulièrement par le FMI.

Par ailleurs, l'autorité produit annuellement un rapport sur les institutions financières. Ces rapports, qui rendent compte de nos travaux et de notre lecture des risques importants, sont déposés à l'Assemblée nationale par le ministre des Finances et disponibles sur notre site Internet. Ils témoignent, à chaque année sans exception depuis 2013, des préoccupations grandissantes de l'autorité à l'égard des cyberrisques. Par exemple, dans notre rapport de 2014, nous écrivions : «Le facteur d'incertitude lié au cyberrisque contribue à accroître l'importance qui devrait lui être accordée. Toutes les organisations y sont confrontées, et a fortiori les institutions financières.

«[...]l'atteinte à la réputation d'une institution financière peut être la conséquence ultime d'une cyberattaque résultant, par exemple, du vol ou de la perte de renseignements confidentiels de clients.»

• (12 h 50) •

Autre exemple, dans notre rapport de 2015, nous écrivions : «Les cyberattaques peuvent provenir de plusieurs sources par exemple, la malveillance interne, le piratage, l'espionnage, l'usurpation d'identité [ou] le vol de données.»

Nous avons dès lors demandé à quelque 80 institutions financières, dont Desjardins, de compléter un questionnaire d'autoévaluation de 78 questions. Dans le cadre de cet exercice, les institutions se sont dites conscientes des menaces auxquelles elles font face et affirmaient avoir entrepris des actions pour rehausser leurs pratiques et niveau de préparation.

Nous avons accru l'intensité de nos activités de surveillance dédiée à ces risques auprès de toutes les institutions financières. Nous avons été le premier régulateur prudentiel au Canada à publier, pour consultation, en janvier dernier, un projet de ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications.

Ainsi, à la question : Est-ce que l'autorité avait identifié le risque possible d'un vol massif de données par un employé malveillant?, la réponse est oui. À la question : Est-ce que l'autorité a porté ce risque à l'attention des dirigeants des institutions financières qu'elle supervise?, la réponse est oui. Et à la question : Est-ce que l'autorité a demandé à toutes les institutions financières qu'elle surveille, incluant Desjardins, de rehausser leur vigilance et leur mécanisme de contrôle à l'égard de ce risque?, la réponse est oui.

Maintenant, un événement majeur qui atteint une institution financière génère de l'inquiétude, en particulier lorsqu'il s'agit d'une institution de la taille de Desjardins. La gestion ordonnée d'une crise, lorsqu'elle survient, constitue l'autre important volet de la mission d'un régulateur prudentiel. Nous devons identifier rapidement tout enjeu potentiel et porter un jugement sur l'efficacité des mécanismes déployés par l'institution pour y faire face ou la contraindre à agir si tel n'est pas le cas.

L'autorité est bien outillée pour jouer ce rôle, tant en termes de pouvoir que de capacité organisationnelle. Nos outils d'échange d'information et d'intelligence d'affaires sont à point. Nous pouvons générer et actualiser aussi souvent que nécessaire, plusieurs fois par jour, s'il le faut, nos tableaux de bord et nos indicateurs. La modernisation de nos pouvoirs, avec l'adoption du projet de loi n° 141 en juin 2018, est également venue renforcer notre coffre à outils.

Pour pouvoir bien jouer notre rôle, toutefois, il faut que l'autorité soit avisée rapidement et en toute transparence par l'institution touchée. Je réaffirme que ce fut le cas dans le présent dossier. Desjardins nous a signalé l'incident dans les heures suivant la première prise de connaissance de celui-ci et nous a tenus informés de tous ses développements au fur et à mesure par la suite.

Nous nous sommes assurés que les mesures requises avaient été déployées afin de colmater promptement le stratagème identifié. Nous avons obtenu réponse à nos questions, permettant de confirmer la prise en charge adéquate

et proactive de l'incident par les dirigeants de Desjardins. Nous avons effectué un suivi serré de la capacité financière et opérationnelle de l'institution, des réactions des marchés financiers, des investisseurs institutionnels et des agences de notation. Nous avons été en constante communication avec la Banque du Canada et d'autres régulateurs responsables de l'encadrement de certaines activités de Desjardins, notamment hors Québec.

Sur cette base, de même que par la réaction des parties prenantes que je viens d'évoquer, je peux affirmer que l'autorité est satisfaite de l'ensemble des actions prises jusqu'ici par Desjardins afin de protéger l'intérêt de ses membres et leurs actifs, et que l'autorité demeure confiante que les dirigeants de l'institution prennent la situation en charge avec la rigueur, la transparence et la célérité que commande la situation.

Ce dossier n'est toutefois pas terminé. Nous nous sommes assurés que l'institution procéderait à un bilan complet et détaillé de l'incident afin d'identifier toute mesure additionnelle ou changement structurel devant être mis en place. Cet exercice est en cours notamment à l'aide de consultants externes. Des décisions seront prises et des plans d'action devront être développés et déployés au cours des prochains mois par l'institution. L'autorité aura pleinement accès à l'analyse et aux constats et elle reverra les éventuels plans d'action qui en découleront. Nous nous ferons notre propre tête sur la rigueur et sur le caractère adéquat et complet de tous ces éléments.

Je peux toutefois vous affirmer que nous serons satisfaits uniquement de mesures alignées avec les meilleures pratiques observées sur le marché, que nous effectuerons un suivi serré de la mise en oeuvre intégrale et dans les temps des plans d'action et que nous nous assurerons que les constats qui pourraient découler des enquêtes en cours seront également traités avec célérité.

En terminant, rapidement, je voudrais vous souligner que, dans la foulée de l'incident chez Desjardins, nous avons rehaussé significativement notre présence médiatique au cours des derniers mois afin d'aider la population à se protéger contre de probables tentatives de fraude. Vous aurez peut-être ainsi vu à la télé ou entendu à la radio nos messages incitant les citoyens à la vigilance s'ils reçoivent des appels, des courriels ou des textos non sollicités leur demandant des renseignements personnels. Nous invitons les citoyens à ne jamais répondre à ces demandes ni à cliquer sur les hyperliens qu'elles peuvent contenir. Nous avons mesuré par sondage l'impact de notre campagne de sensibilisation, et les résultats sont intéressants.

Le Président (M. Simard) : Merci. M. Morisset.

M. Morisset (Louis) : Merci, monsieur.

Le Président (M. Simard) : Vous finissez sur une note positive en disant que les résultats étaient intéressants. Alors, voilà. Je cède maintenant la parole au député de Richelieu. Cher collègue.

M. Émond : M. le Président, messieurs, madame, bonjour, merci d'être avec nous aujourd'hui pour nous aider à faire un peu plus la lumière, à nous éclairer sur cette situation, parce que, si on se réunit aujourd'hui, si on en discute, c'est parce qu'il y a quand même 4,2 millions de Québécois qui sont préoccupés. Je dirais plus que ça, je pense que l'ensemble des Québécois sont préoccupés. En tout cas, dans mon comté, M. le Président, j'en ai entendu parler beaucoup encore aujourd'hui. Des citoyens de ma circonscription sont avec nous et suivent nos travaux aujourd'hui parce qu'ils ont des inquiétudes. Ma propre maisonnée chez moi, il y a des inquiétudes. On a été touchés, j'ai été touché personnellement, et les membres de ma famille, par la fuite des données chez Desjardins.

Je vous remercie pour votre présentation, et je prenais connaissance de votre document, qui fait la description de votre mission. C'est indiqué, et à raison, que vous êtes investis de vastes pouvoirs, l'AMF, hein? Puis, bien entendu, il y a des notions de confidentialité qui doivent dicter vos interventions, parce que, pour le bénéfice de nos auditeurs, des gens qui nous écoutent, vous êtes l'organisme mandaté par le gouvernement du Québec pour encadrer le secteur financier québécois puis prêter assistance aux consommateurs de produits et services financiers.

Mais, dans le cas qui nous occupe, le 20 juin dernier, suite à l'annonce publique de la fuite de données chez Desjardins, on comprend, donc, que c'était de votre rôle, de votre responsabilité d'entrer en contact avec la société pour vous assurer du respect des intérêts des consommateurs québécois. Vous en avez parlé dans votre mot d'introduction, mais j'aimerais avoir un peu plus de détails. Expliquez-nous votre rôle dans cette situation précise. Et puis, pour avoir le fil des événements un peu, quelle est la nature du contact que vous avez eu avec les gens de Desjardins immédiatement lorsque vous avez été avisés du fait?

Le Président (M. Simard) : Merci. M. Morisset.

M. Morisset (Louis) : Merci pour votre question. Écoutez, comme je l'ai mentionné, en effet, lorsque Desjardins a été mis au parfum de cette information-là, ils nous ont contactés immédiatement, et nous avons évidemment, dès ce moment, travaillé avec eux pour nous assurer, dans notre rôle de régulateur prudentiel, qu'ils allaient prendre les mesures appropriées, comme vous l'avez mentionné, pour protéger leurs clients, leurs membres, mais également s'assurer que la confiance du public demeure à travers ce processus et qu'on favorise la stabilité, donc, du système financier, notamment de la viabilité chez Desjardins.

Comme on l'explique, dans le document qu'on vous a remis — on vous a remis deux documents — le rôle de régulateur prudentiel, c'est essentiellement de s'intéresser à la solvabilité, à la stabilité financière, à la solidité financière des institutions afin qu'elles soient en mesure d'honorer leurs engagements auprès de la population, et ça, même si des crises surviennent. Et, quand une crise survient, bien sûr, c'est notre rôle, à ce moment-là, de s'y intéresser de près pour s'assurer que l'institution prenne les choses en charge.

Dans le cas de Desjardins, comme je l'ai mentionné, nous croyons que les mesures qu'ils ont déployées pour préserver, évidemment, les actifs de leurs clients sont les mesures appropriées, et nous les accompagnons, si je peux m'exprimer ainsi, dans ce processus.

M. Émond : Vous avez indiqué, dans votre introduction, que vous avez... lorsque vous avez été avisés de la fuite de données, vous en avez pris connaissance, vous avez mis en marche le protocole selon votre mission qui vous encadre, là, et vous avez même contacté les autres institutions financières pour discuter avec eux, pour les prévenir, quoi, qu'il venait de se passer un vol chez le mouvement coopératif Desjardins, puis j'aimerais vous entendre plus là-dessus. Puis ma question, c'est : Est-ce que c'était déjà arrivé par le passé que vous avez été amenés à investiguer, de vous pencher sur ce type de fuites de données? Et est-ce que c'est dans vos normes de prévenir ensuite l'ensemble du milieu financier qu'il vient de se passer quelque chose, cette fois-ci, qui était majeur? Peut-être, à d'autres occasions dans le passé, est-ce que vous avez dû le faire pour des moments peut-être un peu moins importants?

• *(13 heures)* •

M. Morisset (Louis) : Encore une fois, merci pour votre question, puis j'espère y apporter un éclairage approprié. Encore une fois, dans notre rôle de régulateur prudentiel, la volonté de l'autorité, c'est de s'assurer que Desjardins demeure solide malgré les turbulences, puis pour s'assurer qu'elle demeure solide, parce que, dans une crise comme celle qu'ils ont vécue, il aurait pu y avoir une crise de confiance plus importante au sein de la population. Ça aurait pu avoir des répercussions financières sur l'institution.

Alors, les contacts entre nous et la Banque du Canada, par exemple, sont usuels, sont nécessaire pour s'assurer que, s'il se passait quelque chose, qu'on allait pouvoir travailler de concert. Ça n'arrive pas fréquemment, des contacts avec la Banque du Canada, dans ce type de situation là. C'est arrivé en 2007-2008, lors de la grande crise financière qu'on a connue. Mais des contacts avec d'autres régulateurs et aussi avec la Banque du Canada peuvent arriver de façon régulière. Du côté des équipes de Patrick ou de Gouro, évidemment, qui sont au coeur de ces activités-là, on le voit fréquemment, mais, dans un contexte de crise, ça arrive relativement, je dirais, rarement, Dieu merci. Mais, dans ce cas-ci, il était important, nous, aux premières heures de cette situation-là, de s'assurer que, s'il se passait quelque chose, on allait tous travailler de manière coordonnée avec tous les autres régulateurs, dont la Banque du Canada, qui encadrent Desjardins.

Je ne sais pas si, Patrick, tu souhaiterais ajouter quelques éléments sur...

M. Émond : Bien, je pense... Je vous remercie pour votre réponse puis, M. le Président, je passerais la parole à mon collègue pour la suite des choses, s'il vous plaît.

Le Président (M. Simard) : M. le député de Rousseau.

M. Thouin : Merci, M. le Président. Madame, messieurs, merci d'être ici aujourd'hui.

Deux, trois questions, peut-être mieux comprendre vos positions dans le communiqué que vous avez publié, là, le jour même de l'incident. Vous vous êtes dit satisfaits des gestes posés par Desjardins afin de protéger l'intérêt des membres, là, et leurs actifs. Vous vous êtes aussi dit confiants que les dirigeants de l'institution ont pris la situation en charge avec rigueur et transparence.

Je pense que vous avec déjà expliqué assez bien, là, pourquoi vous avez jugé la situation satisfaisante, en fait, les prises de position satisfaisantes, mais j'aimerais ça savoir si vous croyez qu'il y a d'autres actions qui auraient pu être posées par la société pour mieux protéger leurs clients suite aux fuites de données. C'est peut-être la première question, j'aurai autre chose par la suite, s'il vous plaît.

M. Morisset (Louis) : Parfait. Bien, merci pour votre question. Patrick, veux-tu y répondre?

M. Déry (Patrick) : Oui. Bien, merci. Bonjour, tout le monde. Je crois que la citation à laquelle vous faite référence correspondait à la gestion, je dirais, de la nouvelle le jour même, et c'est par rapport à ce qui avait été fait pour communiquer à la population, aux membres, que l'institution les protégerait, qu'on se déclarait satisfaits.

Est-ce qu'il y a d'autres mesures? Ça, c'est ce que M. Morisset a évoqué dans sa présentation. Il y a un bilan qui est présentement en cours, qui est amorcé au sein de l'institution. Nous, notre rôle, lorsqu'il arrive en événement comme ça, c'est que les institutions fassent en sorte de tirer les leçons qui en découlent, et éventuellement, lorsque le bilan sera complété, nous allons accompagner l'institution pour s'assurer que toutes les mesures additionnelles qui pourraient être requises au sein de l'institution soient mises en place.

Mais il y a comme deux étapes. Il y avait la gestion de communiquer publiquement à l'ensemble de la population ce qui était arrivé. Ça, on était satisfaits de la façon dont ça a été fait. Et il y aura, à venir, dans les prochains mois, un exercice beaucoup plus en profondeur pour aller comprendre comment c'est arrivé, pourquoi c'est arrivé. Il y a un processus que l'institution peut faire par elle-même, mais il y a aussi les enquêtes en cours, tant par la police que les commissions d'accès à l'information qui ont annoncé, également, des enquêtes. Lorsque l'ensemble de ces faits là, cette base de faits là sera connue, nous allons également en tenir compte dans les suivis que nous ferons avec l'institution pour que toutes les leçons de cette crise-là soient bien prises en compte.

M. Thouin : Merci. Peut-être de façon plus générale, là, par rapport aux interventions possibles dans le monde entier et par nos gouvernements aussi, on sait tous que, à l'ère du numérique, les données personnelles sont très prisées, sont très prisées par certaines entreprises avec des intentions plus louables, marketing, bon, et tout ça, on sait comment ça fonctionne,

statistiques, mais très prisées aussi par des organisations qui ont de moins bonnes intentions. Donc, le risque de fuites de données est existant partout, oui, chez Desjardins, mais oui dans les banques, dans les gouvernements, les entreprises privées, médias sociaux, systèmes d'achat en ligne, et puis, tu sais, on a de l'info qu'on donne partout, tellement vrai que 680 entreprises, je pense, Desjardins mentionnait tantôt, là, qui ont déclaré des vols de données personnelles au Canada. Et je sais bien que, dans... et je vous cite, là, dans l'application de la Loi sur la protection des renseignements personnels dans le secteur privé, ça ne relève pas de l'Autorité des marchés financiers. On s'intéresse quand même à la chose parce que ça peut impacter les institutions avec lesquelles on travaille.

Dans le même communiqué — je vous ramène au communiqué — vous avez dit qu'un tel incident met en perspective, justement, le risque omniprésent qui pèse désormais sur les organisations en matière de risques reliés à la sécurité de l'information. Et, pour faire peut-être un peu de pouce sur les propos de mon collègue de La Pinière tantôt, est-ce que vous jugez que le gouvernement précédent aurait pu ou aurait dû agir plus tôt pour assurer une meilleure protection des renseignements personnels des Québécois?

M. Morisset (Louis) : Écoutez, c'est une question qui est difficile pour nous, à l'autorité, de répondre, en ce sens que, dans notre rôle à nous, qui est le rôle de régulateur prudentiel, comme je l'expliquais, on doit s'intéresser aux risques des institutions, on doit s'intéresser aux contrôles que les institutions mettent en place pour gérer ces risques-là. Et, dans le cas d'une institution comme celle de Desjardins, le risque opérationnel, le risque de sécurité d'information, le risque des technologies d'information sont des risques auxquels on s'est intéressé. Puis, comme je le mentionnais un petit peu tôt, nous, dès 2013, on a un peu sonné l'alarme en disant : Ce sont des risques qui se développent, qu'on voit et on incite les institutions à les gérer, et à s'y attarder, et à investir, évidemment, là où il faut pour éviter la matérialisation de ces risques-là.

Maintenant, le risque zéro n'existe pas, mais donc, dans la perspective de l'autorité, c'est certain que le risque de fuite de renseignements personnels s'inscrit dans un risque plus global, je dirais, qui est le risque opérationnel auquel on s'intéresse, le risque de cybersécurité. Puis, encore une fois, je peux juste réitérer que nous avons, de longue date maintenant, posé des gestes concrets pour sensibiliser les institutions à cet égard-là.

Je vais juste mentionner, je l'ai mentionné dans mon propos d'ouverture, la ligne directrice dont j'ai parlé, qui évoque les attentes de l'autorité en matière de gestion du risque des technologies de l'information, qu'on a publié pour commentaires en janvier et que nous allons, dans les prochaines semaines, prochains mois tout au plus, finaliser pour... comment je dirais, pour rendre disponible aux institutions financières, sera une ligne directrice, je dirais, assez robuste, qui réfère à des standards internationaux sur la gestion des risques de cette nature-là.

Donc, encore une fois, l'autorité constate qu'il y a des standards qui se développent, des standards qui évoluent rapidement, et on veut que les institutions s'accrochent à ces standards, choisissent les bons standards et les suivent. Alors, encore une fois, je pense que, de notre perspective, on a identifié ce risque-là et on a mené des actions concrètes pour sensibiliser et rehausser la vigilance des institutions à l'égard du risque.

M. Thouin : Je vous remercie. Peut-être, juste avant de passer la parole, tantôt, vous avez dit que, selon un rapport du FMI, là, l'AMF et le BSIF, là, sont à la hauteur des standards mondiaux, mais je conclurais tout de même qu'il me semble que, sachant... Tu sais, on sait qu'il y a des pays où c'est déjà arrivé et qui ont pris des mesures beaucoup plus robustes. Bien, il me semble qu'on n'a pas besoin d'attendre que ça arrive pour prendre ces mesures-là. On peut sûrement regarder les bonnes pratiques qui ont été faites ailleurs et aller au maximum maintenant. Voici mon opinion.

Le Président (M. Simard) : Merci, M. le député de Rousseau. M. le député de Saint-Jérôme, il vous reste une période de 4 min 20 s.

M. Chassin : Merci, M. le Président. Je vais continuer dans quelques instants, là, sur les meilleures pratiques, tel que mon collègue de Rousseau l'a évoqué.

Vous avez souligné, là, que vous allez réaliser, donc, un bilan détaillé de cet incident-là. J'imagine qu'il y a une partie relative à l'incident qui doit demeurer confidentielle. J'imagine qu'il y a peut-être une réflexion ou des lignes directrices qui émaneront de ce bilan-là, que vous pourrez peut-être rendre publiques. Je vous pose la question un peu à l'avance pour avoir votre perspective là-dessus.

M. Morisset (Louis) : Bien, le bilan qui est en cours, d'abord, c'est un bilan qui est mené au sein de Desjardins. Ils se sont, comme M. Cormier l'a mentionné tantôt, outillés avec des ressources externes pour les accompagner là-dedans, et nous, nous allons regarder de près, évidemment, les constats, les recommandations. Nous allons nous faire, comme je l'ai dit, notre propre tête sur ce qui s'en dégage et sur les plans d'action qui devront être développés. Au besoin, nous irons chercher des ressources externes également, si nécessaire, pour nous accompagner dans ce travail-là.

Ce que j'ai mentionné, c'est que, là, au sein de Desjardins, ce qui est arrivé est arrivé, malheureusement, et on doit aller au fond des choses puis voir s'il y a d'autres mesures additionnelles qui sont nécessaires, s'il y a des structures qui doivent changer. Bref, il faut aller au fond des choses. Si on peut dégager éventuellement de cela des apprentissages qu'on pourra apporter, à travers des lignes directrices ou autrement, aux autres institutions financières, nous le ferons, mais là on est vraiment dans une gestion d'un incident particulier. Et, comme je le mentionnais tout à l'heure, il existe des standards internationaux en matière de gestion des risques technologiques, et on incite les institutions à s'y accrocher.

Le Président (M. Simard) : M. le député, je vous incite à être synthétique. M. le député.

M. Chassin : J'aimerais revenir, parce que vous aviez parlé, dans votre allocution, que vous aviez identifié le risque. Vous allez dire: La réponse est oui, on l'a communiquée, cette information-là, on a demandé de rehausser les mesures de sécurité, la vigilance, vous avez utilisé ce mot-là, et donc vous avez des éléments pour aussi évaluer à quel point ça a été suivi. Je ne veux pas vous mettre dans une position difficile, mais le jour où vous avez fait paraître un communiqué de presse pour vous déclarer satisfaits des mesures prises par Desjardins... Vous m'ouvrez un peu la porte. Aujourd'hui, est-ce que vous seriez en mesure de dire que vous êtes satisfaits des mesures prises non seulement par Desjardins, mais par les assureurs, par les autres acteurs qui relèvent de votre responsabilité?

• *(13 h 10)* •

M. Morisset (Louis) : Je vais revenir sur la ligne directrice que nous allons rendre publique, là, finale dans les prochaines semaines. Je pense qu'on va trouver beaucoup de réponses à cet égard-là. Les attentes de l'autorité vont être bien, bien claires quant aux mécanismes de gouvernance, quant aux lignes de défense, le rôle des différents paliers dans ces organisations-là. Donc, je pense qu'à travers...

M. Chassin : ...votre évaluation ou votre satisfaction par rapport au suivi de ces lignes-là?

M. Morisset (Louis) : Oui. Je céderais la parole à Patrick pour poursuivre là-dessus.

M. Déry (Patrick) : Juste pour faire une petite nuance, on ne peut pas, comme régulateur prudentiel, vous comprendrez pourquoi, commenter sur la situation d'une institution versus une autre dans le détail. Ça peut être contre-productif ou amener le résultat contraire à la mission qu'on a de favoriser la confiance et la stabilité financière. On pourrait précipiter une crise ou provoquer une crise si on était maladroit dans nos communications.

Par contre, ce qu'on fait, c'est que, de façon générale, on va communiquer les leçons apprises des meilleures pratiques. On va sensibiliser sans révéler tous les détails à d'autres institutions lorsqu'on voit des pratiques moins bonnes que ce qu'on a vu ailleurs. On voit l'ensemble, nous, des entreprises. On est capable de guider les directions des compagnies en question vers des meilleures pratiques lorsqu'on voit des zones possibles d'amélioration.

M. Chassin : ...en conclusion, je pourrais vous amener... parce qu'on a entendu Desjardins parler, entre autres, d'identité numérique. Est-ce que, pour vous, c'est une piste à poursuivre?

M. Morisset (Louis) : Absolument, puis on sera heureux de pouvoir contribuer à ces réflexions-là, si on nous y invite.

M. Chassin : Vous en faites déjà, du travail, là-dessus?

M. Morisset (Louis) : Oui, oui, oui.

M. Chassin : Merci.

Une voix : Est-ce qu'on a quelques secondes ou c'est terminé, M. le Président?

Le Président (M. Simard) : C'est terminé, cher collègue. Vous pourrez éventuellement poursuivre plus tard. Mme la députée de Saint-Laurent, à vous la parole pour 10 min 40 s.

Mme Rizqy : Merci. J'aimerais juste bien comprendre. Donc, cet été, vous avez fait un communiqué de presse pour dire que vous avez apprécié la gestion de Desjardins. C'est bien ça?

M. Morisset (Louis) : Oui. Lorsque Desjardins est sorti, effectivement, on a été en contact avec eux, évidemment, dans les heures qui ont précédé, puis la prise en charge de cette situation-là, effectivement, nous a satisfaits, à ce moment-là. On était au tout début, bien sûr.

Mme Rizqy : Parce ce vous êtes conscient que, dans votre mission, encadrer, surveiller les activités... mais vous avez aussi l'autre volet, protéger les consommateurs et les mettre en garde de toute approche frauduleuse.

Vous vous rappelez que, vers le mois d'août, après plusieurs semaines, il y avait moins de 20 % des membres de Desjardins qui étaient en mesure d'être inscrits à Equifax, n'est-ce pas?

M. Morisset (Louis) : Oui.

Mme Rizqy : Vous vous rappelez aussi que plusieurs n'ont pas été capables d'avoir un service en français.

M. Morisset (Louis) : C'est ce qu'on comprend, oui.

Mme Rizqy : Et vous vous rappelez aussi qu'il y a plusieurs membres de Desjardins qui sont des aînés, qui n'ont pas non plus accès à un service Internet ou ne sont pas à l'aise et que le clavier avait des défaillances lorsqu'on tapait en français. Vous vous en rappelez?

M. Morisset (Louis) : Oui, bien sûr.

Mme Rizqy : Lorsque vous parliez tantôt de l'OCDE, des rapports, dans les règles de bonne gouvernance, il y a aussi une question de gestion de risques. Ça aussi, j'aimerais qu'on revienne là-dessus, car, il n'y a pas si longtemps, il y avait des entreprises... là, maintenant, je ne fais pas référence à Desjardins, je parle aux entreprises, institutions financières, et tout cela.

Il n'y a pas si longtemps, il y avait des choix qui ont été faits, de polluer parce que les pénalités coûtaient moins cher. Alors, il y avait ça comme dans gestion de risques. Et maintenant je m'en viens ici, au Canada. On voit qu'ailleurs dans le monde, depuis 2012, 2013, 2014, il y a eu plusieurs fuites de données et des pénalités à l'international, on parle de centaines de millions de dollars. Un Marriott, 162 millions; British Airways, 300 millions; Facebook, 500 millions de dollars.

Ici, au Canada, dans le dossier, par exemple, d'une entreprise ou d'une institution financière qui se fait prendre, en ce moment, l'amende est de 10 000 $ et pour un maximum de 100 000 $, récidive. Pensez-vous qu'il est grand temps qu'on augmente les pénalités?

M. Morisset (Louis) : Merci. Peut-être, je reviendrais juste d'abord sur le premier volet de votre question. C'est pour ça que je l'ai mentionné tantôt, pourquoi l'autorité est intervenue rapidement pour tenter de rejoindre la population qui peut avoir des difficultés à s'inscrire. Donc, on a fait plusieurs mesures pour sensibiliser la population.

Maintenant, pour revenir sur le dernier volet de votre question, les choix législatifs au Québec, au Canada ont été différents, au fil des années, sur l'ampleur des pénalités. On voit des différences notables entre le Canada et les pays ailleurs dans le monde. Est-ce que des pénalités plus sévères pourraient avoir un effet plus dissuasif? Possiblement. Cela étant dit, ce sont des choix de longue date qui ont été faits dans notre juridiction. Peut-être qu'il est temps de les revoir à cet égard-là.

Mme Rizqy : Par exemple, la Loi sur la protection des renseignements personnels dans le secteur privé, on parle de 1978 ou 1979, si ma mémoire est bonne, donc ça fait pratiquement 40 ans. Donc, si, à l'époque, 10 000 $, ça peut être une grosse tape sur les doigts, vous comprendrez qu'aujourd'hui, en 2019, ce n'est pas grand-chose.

Alors, c'est pour ça que, oui, je pense que, si... Il y a plusieurs pays, je parle de l'Angleterre, je parle des États-Unis, je parle de la France, parce que vous faites référence à l'OCDE. Ils sont membres eux aussi de l'OCDE et ils ont fait le choix d'avoir des amendes sévères pour, justement, qu'à l'interne le privé puisse aussi se dire : Bon, si jamais on a un employé qui a accès à plusieurs bases de données, on va s'assurer d'avoir mis plusieurs pare-feu et vraiment s'assurer que, dans ce cas-ci, il ne va pas exposer l'entreprise à des poursuites non seulement civiles, criminelles, mais aussi des pénalités excessivement élevées.

Pensez-vous, je vous repose la question, qu'ici il serait peut-être grand temps d'avoir des pénalités qui rejoignent la norme internationale des pays membres du G7?

M. Morisset (Louis) : Bien, encore une fois, c'est difficile pour moi de commenter spécifiquement. Je pense que ça fait partie d'un environnement canadien, québécois, où les pénalités sont beaucoup moins sévères qu'aux États-Unis ou qu'ailleurs dans le monde à bien des égards, dans ce domaine comme dans d'autres. Alors, je pense que c'est un choix de société que vous, comme parlementaires, avez tout le loisir de revoir ou de réfléchir.

Mme Rizqy : Merci beaucoup, Me Morisset.

Le Président (M. Simard) : M. le député de Robert-Baldwin, il vous reste six minutes, cher collègue.

M. Leitão : Merci, M. le Président. Alors, M. Morisset, M. Déry, madame, bonjour, merci d'être là.

Écoutez, je vais vous amener sur certains éléments. On a parlé tantôt de l'identification numérique, et vous avez déjà fait un certain... un petit peu de travail à cet égard-là. Pouvez-vous nous parler brièvement de ce vous avez fait, brièvement?

M. Morisset (Louis) : Je céderais la parole à Patrick.

M. Déry (Patrick) : Écoutez, à l'autorité, on s'intéresse évidemment à l'innovation dans le secteur financier, ce qu'on appelle les «fintech», donc l'innovation technologique appliquée à la finance, qui couvre un paquet, je dirais, de chantiers ou d'éléments d'innovation. Et, parmi... un, un d'entre eux, c'est la finance ouverte ou, en anglais, on parle d'«open banking».

Vous n'êtes pas sans savoir qu'on a un rendez-vous de l'autorité avec l'industrie à chaque année, M. le député, et, lundi prochain, on a un atelier spécifiquement sur cette question. Et une des premières, je dirais, contraintes qu'on frappe lorsqu'on discute d'«open banking» ou d'innovation dans le secteur financier, c'est la protection des renseignements personnels.

Donc, avant même, je dirais, l'enjeu qu'on gère dans la situation de Desjardins, du vol de données, toute l'innovation qui se déploie dans le secteur financier nous a amenés à s'intéresser de près aux travaux, aux recherches, aux idées de spécialistes du domaine qui peuvent aider à renforcer la protection de ton identité comme consommateur de services financiers dans l'Internet. Donc, oui, on s'intéresse à cette question-là. On a beaucoup de spécialistes à l'interne, à l'autorité, qui suivent ces questions-là.

M. Leitão : Merci. Bien, juste ça, je pense, M. le Président, on pourrait avoir une commission parlementaire juste sur ça, pour entendre les experts dans ce domaine. Et je vous cite juste un rapport, un discours du président de l'exploitation

de la Banque du Canada, M. Dinis, qui a parlé de la cybersécurité, de lever les obstacles, et donc, pour lui, c'est surtout la collaboration qui est la voie à suivre. Donc, voilà, je pense que... je nous incite, nous tous, à aller dans cette direction aussi de collaboration et d'un regard large sur cette question.

Revenons à l'ordre du jour. Bon, ici, on n'est pas dans les grandes tactiques de cybercrime très sophistiqué, on est carrément dans le vol de données. Comment est-ce que ça a pu arriver? Comment est-ce qu'une personne peut aller chercher, malgré tous les moyens de contrôle internes qui, je suis sûr, existent, comment cela a pu se passer? Je ne sais pas si vous avez une réponse à ça ou pas. Et, surtout, qu'est-ce qu'on fait pour prévenir de telles fuites massives qui viennent de l'interne à l'avenir?

M. Morisset (Louis) : Bien, on ne peut pas répondre à la question, comment s'est arrivé, qu'est-ce qui est arrivé. Je pense que l'institution elle-même attend l'enquête policière pour savoir exactement ce qu'il s'est passé. Vous avez entendu les réponses que les membres de Desjardins ont données plus tôt avant nous.

Mais je pense que ce qu'il faut faire, c'est de réitérer, renforcer les contrôles en place au niveau de la gestion du risque technologique. Et, nous, comme régulateur, on va poursuivre évidemment nos efforts, nos démarches. Puis la ligne directrice à laquelle je faisais référence tantôt va être utile pour amener les institutions à focaliser encore davantage sur ce risque.

• *(13 h 20)* •

M. Leitão : Merci. Et, dans cette quête, donc, d'améliorer les procédures de gestion du risque, est-ce qu'on devrait garder une meilleure réglementation, meilleur encadrement sur l'utilisation des données? Donc, il y avait, chez Desjardins comme dans toutes les autres institutions financières — et ici on ne cible pas Desjardins, c'est toutes les institutions financières — donc, des groupes d'employés qui ont accès à toute la banque de données interne de l'entreprise pour toutes sortes de stratégies, de politiques, de marketing, etc. Encore une fois, ce n'est pas Desjardins, c'est toute l'industrie. Est-ce qu'on devrait réglementer cet accès-là aux banques de données internes des institutions financières?

M. Morisset (Louis) : Parfait. Bien, écoutez, je reviens, encore une fois, sur la ligne directrice. On va toucher ces aspects-là dans la ligne directrice. Peut-être Patrick souhaiterait ajouter quelques éléments?

M. Déry (Patrick) : Oui. En fait, juste sur le mot «réglementer», que je m'interroge sur le sens, la portée de votre question. Mais, nous, quand on parle de standards internationaux, on a les normes NIST, les normes COBIT, les normes ISO, qui sont toutes des façons de faire ce que vous dites, là, comment qu'une entreprise doit gérer les accès en fonction de qui doit avoir accès ou pas à des renseignements pour faire leur travail, etc. La gouvernance entourant ça, les mécanismes de sécurité, tout ça, c'est codifié par des spécialistes qui font des conférences à l'année longue sur ces domaines-là.

Et, nous, ce qu'on dit aux institutions financières : Ne réinventons pas la roue. Assurez-vous de choisir, parmi les standards qui existent, les meilleures pratiques qui s'appliquent à vous et montrez-nous, démontrez-nous un régulateur, que vous gagnez en maturité, vous rehaussez vos postures en vous inspirant de ces meilleures pratiques là. Et c'est comme ça, je crois... le mot «réglementation» n'est peut-être pas comme un règlement, là, mais par l'encadrement, par le travail de surveillance qu'on va faire, qu'on pense atteindre l'objectif d'avoir des institutions qui suivent les meilleures pratiques au fur et à mesure qu'elles évoluent.

Mme Rizqy : Merci. M. le Président...

Le Président (M. Simard) : Bien sûr, madame... chère collègue, allez-y. Il vous reste 50 secondes.

Mme Rizqy : À la page 5 de votre article que vous avez déposé, la gestion ordonnée d'une crise, dans votre mandat, encadrer et surveiller les activités, lorsque vous êtes informé qu'une institution financière vit une situation de crise, est-ce que vous les accompagnez? Est-ce que vous leur offrez aussi votre expertise? Parce que vous en faites, vous, des enquêtes, donc vous comprenez parfaitement à quel point c'est important de protéger la preuve et la chaîne qu'on doit tenir par rapport à la preuve, qui pourrait nous être utile dans une enquête policière. Est-ce que vous, dans ce cas-ci... avez-vous fait un accompagnement auprès de l'institution financière ou pas du tout?

M. Morisset (Louis) : Non. Dans ce cas-ci, nous n'avons pas fait ce genre d'accompagnement.

Mme Rizqy : Pensez-vous que ça pourrait être utile, justement, d'avoir une ligne d'urgence avec, vraiment, un modus operandi pour dire que...

Le Président (M. Simard) : En conclusion.

Mme Rizqy : ...lorsqu'on sait qu'il y a une preuve qui est potentiellement chez un employé...

Le Président (M. Simard) : En conclusion.

M. Morisset (Louis) : Je vous dirais, je pense que les corps policiers sont bien placés pour aider dans un tel contexte.

Le Président (M. Simard) : Merci. Merci beaucoup. M. le député de Rosemont, à vous la parole.

M. Marissal : M. le Président, alors, je vous salue et remercie prestement pour gagner du temps.

Page 5, à la question : Est-ce que l'autorité a demandé à toutes les institutions financières qu'elle surveille, incluant Desjardins, de rehausser leur vigilance et leur mécanisme de contrôle à l'égard de ce risque?, la réponse est oui. Je comprends donc que la vigilance dont on parle ici n'était pas à un niveau adéquat puisque vous avez demandé de rehausser. Et qu'est-ce qui devait être relevé dans la vigilance? Qu'est-ce qui clochait?

M. Morisset (Louis) : Oui. Bien, je céderais la parole à Patrick Déry, s'il vous plaît.

M. Déry (Patrick) : Écoutez, comme on l'a dit dans le discours, puis on y fait référence dans un hyperlien qu'on peut aussi vous remettre, un communiqué de 2016 qu'on a émis, l'exercice d'autoévaluation qu'on a mené auprès des institutions visait à prendre acte ou à faire un constat, je dirais, du niveau d'autoévaluation de chaque compagnie par rapport à sa maturité. Et évidemment que, comme c'est des risques émergents, des sujets qui prennent de plus en plus d'ampleur, qui deviennent aujourd'hui un problème, un fléau auquel il faut s'attaquer... Il y a quelques années, le niveau de maturité n'était pas, je dirais, au niveau qu'il est aujourd'hui et au niveau qu'il sera demain. C'est un processus de rehaussement continu de la posture dans toutes les institutions qu'on surveille, auxquelles on...

M. Marissal : Je vous arrête une seconde. Je ne veux pas être impoli, mais je n'ai pas de temps. Vous avez demandé de rehausser après la fuite ou le vol de données chez Desjardins, cet été.

M. Déry (Patrick) : Ce qu'on a dit, c'est que, dès 2015, en faisant un exercice d'autoévaluation, ce qui ressortait de l'exercice, c'est ce qu'on a communiqué à chacune des institutions : parfait, on regarde le constat, vous reconnaissez que c'est un enjeu émergent et sur lequel on doit s'y attarder. Nous, on vous demande de rehausser votre jeu par rapport à ça dès 2015, et c'est un suivi qu'on fait en continu depuis.

M. Marissal : Et qu'est-ce qui a été fait chez Desjardins en particulier?

M. Déry (Patrick) : Malheureusement, je ne peux pas commenter un dossier spécifique, parce que, là, c'est révéler... puis une compagnie par rapport à une autre, on créerait des problèmes qui sont incompatibles avec la mission de l'autorité. Mais, de façon générale, les éléments de gouvernance, de saine gestion de leurs risques, etc., c'est ça qu'on veut voir rehausser.

M. Marissal : Question un peu technique ici, là. Page 6 : «Pour pouvoir bien jouer son rôle, toutefois, l'autorité doit être avisée rapidement par l'institution touchée, et ce, en toute transparence.» Le «doit» ici, est-ce qu'il fait référence à une obligation légale ou c'est quelque chose qu'on prend pour acquis, que l'institution le fera?

M. Morisset (Louis) : ...je veux dire, bien, c'est une attente dans nos lignes directrices. Donc, ce n'est pas...

M. Marissal : Mais ce n'est pas une obligation légale.

M. Morisset (Louis) : Bien, c'est une attente explicite, mais ce n'est pas enchâssé dans la loi.

M. Marissal : Est-ce que ce serait utile d'avoir une telle obligation légale?

M. Morisset (Louis) : Il faut y réfléchir, absolument.

Le Président (M. Simard) : Merci beaucoup. M. le député de Jonquière.

M. Gaudreault : Oui, merci. J'étais un peu dans ce même sens, parce que, contrairement aux lois fédérales — qui s'appliquent évidemment aux banques et aux institutions, aux entreprises de télécommunication, par exemple — la Loi sur la protection des renseignements personnels dans le secteur privé du Québec n'a pas d'obligation de divulgation des incidents de vols de données, par exemple.

Donc, est-ce que, même pour le privé, il devrait y avoir cette obligation de divulguer les incidents, soit à la Commission d'accès à l'information ou à une autre institution renforcée ou plus forte et à votre institution quand c'est le cas d'une institution financière?

M. Morisset (Louis) : Bien, notre perspective là-dessus, c'est clairement oui. Tous les incidents doivent être rapportés pour permettre, justement, une meilleure gestion de crise lorsqu'une crise survient ou une gestion de l'incident comme tel. Alors, effectivement, je pense que c'est des obligations qui devraient être renforcées, devraient être clarifiées. Ce qu'on constate, nous, c'est qu'on en reçoit parfois, donc, des divulgations de moindre nature, mais, encore une fois, c'est dans une ligne directrice, ce n'est pas dans la loi. Donc, il faut y réfléchir dans l'environnement de l'autorité, mais de façon plus globale, je pense, aussi.

M. Gaudreault : Donc, si cette commission ici arrive avec une recommandation disant : L'AMF recommande aux parlementaires de modifier la Loi sur la protection des renseignements personnels dans le secteur privé pour avoir cette obligation de divulgation, vous seriez d'accord avec cette recommandation?

M. Morisset (Louis) : Oui.

M. Gaudreault : Parfait. Merci. Concernant les pénalités pour les problèmes ou les fuites de données, il y a d'autres législations à travers le monde qui ont, je dirais, des pénalités proportionnelles selon la durée des conservations des données. Comme par exemple, si c'est des données qui sont périmées, entre guillemets, depuis 10 ans, mais que l'institution les garde quand même, puis là elles sont volées, bien là, ça pourrait être... Je veux dire, il faut faire un ménage, autrement dit, dans les données. Est-ce que vous pensez que ça pourrait être un type de système de pénalités?

M. Morisset (Louis) : Bien, je dirais, encore une fois, je pense que le volet dissuasif, qui vient avec une pénalité sévère, est certainement un outil pour encourager les institutions et les organisations à se comporter de la meilleure façon. Je pense que ce que les entreprises conservent, on doit y réfléchir parce qu'effectivement il y a des données qui devraient disparaître à un moment donné pour éviter ce genre de situation.

Le Président (M. Simard) : Alors, merci à vous, M. Morisset. Madame, messieurs, merci pour votre contribution à nos travaux.

Sur ce, nous suspendons jusqu'à 15 heures.

(Suspension de la séance à 13 h 28)

(Reprise à 15 h 04)

Le Président (M. Simard) : Alors, chers amis, bon retour à toutes et à tous. La commission, comme vous le savez, est réunie afin de poursuivre les consultations particulières et auditions publiques sur la question de la fuite de données personnelles chez Desjardins.

Cet après-midi, nous entendrons Equifax Canada, l'Association des banquiers canadiens, l'Office de la protection du consommateur ainsi que M. José Fernandez, professeur titulaire au Département de génie informatique et génie logiciel à Polytechnique Montréal.

Avant de débuter, je crois comprendre qu'il y aurait consentement afin que le député de Gouin remplace le député de Rosemont. J'ai bien compris qu'il y avait consentement? Il y a consentement. Alors, bienvenue à vous, M. le député de Gouin.

Comme nous avons légèrement commencé en retard, j'aurais également besoin de votre consentement afin que nous puissions légèrement dépasser le temps qui nous était initialement alloué. Il y a consentement? Très bien.

Alors, nous allons, d'entrée de jeu, immédiatement, commencer avec le représentant d'Equifax Canada. Vous savez que M. Heft est présentement en Belgique. Une partie de sa présentation sera en français, l'autre sera en anglais. Nous avons donc prévu un service de traduction. Plusieurs d'entre vous ont déjà reçu les masques requis pour l'audition.

Des voix : ...

Le Président (M. Simard) : Pardon? Oui... les masques! Là, comment on appelle ça, d'abord?

Des voix : ...

Le Président (M. Simard) : Un casque, oui!

Des voix : Ha, ha, ha!

Le Président (M. Simard) : Oui, voilà! Alors, les casques requis. Et donc, conséquemment, je vous inviterais néanmoins à parler peut-être avec un débit un peu plus lent pour faciliter le travail de nos traducteurs, qui, par ailleurs, sont d'un très grand professionnalisme.

Alors, M. Heft, soyez le bienvenu parmi nous, et vous savez que vous disposez d'une période de 10 minutes.

Equifax Canada inc.

(Visioconférence)

M. Heft (Joel) : Merci beaucoup. M. le Président, M. le vice-président et membres de la commission, je suis heureux de participer à l'audience aujourd'hui. Mon nom est Joel Heft, et je suis vice-président directeur des solutions en matière de brèches et de réglementations internationales chez Equifax.

Je travaille à Equifax depuis 23 ans. Je me suis joint à Equifax en 1997 comme avocat général pour l'entreprise canadienne. En 2007, j'ai été nommé vice-président directeur, avocat général de l'entreprise internationale d'Equifax, responsable de superviser les affaires juridiques, les relations gouvernementales, la gouvernance de l'entreprise et la protection de la vie privée dans les 23 pays où nous exploitons nos activités à l'extérieur des États-Unis. Au cours des cinq dernières années, j'ai dirigé les services liés à la réglementation aux brèches à l'échelle mondiale. Dans le cadre de ce poste, je gère notre équipe de résolution d'incidents touchant les données partout dans le monde.

Allow me to take a minute to apologize for not being with you in person today, I truly wish I was, and for any technical difficulties which may be associated with the translation services required to make my participation possible by teleconference. I'm not able to cancel my previously scheduled commitment this week in Europe. But, because I'm likely the best suited person at Equifax to provide you with the information about the services that we are providing to Desjardins and its members, we are trying to be as helpful as possible by having me testify by phone from Brussels this evening.

I intend to brief you about the data incident response services that Equifax is providing to Desjardins and its members, and I intend to use my opening remarks to provide you with : a, an overview of the data incident response services that Equifax offers in Canada, and, b, a description of the services that we are providing to Desjardins in support of its members.

I was chosen as a witness because of my responsibility and knowledge regarding incident response services we are providing to Desjardins. This is where I'll focus my remarks.

Equifax is a global leader in data incident and response services for organizations, both private and public, that have experienced a data security incident impacting employees or customers. Since 2016, we have assisted over 2,500 organizations globally and 500 in Canada alone.

The response and remediation services we offer to organizations facing a data incident fall into four categories : notification, call center support, credit monitoring and identity restauration. I will elaborate on each.

• *(15 h 10)* •

Notification. This is to ensure that impacted consumers are efficiently notified of a breach. We provide mail and email notification services on behalf of our clients.

Call center support. On behalf of our clients, we provide incident specific call center support for the impacted consumer population in order to answer questions about the data incident itself.

Credit monitoring. For the impacted population, we provide daily credit monitoring and automated alerts of key changes to the information in the credit reports of impacted consumers. A current credit report is available to consumers with all credit monitoring solutions.

Identity restauration. We provide assistance and guidance for identity theft victims to help them restore their identities as quickly and effectively as possible. Our data incident response solutions are comprehensive and help provide protection and remediation to impacted consumers.

Equifax understands all too well that the threat of data theft, whether by cyberattack or by rogue insiders, is real and increasing. Cybercrime and data theft that targets individuals, our businesses and even our governments are some of the greatest threats facing our country. Canadian companies are continually trying to thwart criminals that operate outside the rule of law and attempt to extract data for their own gain.

The Privacy Commissioner of Canada states that in the last year alone, it has received reports of 680 data breaches at Canadian companies, impacting over 28 million people. These attacks on Canadian companies are attacks on Canadian consumers and attacks on our country. Fighting theses attackers will require partnership and cooperation amongst government, law enforcement and private business.

I'd like to turn now to the specific services that we are providing to Desjardins and its members. Desjardins chose to provide its impacted members with five years of Equifax's best-in-class consumer credit monitoring and identity theft protection service. That's called the Equifax Complete Premier Plan. For the benefit of those in the room and your constituents, let me describe the key features of this plan.

Equifax credit report monitoring provides alerts of key changes to a consumer's Equifax credit report. It provides the individual with access to his Equifax credit report on a daily basis and also contains an easy to read summary of the information contained in his or her Equifax file; identity theft insurance, which helps paying certain out-of-pocket expenses in the event a consumer becomes a victim of identity theft; identity restauration : a dedicated identity restauration specialist will work a on consumer's behalf to help restore his or her identity, should the consumer become the victim of identity theft; Internet scanning : our Internet scanning alerts a consumer in the event that his or her credit cards numbers, bank account numbers or social insurance numbers are found on suspected fraudulent websites; and lost wallet assistance : if a consumer loses his or her wallet, our agents will help the consumer and have his or her cards and ID cancelled and reissued.

The plan also includes Equifax's credit score monitoring, access to the Equifax's credit score and Equifax's credit score trending. Consumers can access our customer care representatives seven days a week, from 8:00 a.m. to 12:00 a.m. Eastern time.

In order to best serve affected Desjardins members, we work together with Desjardins to devise new processes and procedures to improve our traditional services. I'll walk you through some examples.

We established a new process for minors who are affected by the data breach. Equifax established a credit file for the minor where none existed before, and, on the newly created credit file, an alert flag was posted to ensure any... to the file of a minor would return a notification of the alert, along with direction to contact the consumer directly.

New process for individuals without Internet. To support individuals without Internet or email access, Equifax worked with Desjardins to establish a new process whereby impacted consumers could access Equifax's services directly through Desjardins.

But we also addressed some of the challenges that we faced in the rollout of our services to Desjardins members. Simply put, at the outset of the announcement of the Desjardins incident our systems and call centers were overwhelmed by the tremendous and unprecedented demand by consumers to enroll in our services. During that period, we were unable to meet our high standards of consumer care. With regard to consumer support in French, we did not provide a level of service to which we strive and to which Quebeckers are entitled. We apologize for this.

At all times, however, we did our best to support consumers during difficult circumstances and endeavored to make process improvements in their interest. For example, within the first month of the announcement, we increased call

center capacity by over 60%. Between June 2019 and October 2019, we increased the number of agents in our call centers by 1,000%, having introduced new waves of agents almost every week.

I'm pleased to report that our services levels...

Le Président (M. Simard) : ...left.

M. Heft (Joel) : ...have improved. Oui?

Le Président (M. Simard) : There is 30 seconds left, sir, in time... in your time.

M. Heft (Joel) : OK, alright, thank you. I'm pleased to report that our service levels have improved significantly since the outset, and today the average consumer wait times are mere seconds. It is difficult to overestimate the incredible demand following the initial announcement of the data incident. To put that in perspective, during our support of the Desjardins incident, it was common for us to be enrolling more consumers in credit monitoring services in a single day than we would typically enroll in an entire...

Let me conclude...

Le Président (M. Simard) : Sir, your time is over now. Votre temps est écoulé maintenant. Merci beaucoup pour votre contribution.

M. Heft (Joel) : O.K. Je m'excuse.

Le Président (M. Simard) : Non, non, non. Nous vous remercions, monsieur. Et en fait j'avais une question : Quelle heure est-il en Belgique à ce moment-ci?

M. Heft (Joel) : Oh! il est 9 h 15.

Le Président (M. Simard) : Wow! Bon. Alors, nous allons maintenant céder la parole à notre collègue le député de Vachon. Et nous entreprenons, donc, M. Heft, une période d'échange qui va durer un peu plus de 30 minutes. Différents députés de l'Assemblée nationale, de différentes formations politiques, s'adresseront à vous. M. le député de Vachon.

M. Lafrenière : Well, first of all, thank you so much, M. Heft, for being with us. We do appreciate that. Thank you for being here today. You don't try to escape reality.

M. Heft (Joel) : No, never.

M. Lafrenière : Ça va être la fin de la partie en anglais, M. Heft. Je vais parler en français pour le reste. Et je vais vous dire que, malheureusement, aujourd'hui, ça confirme un peu la prétention de certains de mes gens dans mon comté, qui me disent qu'ils ont de la difficulté d'être servis en français avec Equifax. Sur votre site Web, encore aujourd'hui, je suis allé faire des vérifications, il y a du franglais beaucoup. Et, sans mettre en cause votre service ou quoi que ce soit, il y a une chose qui est claire : pour l'accès à des services en français, il y a un petit peu de difficultés. Alors, je tenais à vous le redire aujourd'hui au nom des gens de chez moi, de Vachon.

Question technique, pour vous, M. Heft : Est-ce qu'il est vrai de dire que votre compagnie a accès à 70 % du marché? Donc, vous n'avez pas accès à toutes les informations, à toutes les transactions, c'est seulement 70 % du marché.

M. Heft (Joel) : No, it's... So, we do have, I think... Is it OK if I respond in English?

Le Président (M. Simard) : Oui, vous pouvez continuer, M. Heft, en anglais.

M. Heft (Joel) : Yes, OK. So, it is true that we have... I think you said 70% of the market share. I believe that was the number you gave. Please confirm.

M. Lafrenière : This is exactly what I said.

M. Heft (Joel) : OK, perfect. So, while that's true, it doesn't mean that we don't get the information on virtually 100% of the transactions, the credit adjudication, the loans, the mortgages taking place in Canada or in Québec in particular. Now, in Québec, I would argue that our market share is quite significantly higher than 70%. But that's neither here nor there for my answer. If you'll indulge, I could explain to you what I mean by that.

M. Lafrenière : Ça va aller, M. Heft, merci beaucoup. Est-ce qu'il est vrai aussi de dire que vous n'avez pas accès à l'information en temps réel? Est-ce que vous avez toujours ces transactions-là en temps réel?

M. Heft (Joel) : We receive trade data from credit... from lenders on a... There's no exact answer. It's either daily, weekly, or, in some cases, monthly, depending on the lender and the frequency at which they provide the information.

M. Lafrenière : Donc, monsieur...

M. Heft (Joel) : The alerts to the... Sorry.

• *(15 h 20)* •

M. Lafrenière : M. Heft, donc, si je comprends bien, il est possible que, dans mon compte... je suis un des individus qui a été touché par Desjardins, il est possible qu'il y ait une transaction et que je ne sois pas avisé en temps réel. Est-ce que c'est bien ça, M. Heft?

M. Heft (Joel) : Well, partially. You will be advised by us in real time when we receive the data from the lender. Does that make sense? I can go much deeper.

M. Lafrenière : Oui. Donc, ça peut être à la semaine, aux deux semaines ou au mois, comme vous avez expliqué. Parfait.

J'ai une autre question pour vous, M. Heft. Ce matin, nos collègues de l'opposition nous ont fait témoigner une dame qui avait eu un vol d'identité, son identité avait été volée, Mme Aubry. Et ce qu'on m'a rapporté, c'est que, si une personne se présente chez vous, chez Equifax, avec un vol d'identité, elle veut retrouver son identité — puis on sait que c'est très difficile, ça prend près de 80 heures pour régler son dossier — elle se fait répondre par Equifax qu'il n'y a rien à faire, on la réfère, donc, à la Commission d'accès à l'information.

Donc, la personne est victime, elle n'a rien fait de mal, est une victime d'un vol d'identité, et on n'est pas en mesure d'aller rétablir son score de crédit avec Equifax, il faut passer par la Commission d'accès à l'information. C'est ce que les victimes me rapportent. Puis j'aimerais comprendre pourquoi, parce qu'ils sont... c'est comme s'ils étaient victimisés deux fois : un, ils se sont fait voler leur identité, et, pour aller corriger ça, on leur dit : Attendez, votre crédit va aller mieux un jour.

M. Heft (Joel) : So, can I ask the question of the translator? I think it's easier for me to understand the question in French, it's very confusing to hear the question in French and English at the same time, so... I apologized in my initial comment and I'm going to ask the translator to please translate my English to French for the members of the commission. But I'll just listen to the question in French and answer in English. I can understand and, if I can't, I'll ask for an explanation. Would that be OK?

M. Lafrenière : Oui. Yes.

M. Heft (Joel) : OK. Thank you. It's just very confusing to hear it in both languages.

Le Président (M. Simard) : Voulez-vous répéter, M. le député de Vachon?

M. Lafrenière : You heard that one right? You want me to tell you that again?

M. Heft (Joel) : I believe the question... No, no, let me play it back and see if I got it into the two languages. I think you were talking about the specific instance were someone in your district had trouble both with their credit file and, potentially, identity theft. Did I catch that right? And...

M. Lafrenière : ...right.

M. Heft (Joel) : ...there were some delays... Pardon?

M. Lafrenière : You have that right. Actually, it's not even a delay, they've been sent to the Commission d'accès à l'information.

M. Heft (Joel) : Yes. So, the... It's incredibly... I could talk about the way the system should work. It's hard to talk about one consumer, but what I would offer personally is, if that consumer wanted to get in touch with me personally, I will make sure that they get... I can't do that for every consumer, but, if it's of importance to you, which it is, I will gladly make sure that I review their file with the appropriate people in Canada. Understanding that's not what I do in Canada, but it's important that consumers are treated... It sounds like an anomaly, and I'd be glad to step in and see what we can do.

M. Lafrenière : But to be honest with you, sir, I heard that numerous times, not only for that person. I used to be police officer for numerous years, and this is the way they've been answered. But I'm not going to get into details for that.

Une autre question pour vous, M. Heft : Pour vos employés... vous faites une vérification d'antécédents judiciaires à l'embauche de vos employés?

M. Heft (Joel) : Yes. I can tell you that, as an employee, I've gone through... I mean, I was hired 23 years ago, I went through rigorous background checks then. Our background checks are more rigorous today, way more rigorous than they were then. I wouldn't be the right person to be able to walk you through, chapter and verse, what that is, but I can tell you that we do put every employee through substantial background checks.

M. Lafrenière : Parfait. C'est fait à l'embauche. Est-ce que c'est fait périodiquement pendant le travail? Est-ce que vous le refaites une fois que les employés travaillent pour vous?

M. Heft (Joel) : I believe we do, yes.

M. Lafrenière : Vous le croyez ou vous êtes sûr, M. Heft?

M. Heft (Joel) : I believe. I would be more than happy to get back to you with that, I just... Again, it's not what I do day to day, so I'm doing my best to give you a response. But I can't give you the chapter and verse on that, I just don't know.

M. Lafrenière : Parfait. Parce que la réalité fait en sorte que, des fois, on peut embaucher une personne qui a un bon passé judiciaire, et, par la suite, il peut commettre des actes criminels. Et je voulais savoir de quelle façon votre entreprise, étant donné que vous êtes en lien avec de l'information très sensible... de quelle façon on vérifie le passé de nos employés pour s'assurer qu'il n'y a pas personne qui est accusé, exemple, de fraude. Parce que je pense que j'ai déjà vu, dans une revue de presse, des cas d'employés d'Equifax qui ont été accusés.

M. Heft (Joel) : I'm not aware of those. I'm not doubting you, I'm just saying I'm not aware of anywhere where an employee of Equifax was accused of fraud. Again, I'm not saying you're wrong, I'm just not aware of it. And it would be surprising to me but I just... I'm not aware of that.

M. Lafrenière : That will be the end of my question, but I strongly suggest that you will look into that. Thank you, sir.

M. Heft (Joel) : You have my absolute assurance.

M. Lafrenière : Thank you.

Le Président (M. Simard) : Merci beaucoup, M. le député de Vachon. Mme la députée de Charlevoix—Côte-de-Beaupré.

Mme Foster : Bonjour. Merci beaucoup de votre présence ici, aujourd'hui. Première question. Vous êtes conscient que vous allez devoir offrir un service d'alerte au crédit à tous ces clients de Desjardins. Il y a sûrement un bon nombre d'entre eux qui en ont encore pour 50 ans à vivre. Est-ce que vous êtes prêts à cela, comme organisation? Et quels moyens prenez-vous pour y faire face?

M. Heft (Joel) : Sorry. Can I get a translation of the question? I apologize. Can I get a translation of that question?

Le Président (M. Simard) : Alors, pourriez-vous, s'il vous plaît, Mme la députée, répéter votre question pour assurer une traduction adéquate?

Mme Foster : O.K. Vous êtes conscient que vous allez devoir offrir les services de clients Desjardins à vie. Pour beaucoup de ces clients-là, ils en ont encore pour 40, 50 ans à vivre. Donc, est-ce que vous êtes prêts à faire face à cela, en tant qu'organisation? Et quels sont les moyens que vous prenez?

M. Heft (Joel) : OK, I understand the question now, it's about providing service for life, and some people will live another 40 or 50 years. What are we doing? Is that the question?

Mme Foster : Oui, le volume supplémentaire que ça va générer sur 40 ans.

M. Heft (Joel) : OK. So, yes, I mean... So, there's two offerings, one I can speak to, one I really only know peripherally. The offering of the Equifax credit monitoring service is for five years, and then it will expire. Now, to put that in context, five years is above and beyond pretty much anything I've ever seen, and I run... you know, I've been running this business for the last five years. There's is a secondary offering that Desjardins is offering, and I can't speak to the conditions surrounding that one. But ours is being offered to those who take it for five years.

Le Président (M. Simard) : Merci. Mme la députée, auriez-vous une autre question?

Mme Foster : Est-ce qu'il y avait un moyen, pour Desjardins, de pouvoir inscrire directement au service d'alerte de crédit les clients? Pourquoi est-ce que ce sont les clients qui doivent impérativement faire la démarche eux-mêmes de s'inscrire? Est-ce que le problème était de votre côté? Qui a demandé quoi dans cette histoire-là? Pourquoi c'est le consommateur qui doit faire les démarches fastidieuses pour s'inscrire au service?

M. Heft (Joel) : That's actually a really good question, and thank you for asking it. We've talked about this one a lot. So, the reason... there's a few reasons, but number one, the worse thing you want to do, in a case of a data incident like this, is allow a fraudster, a bad person to be able to get access to the real person's credit file. Are you with me so far? Am I being clear so far?

Mme Foster : Oui.

M. Heft (Joel) : OK. So, part of what we do is, if you've ever had access to our service, before you get access, you go through what's called authentication, and authentication is a number of questions back and forth to assure that you are really you. So, there are questions that you will answer to prove that you are you. That's number one. Without authentication, we would run a big risk of higher fraud because we wouldn't have any idea that the person getting the file is actually the person they say they are.

The second reason is there's a consent aspect. Some people just don't want it, they don't want to know about it. It's a personal choice. I don't agree with it. I have it, my wife has it, my children have it, but there are people that do not want it. And we, or any of our customers, wouldn't be in a position to force it to them because, frankly, that would be taking their privacy rights of not wanting it, so it's an opt in versus an opt out.

• *(15 h 30)* •

Le Président (M. Simard) : Mme la députée de Charlevoix, cela vous satisfait? M. le député de Saint-Jérôme, il vous reste 3 min 40 s, cher collègue.

M. Chassin : D'accord. Merci, M. le Président. Merci, M. Heft.

Dans votre rapport annuel — et je cite — vous mentionnez : «We understand that credit reporting agencies like Equifax have an important responsibility to protect the personal data we hold.» Évidemment, vous n'êtes pas sans savoir que ce qui nous occupe aujourd'hui, c'est un événement où un vol de données est survenu chez Desjardins. Et, vous-même ayant été victimes d'une fuite de données en 2017, à quel point vous sentez-vous aujourd'hui mieux outillés qu'en 2017 pour faire face à cette réalité?

M. Heft (Joel) : That is another really good question, and I thank you for asking that. When our CEO presented in front of... I think it was a Senate committee about a year ago, he laid out the $1,250,000,000 that we have spent or will spend from 2017 until the end of 2021 to absolutely overhaul and, you know, strengthen every system related to our business. We have put substantial time, substantial effort and a tremendous degree of seriousness, professionalism and, frankly, the absolute best talent available into meeting exactly the quote you just read me. So, I thank you for asking because, listen, everybody would wish it didn't have...

M. Chassin : Au-delà des moyens...

M. Heft (Joel) : Sorry.

M. Chassin : Let me say this in English. Do you feel confident that you've reduced substantially the risk of another event like this?

M. Heft (Joel) : Thank you for asking me in English. I feel incredibly confident that we have. And we're on a path to being even better than we are today. But, yes, the answer to your question is absolutely, yes.

M. Chassin : ...ask for how long are you doing business in Québec or have you been doing business?

M. Heft (Joel) : We have been doing business in Québec... I will say that it's roughly 90 years.

M. Chassin : So, basically, you have a 70% market share. You've been doing business in Québec for a long time. Can you explain, sir, why Equifax struggles to provide service in French, the only official language in Québec?

M. Heft (Joel) : Well, I mean, there's two points in time that I'd like to give to be able to answer your question. I've said in my opening comments that due to the overwhelming response to the offering in the case we're talking about today, for a period of time, we did not meet our incredibly high standards to service — let's just use — the French canadians, Quebeckers, in French for that period of time.

M. Chassin : Well, do you feel that you will be able today to say that you will update at least your Web site in French?

Le Président (M. Simard) : Très bien.

M. Heft (Joel) : Absolutely, yes.

Le Président (M. Simard) : Merci.

M. Heft (Joel) : Now, to finish my answer, though, if I can just finish, you know, for the period...

Le Président (M. Simard) : No, sorry, sir.

M. Heft (Joel) : OK.

Le Président (M. Simard) : Nous allons changer. M. le député de Robert-Baldwin, à vous la parole.

M. Leitão : Très bien. Merci beaucoup.

For the purposes of efficiency, I will conduct our exchange in English so we can go a little faster, since our time is limited. Just to check something quickly with you, you said you've been doing business in Québec for nine years or 90?

M. Heft (Joel) : 90.

M. Leitão : 90.

M. Heft (Joel) : Quatre-vingt-dix.

M. Leitão : 90 years, OK, that changes things. Nine years, we could understand the difficulty in providing services in French, but 90, well, it's quite a long time. But anyways.

You mentioned as well that, from June to October, you increased the number of, you know, employees answering questions from the citizens by 1,000%. That's fine, but what does that translate into actual numbers of people? You went from one to 10, you went from 10 to 100?

M. Heft (Joel) : No. I'm going to give you general because I don't have the exact numbers as of today in front of me, but we've gone from approximately 40 to over 400.

M. Leitão : OK. Thank you.

M. Heft (Joel) : And the thing that I want to point out to you though...

M. Leitão : OK, go ahead.

M. Heft (Joel) : Yes, sorry. Yes. I want to point out that again we have... I have already apologized for the period of time post-Desjardins. But, if you want to look at the 90 years of servicing any language in Canada through our consumer call centers, there has been... I mean, we keep stats every minute of every day, as you can imagine. There has been exemplary service up to the Desjardins breach. And, frankly, for a considerable amount of time now... I could tell you that today, just today, we were answering... and this has been for a least a month and a half, we have been answering French and English calls in under five seconds. So, you know, it doesn't...

M. Leitão : OK, thank you, thank you. Just on another issue, and, again, I'm sorry, I have to go quick because our time is limited, but, on another issue, you say that one of the services... Well, you offer several services, one of them being a notification, credit monitoring, and all that. How do you communicate with people? Is it by phone, by Internet? How is that done?

M. Heft (Joel) : If I could ask in what context because we do mail...

M. Leitão : In the context of Desjardins, so the five-year protection. If you do notice there's something untowards in somebody's credit report, you contact the citizen how, by phone, by Internet?

M. Heft (Joel) : By Internet, so that it's real time.

M. Leitão : OK, by Internet. Of course, you're aware that not everybody has access to Internet, and particularly the more vulnerable people, seniors, it's a bit more difficult, which brings me to my next question which was raised by one of my colleagues just before. I propose to you that we should perhaps reverse the process, in the sense that rather then being the citizens that contact you and have to register, again I didn't quite follow the reasoning, why don't you deal directly with the financial institution, Desjardins, so that Desjardins will provide you with the necessary information for you to start the monitoring? Why do you have to have the individuals contact you to register?

M. Heft (Joel) : Well... and the two answers I gave, I'll just summarize them quickly because I know we're under the gun. Number one is for the security and the protection of the consumers themselves, and number two is the product requires consent. The consumer needs to consent. We're not even allowed to monitor their file without their consent. So, as long as the Québec, canadian privacy laws stay the way they are, the consumer's consent is required for us to provide the service.

M. Leitão : OK, which brings me to another question, which is, as I'm sure you know or, at least, I'm under that impression, the data that you hold, in fact, is not yours. I mean, it's ours. It's my data. It's the individual's personal information. You manage that data. So, again, how could we reverse the process so that it's Equifax that monitors the situation, but only at the request of the individual, so, if somebody else asks for some sort of a credit update, that will not be processed until and unless the citizen approves?

M. Heft (Joel) : I understand that there's a parallel proceeding going on in the province of Québec where they're looking at the Credit Bureau. I'm not part of it. I have no, you know, stake in it. But, you know, I think that that question is a very good one, should be asked hopefully at that level versus this one because I just... You know, I'm not in a position to respond to that. All I know is that the way it stands...

• (15 h 40) •

M. Leitão : If that were to be decided by the Legislature, then, obviously, for you, it wouldn't be, you know, a technical problem to follow that instruction.

M. Heft (Joel) : Yes. It may be a security problem. But, you know, these are all things that, I think, with the fullness of time, we can discuss and have really fruitful and... I think the one thing is, and I hear it in all of your voices, what we're all trying to do is find the very best solution for impacted consumers. And so I think we all agree on that. And I think that what you're raising is a very, very honest, very solid, very well thought out thought that needs to be or should be vetted out in a different forum.

M. Leitão : Thank you. One last question from my side because I want to clarify something that you said earlier, and I want to make sur that we all understand. One of my colleagues mentioned that a number of people affected by the data breach at Desjardins are fairly young, and therefore they'll be around for a number of years. The service you provide is for five years only. Is that correct?

M. Heft (Joel) : It's for five years from the day the person signs up, yes.

M. Leitão : Correct. What happens after? What happens on year six?

M. Heft (Joel) : In year six, our service would lapse. It would no longer be, you know, valid, unless the consumer specifically liked it so much that they wanted to keep it up. But our relationship with the consumer is for a five-year term.

M. Leitão : And finally I understand that this service is available, obviously, but for a price. You're not providing these additional protection services free of charge. In this case, it's Desjardins that is paying for the five years. But, if a consumer wants to maintain the service beyond five years, he would have to negotiate with you some sort of fee or something?

M. Heft (Joel) : You are correct.

M. Leitão : OK. Thank you.

Le Président (M. Simard) : Mme la députée de Saint-Laurent, je vous avise qu'il vous reste 2 min 44 s.

Mme Rizqy : Pour ce qui est des scores de crédit, vous ne croyez pas que, pour tous ceux qui sont affectés par Desjardins, par Capital One, que vous devriez peut-être revoir leur score de crédit parce que ça a un effet direct sur les prêts qui leur sont consentis puisqu'ils paient, par conséquent, lorsque leur cote de crédit est diminuée, des montants d'intérêt supplémentaires?

M. Heft (Joel) : So let me play the question back. Will the consumer score be affected as result of the breach, or Capital One breach, or Desjardins, or any breach? Was that the question?

Mme Rizqy : Any breach.

M. Heft (Joel) : Yes. No, I mean, it's hard to say without... Scores are very complicated things for someone like me to explain just because I don't... You know, it's not what I do every day, but they should...

Mme Rizqy : ...president of Equifax, you know that, right? And I think credit scores is something that is a core business for you. And, when we have right now a woman who has two mortgages that she never contracted and now she has to fight with Equifax to make sure that that can go away, do you think this is fair?

And, in the meantime, if I can go back, March 2017, you were first alerted that you had a breach. Back in May, first data breach, and you went only public in September 2017. In the meantime, you have three top executives who decided to sell their shares. For a business who has $17 billion at the stock market, I think you should be aware what is your core business.

M. Heft (Joel) : Well, I'm aware of scores. What I would say is I don't know enough about any particular individual because everybody's score is different. I don't know anything... I don't know enough about any particular individual to be able to respond to that question on an individual basis. Will a person's credit score generally be affected by the fact that they may have had a Capital One card and were part of the Capital One breach? If the story stopped right there, the answer would be most likely no. If bad stuff happened as a result of... it's not even any data breach, it's anyone, then there is a chance that, you know, if somebody applies for credit...

Mme Rizqy : Excuse me. I have to reclaim my time because time is very limited. I'm very sorry about that.

M. Heft (Joel) : Yes. Sorry.

Mme Rizqy : But we have people here, in Québec... lives are devastated because now they have to fight with Equifax to just wash away all the mortgages that were wrongfully contracted. Do you have a fast track to help all the Quebeckers who now have to fight to make sure that their credit score is back to normal?

Le Président (M. Simard) : Malheureusement, cela met fin à votre...

Mme Rizqy : That can... yes or no. A fast track?

M. Heft (Joel) : Well, if their...

Le Président (M. Simard) : Très bien. Nous allons devoir passer...

M. Heft (Joel) : Let me just answer. In the context of what we're talking about today...

Le Président (M. Simard) : Thank you, sir. Your time is over.

M. Heft (Joel) : ...if they are on a Desjardins product, they have restoration services.

Le Président (M. Simard) : OK, thank you, sir. Maintenant, je cède la parole au député de Gouin, 2 min 40 s.

M. Nadeau-Dubois : Merci. Bonjour, M. Heft. Permettez-moi de vous partager — je le ferais si vous étiez ici en personne, je vais le faire même si vous êtes à distance — ma déception à l'effet qu'Equifax, qui est censée être responsable de la protection des données de maintenant plus de 4 millions de Québécois qui ont été victimes de cette brèche de données... déçu, donc, qu'Equifax n'ait pas jugé pertinent de nous envoyer quelqu'un ici en personne en mesure de répondre avec précision aux questions des députés de l'Assemblée nationale du Québec.

Ceci étant dit, j'ai une question très précise pour vous. Êtes-vous capable de me dire, à l'heure actuelle, combien il y a d'employés dans vos bureaux de Montréal qui desservent l'ensemble du Québec pour donner des services aux gens, aux clients de Desjardins qui ont été victimes de la brèche de données dont nous discutons aujourd'hui?

M. Heft (Joel) : In the Montréal office specifically, I can't answer that question. I do not know.

M. Nadeau-Dubois : Au Québec?

M. Heft (Joel) : I can't... This is a question that we can certainly get from our operations team, but I don't run that team. I don't have access to, you know, those numbers. I apologize. I just don't know the answer to that question.

M. Nadeau-Dubois : Merci. Lorsque Desjardins vous a fait part qu'ils avaient été l'objet d'un vol de données, pouvez-vous nous expliquer pourquoi Equifax n'a pas simplement inscrit une alerte de fraude sur le dossier de crédit des victimes? À ce que je sache, c'est une démarche qui est gratuite et qui est obligatoire en vertu de la loi.

M. Heft (Joel) : Well, any consumer can call us and put a fraud alert on their file. We couldn't put it on for them. They need to put it on themselves.

M. Nadeau-Dubois : Est-ce que vous pouvez nous expliquer pourquoi, quand plusieurs consommateurs québécois tentent d'appeler, l'appel est redirigé vers un centre d'appel situé en Inde?

M. Heft (Joel) : I'm interpreting that your question is : Why do people get an agent that's located in India?

M. Nadeau-Dubois : ...the question.

M. Heft (Joel) : Yes. I know that we do have call centers, because we operate many hours during the day, that are located in various jurisdictions, and I would gather that there is a possibility that some of the calls could be answered from somebody located in India.

M. Nadeau-Dubois : Est-ce que vous jugez que c'est sécuritaire dans le contexte actuel?

M. Heft (Joel) : Is it secure? Absolutely. Absolutely. Any facility that is handling our consumers has to meet our own security standards.

Le Président (M. Simard) : Très bien. Merci. Je cède maintenant la parole au député de Jonquière.

M. Gaudreault : Oui. Alors, merci beaucoup d'être avec nous, M. Heft.

Alors, moi, j'ai un gros malaise parce que j'ai l'impression que plus il y a de fuites, plus c'est payant pour Equifax. Alors, vous comprenez que, comme citoyen et comme consommateur, ça me cause des problèmes parce que vous avez, comme entreprise, augmenté vos revenus de façon incroyable cette année à cause, justement, de la multiplication des fuites de données comme chez Desjardins ou comme chez Capital One. Par exemple, en sol canadien, Equifax a récolté 39 millions de juillet à septembre dernier, et, depuis janvier, la cagnotte s'élève à 114,9 millions de dollars. Donc, plus il y a de fuites, plus c'est intéressant pour vous, alors que, moi, ce qui m'intéresse, c'est vraiment la protection des données des citoyens, la protection des données des consommateurs. Donc, parfois, j'en viens à me dire : Est-ce que c'est la meilleure façon de protéger les données des consommateurs de faire affaire avec des entreprises qui font de l'argent avec ce système-là? Donc, c'est un genre de paradoxe que j'ai de la difficulté à m'expliquer.

Mais, quand même, vous êtes présents partout à travers le monde. Avec votre expérience, êtes-vous capable de nous donner des exemples des meilleures pratiques que vous avez vues, à travers le monde, sur la protection des données personnelles, de l'identité numérique à travers le monde? On s'attend toujours à des exemples venant de la Scandinavie, là. Mais est-ce qu'il y a d'autres exemples à travers le monde qui peuvent nous inspirer, nous, comme parlementaires, pour pouvoir modifier la loi, toujours dans un souci de protection, d'abord et avant tout, des citoyens et des données personnelles? Merci.

• *(15 h 50)* •

M. Heft (Joel) : It's a great question. It's clearly something that... As I have the opportunity to travel around the world, many, many, many governments like yours are looking at and trying to, you know, figure out what is the best way to protect the consumers, citizens. I'm not sure anybody... I think it's really going to take a concerted effort between government, business and consumers. I think you have to have all three who really need to study this a lot harder and come up with a solution that I haven't seen yet. I have not seen it yet.

Le Président (M. Simard) : Très bien. Alors, M. Heft, je tenais à vous remercier d'avoir participé à cette commission. Au revoir.

M. Heft (Joel) : Au revoir. Merci beaucoup.

Le Président (M. Simard) : Alors, voilà. Nous allons donc suspendre nos travaux, le temps de faire place à nos prochains invités.

(Suspension de la séance à 15 h 51)

(Reprise à 15 h 56)

Le Président (M. Simard) : Alors, très chers amis, à l'ordre, s'il vous plaît! Avant de reprendre nos travaux...

Des voix : ...

Le Président (M. Simard) : À l'ordre, s'il vous plaît! Merci beaucoup. Alors, avant de reprendre nos travaux, je tenais à souligner la présence dans cette salle d'un ancien parlementaire qui a siégé ici très longtemps, qui a notamment été chef de l'opposition officielle, M. Guy Chevrette. Soyez le bienvenu, monsieur.

Très bien. Alors, nous allons recevoir... nous recevons, en fait, des représentants de la l'Association des banquiers canadiens. Madame, monsieur, soyez les bienvenus. Auriez-vous d'abord l'amabilité de vous présenter? Et vous savez que vous disposez d'une période de présentation de 10 minutes.

Association des banquiers canadiens (ABC)

M. Prud'homme (Eric) : Alors, bonjour. Permettez-moi de vous remercier pour cette occasion que vous m'offrez aujourd'hui de m'adresser à vous. Alors, mon nom est Eric Prud'homme. Je suis directeur général à la direction du Québec de l'Association des banquiers canadiens. À mes côtés se trouve ma collègue Angelina Mason, avocate en chef et vice-présidente des affaires juridiques à l'association des banquiers.

L'association est la voix de 70 banques membres, soit des banques canadiennes ainsi que des filiales et des succursales de banques étrangères, exerçant des activités au Canada. Les banques, qui emploient 275 000 personnes au Canada, dont près de 45 000 au Québec, contribuent à l'essor et à la prospérité économique du pays. L'ABC, l'association des banquiers, préconise l'adoption de politiques publiques favorisant le maintien d'un système bancaire solide et dynamique, capable d'aider les citoyens à atteindre leurs objectifs financiers.

Nous tenons à préciser que le Mouvement des caisses Desjardins n'est pas membre de l'association des banquiers, étant donné que l'association représente des institutions bancaires sous réglementation fédérale, assujetties à la Loi sur les banques.

Les banques sont conscientes de la confiance que les consommateurs leur accordent pour garder en sécurité les dépôts ainsi que les renseignements personnels et financiers. Elles emploient des équipes de professionnels hautement qualifiés en matière de cybersécurité et de protection des données et investissent massivement dans la technologie et

les mesures de sécurité. Entre 2007 et 2017, les six plus grandes banques canadiennes ont investi 84,5 milliards dans la technologie, dont une grande partie en solutions destinées aux mesures de sécurité.

Malgré l'évolution soutenue des cybermenaces, les banques maintiennent un excellent bilan en matière de protection de leurs systèmes et de leurs clients. À titre d'institution financière sous réglementation fédérale, les membres de l'association des banquiers sont déjà assujettis à des exigences législatives et réglementaires strictes en matière de cybersécurité et de protection des renseignements personnels. La protection des renseignements personnels ayant toujours été une pierre angulaire des activités bancaires, des mesures solides à cette fin font partie intégrante des politiques et des pratiques des banques depuis longtemps.

Toutes les banques ont prévu une politique en matière de renseignements personnels et ont nommé un responsable de la conformité pour veiller à ce que cette politique soit respectée et que les renseignements personnels des clients soient protégés et tenus à jour, comme l'exige la Loi sur la protection des renseignements personnels et les documents électroniques. Je vais y référer par la suite en utilisant l'expression «loi fédérale».

• *(16 heures)* •

Alors, nous sommes d'avis que la loi fédérale fonctionne bien. Elle a permis d'atteindre un bon équilibre entre la protection des renseignements personnels d'un individu et l'usage légitime des renseignements personnels par les organisations. Basée sur des principes et technologiquement neutre, la loi fédérale fournit les dispositions nécessaires pour encadrer les innovations, les nouvelles technologies et les nouveaux modèles de gestion.

Dans les très rares cas de fuite de données, les banques sont tenues de signaler certaines atteintes à la sécurité mettant en cause des données personnelles au Commissariat à la protection de la vie privée du Canada et d'aviser les personnes affectées par l'atteinte en question ainsi que les organisations susceptibles d'atténuer les dommages causés par l'incident. Dans l'avis aux personnes atteintes, les banques doivent inclure suffisamment d'information pour permettre à ces personnes de comprendre l'importance pour elles de l'atteinte et de prendre, si cela est possible, des mesures en vue de réduire le risque de préjudice qui pourrait en résulter ou d'atténuer un tel préjudice. Dans les cas où l'atteinte pourra produire d'importants dommages, les banques surveillent les activités sur le compte afin de détecter un piratage de renseignements personnels potentiel ou actuel et d'arrêter toute activité non autorisée, le cas échéant. Par ailleurs, dans certains cas, les banques indemnisent le titulaire du compte pour la perte de fonds due à des opérations non autorisées. Également, les banques font appel aux agences de crédit afin de réduire le risque de dommages.

Parallèlement, les banques sont assujetties à l'obligation de signaler les incidents liés à la technologie et à la cybersécurité établis par le Bureau du Surintendant des institutions financières — «bureau du surintendant» pour la suite, c'est moins long. Lorsqu'une institution financière sous réglementation fédérale fait face à un incident lié à la technologie ou à la cybersécurité qui pourrait avoir des conséquences importantes sur ses activités habituelles, elle est tenue de le signaler au bureau du surintendant dans un intervalle de 72 heures. Aussi, les banques doivent communiquer les mises à jour au bureau du surintendant à mesure que de nouveaux renseignements deviennent disponibles, notamment au sujet de leur plan de redressement à court et à long terme, et lui soumettre un compte rendu sur les leçons apprises.

La cybersécurité et la résilience sont des priorités collectives pour les banques. Il n'y a aucun avantage concurrentiel à travailler individuellement. Avec l'augmentation des opérations effectuées électroniquement, les réseaux et les systèmes deviennent de plus en plus interconnectés, ce qui amplifie la collaboration entre les banques, les gouvernements, les forces de l'ordre et d'autres secteurs. Aujourd'hui, au Canada, 72 % des consommateurs utilisent principalement les services bancaires en ligne et mobiles, une hausse par rapport aux 52 % d'il y a tout juste quatre ans.

Les banques ont activement participé aux consultations du gouvernement fédéral qui ont mené au développement de la Stratégie nationale de cybersécurité et appuient fermement la démarche intégrée public-privé envers la cybersécurité et la cyberrésilience. Les banques maintiennent leur collaboration avec les organismes gouvernementaux dans l'échange de connaissances récentes, y compris le nouveau Centre canadien pour la cybersécurité, et participent activement à des projets avec d'autres organisations comme l'Échange canadien des menaces cybernétiques. Ces actions favorisent grandement la collaboration entre les secteurs public et privé, assurent la protection des consommateurs et, par conséquent, mènent à la création d'un cyberenvironnement plus résilient et plus sécurisé.

Pour conclure, j'aimerais rappeler que les banques attachent une grande importance à la protection des données personnelles des citoyens. En effet, parallèlement à l'évolution rapide de la technologie et à l'adoption des outils bancaires numériques par un nombre croissant de consommateurs, les banques poursuivent leur recherche de solutions technologiques susceptibles d'améliorer la protection des renseignements personnels de leurs clients. Un simple exemple serait les solutions d'identification et d'authentification numérique.

Je vous remercie pour votre temps. Nous serons heureux de répondre à vos questions.

Le Président (M. Simard) : Alors, merci beaucoup, cher monsieur. Je cède immédiatement la parole au député de Rousseau.

M. Thouin : Merci. Bonjour, Mme Mason, M. Prud'homme. Merci d'être ici aujourd'hui.

Évidemment, le dossier principal, là, à la base de cette rencontre, c'est le dossier des fuites, là, chez Desjardins. Donc, après que la fuite de données ait été rendue publique, Desjardins a réagi rapidement en offrant à plusieurs de ses... plusieurs services à leurs clients. Le plus connu de ces services-là et qui a été le plus discuté, c'est le service de surveillance de crédit offert par Equifax. D'ailleurs, ils viennent de nous en parler il n'y a pas si longtemps. Qu'est-ce que vous pensez de ce service-là?

M. Prud'homme (Eric) : Alors, moi, ce que je peux vous dire, c'est qu'au niveau de la cybersécurité, ce qui est important, et c'est ce qu'on a dit à l'Association des banquiers canadiens lors des consultations au niveau fédéral sur la

stratégie nationale en matière de cybersécurité, c'est le fait de pouvoir partager et discuter avec tous les intervenants de l'écosystème financier. Dans le domaine... Au niveau du secteur bancaire, ce sont des milliards de dollars qui sont investis au niveau de la technologie, incluant les systèmes de cybersécurité.

Donc, c'est le partage d'information, être en mesure, justement, de pouvoir parler aux différents acteurs de la société, qui évoluent dans le domaine de la cybersécurité et dans le domaine financier.

M. Thouin : Est-ce que, autre que ce système-là qu'ils ont mis en place, là, de surveillance de crédit, là, plus précisément, est-ce qu'il y a d'autres types de protection que vous auriez proposé de mettre en place dans une des autres institutions, si ça arrivait?

M. Prud'homme (Eric) : Alors, d'abord, moi, je dois vous dire une chose, là, c'est... La protection des données personnelles, pour les banques, là, ça fait partie de leur ADN, O.K.? Première chose.

Deuxième chose, dans mon entourage... moi, je vis au Québec, je suis ici. Dans mon entourage, il y a beaucoup de personnes proches de moi qui ont été touchées. Donc, on est très conscients de ça, et je ne peux pas parler au nom de Desjardins. Je ne représente pas Desjardins, Desjardins n'est pas une banque. Mais, moi, ce que je peux vous dire, ce que je sais de l'industrie bancaire, c'est que tout est mis en place, justement, pour que des choses comme ça ne puissent pas se produire.

D'abord, on a des mesures... on a des systèmes d'alerte, O.K., au niveau... À partir du moment où un employé se mettrait à tenter d'utiliser de l'information à laquelle il n'a pas accès, il y a des drapeaux rouges qui vont se lever, puis on va agir automatiquement. Ça, c'est une chose.

Maintenant, au niveau physique, il y a des mesures physiques qui sont en place. Ce n'est pas tout le monde qui a accès aux buildings où il y a de l'information sensible qui est entreposée. Ce n'est pas tout le monde qui a accès aux équipements, en plus des systèmes, bien sûr, au niveau de la technologie, les coupe-feux et ces choses-là, et l'information est classée selon son niveau de sensibilité.

M. Thouin : ...M. Prud'homme, je suis plus dans après. Tu sais, une fois que c'est arrivé, là, comment on gère ça? Là, Desjardins a décidé de mettre ça dans les mains d'Equifax, mais pourquoi ça n'a pas été géré à l'interne? Pourquoi ce n'est pas à l'interne directement qui offre le service de protection, de surveillance du crédit, par exemple?

M. Prud'homme (Eric) : Bon, alors, écoutez, moi, encore une fois, je ne vais pas parler au nom de Desjardins, je vais vous dire ce qu'il se fait dans l'industrie bancaire.

Je l'ai mentionné lors de notre présentation, à partir du moment, dans le système bancaire, où il y aurait une fuite de données ou un vol de données personnelles, on a l'obligation d'aviser le Commissariat à la protection de la vie privée du Canada, O.K.? Et qu'est-ce qu'on fait, à ce moment-là? On avise et puis on va aviser aussi les gens qui ont potentiellement été touchés par ça. Maintenant, ces gens-là, dans le système bancaire, bien sûr, s'ils n'ont pas partagé... qu'ils n'ont pas participé à cette fuite de données là, sont indemnisés. On les accompagne, tous les efforts sont mis, des employés et des banques, pour les soutenir dans ces moments difficiles là. Encore là, je le rappelle, il y a des gens près de moi qui ont été touchés ici par ces choses-là, donc je peux très bien comprendre que ce n'est pas des situations faciles.

Et, oui, on va aussi avoir recours, dans certains cas, aux bureaux de crédit pour suivre l'évolution des choses. Et aussi, les comptes qui auraient pu être affectés, on va, en plus de tous les systèmes qu'on a en place... il faut comprendre qu'on a des systèmes en place, là, c'est plusieurs couches de systèmes de sécurité, une par-dessus l'autre, O.K.? Et, excusez l'expression, là, mais c'est ça, et voilà, donc on est là... On est là pour les consommateurs, et bien évident qu'on est là pour les consommateurs, parce que les banques sont dans une relation à long terme et tout est basé sur la confiance dans les relations avec les consommateurs.

M. Thouin : Dernière question très rapide, facile, oui ou non. Donc, vous avez dit tantôt que, dans des très rares cas de fuites de données dans notre système bancaire, là, avec les banques à charte fédérale... Question : Est-ce que Capital One est membre de l'ABC?

M. Prud'homme (Eric) : Oui, Capital One est membre de l'ABC.

M. Thouin : Merci.

Le Président (M. Simard) : Merci beaucoup. M. le député de Vanier.

M. Asselin : Merci, M. le Président. M. Prud'homme, Me Mason, je suis quand même curieux de savoir, si Desjardins avait été membre de l'ABC, auriez-vous réagi de la même façon que Desjardins l'a fait?

M. Prud'homme (Eric) : Alors, j'ai déjà un petit peu commencé à expliquer. Nous, au niveau fédéral, là, la première chose, O.K., on parle... Vous parlez de fuites de données, c'est bien ça?

M. Asselin : Oui, oui.

• *(16 h 10)* •

M. Prud'homme (Eric) : O.K. Moi, je vais vous parler au niveau fédéral, O.K., qu'est-ce qui se passe s'il y avait une fuite de données chez une banque.

Bon, d'abord, il faut informer — je me répète, mais je vais le dire — le Commissariat à la protection de la vie privée du Canada. On avise les personnes qui ont potentiellement pu être touchées...

M. Asselin : ...vous avez l'impression que ça n'a pas été fait?

M. Prud'homme (Eric) : Ah! ce n'est pas ça que je dis, là. Moi, je suis en train de vous expliquer, si vous voulez... Alors, ça, c'est la première étape, commissariat. Il y a une ligne directrice aussi, auprès du Bureau du Surintendant des institutions financières, en ce qui concerne les incidents qui touchent les systèmes technologiques ou de cybersécurité. Encore là, on est obligés... il faut agir le plus tôt possible puis dans un délai maximum de 72 heures pour aviser le Bureau du Surintendant des institutions financières. Et il faut prendre les démarches, justement, pour ne pas que des choses comme ça se reproduisent. Mais jamais on ne laisse tomber les clients dans le secteur bancaire. On est là, on les accompagne et puis on les indemnise.

M. Asselin : Est-ce que je peux prendre le risque de vous demander : Ce que vous venez d'entendre, là, avant vous, comment vous trouvez ça?

M. Prud'homme (Eric) : Bien, écoutez, d'abord, j'étais présent seulement pour quelques minutes. Alors, moi, ce que je peux vous dire, ce qui est important, c'est qu'un exercice comme aujourd'hui... puis c'est ça, la cybersécurité, c'est qu'on puisse écouter et, comment dire, partager les meilleures pratiques entre les différents intervenants du secteur bancaire.

Et là-dessus, peut-être, je peux vous dire que, nous, à chaque année, l'Association des banquiers canadiens... Vous allez me demander : Mais qu'est-ce que vous faites, justement? Bien, on essaie toujours d'être au-delà des systèmes les plus performants. Et on organise un sommet sur la cybersécurité, avec des experts qui viennent de partout, du monde entier, une journée complète où on fait un genre, excusez-moi l'anglicisme, mais un genre de brainstorming sur les meilleures pratiques, les meilleurs systèmes en place. Donc, c'est ça, on a tous un rôle à jouer dans l'écosystème financier.

M. Asselin : Merci beaucoup.

Le Président (M. Simard) : Merci à vous, M. le député de Vanier. M. le député de Saint-Jérôme, il vous reste 8 min 30 s.

M. Chassin : Est-ce que ce n'est pas le député de Vachon qui prenait la suite, M. le Président?

Le Président (M. Simard) : Alors, M. le député de Vachon, c'est parce que vous êtes le plus loin, hein, puis j'ai de la difficulté à vous voir.

M. Lafrenière : Je suis loin de vous, je m'excuse...

Le Président (M. Simard) : Vous êtes trop petit. Alors, je vous laisse la parole.

M. Lafrenière : ...mais très près de nos invités. Merci beaucoup, M. Prud'homme, Mme Mason, merci d'être là aujourd'hui. J'ai quelques petites questions techniques. Lors de votre présentation, vous avez parlé de l'échange d'information, puis je veux vous amener là-dedans, puis je ne veux pas partir un débat Québec-Canada. Je ferais plaisir à certains de mes amis ici. Ce n'est pas ça que je veux faire du tout, mais je veux comprendre de quoi.

Vous m'avez parlé de l'information que vous transmettez, que vous avez l'obligation de transmettre du côté canadien. Qu'est-ce qu'il en est du côté du Québec? Est-ce que vous envoyez ça au centre de cyberdéfense du gouvernement du Québec? Est-ce que c'est partagé, à ce moment-là?

M. Prud'homme (Eric) : On est de juridiction fédérale, là. Donc, nous, on va aviser le surintendant des institutions financières, mais on va aviser aussi les intervenants pertinents dans le secteur. Donc, je mentionnais... Entre autres, on travaille avec les corps policiers. Donc, oui, on va informer les corps policiers.

M. Lafrenière : ...mais pas le centre de cyberdéfense.

M. Prud'homme (Eric) : Bien, on va travailler avec... au niveau, là... le centre d'échange de cybermenaces, au niveau fédéral, bien, tout autre intervenant où on est en mesure de transmettre de l'information. Ça peut être le Centre antifraude aussi. Vous me faites penser, justement, au niveau... dans le cadre des consultations, au niveau fédéral, sur l'établissement d'une stratégie nationale au niveau de la cybersécurité... On comprend aussi que, maintenant, au niveau de la Gendarmerie royale du Canada, il y a une unité spéciale dédiée à la cybersécurité. Donc, tout ça, c'est des choses positives qui sont en place, justement, pour que, collectivement, on puisse étudier ces questions.

M. Lafrenière : Notre temps est super limité. Je suis désolé, je vais y aller avec des questions rapides, comme dirait quelqu'un, en rafale, un peu. Donc, vous le partagez du côté canadien. Tantôt, vous nous avez dit que les caisses ne font pas partie de votre association. Est-ce que vous partagez l'information avec les caisses Desjardins?

M. Prud'homme (Eric) : Bon, je reviens un peu au niveau... On va parler avec les différents secteurs, différents joueurs clés du secteur financier. On va parler des grandes...

M. Lafrenière : ...précisément Desjardins?

M. Prud'homme (Eric) : Oui, on a des discussions sur les grandes tendances, sur qu'est-ce qui se passe dans l'industrie financière, avec tous les intervenants. Desjardins est un intervenant important au Québec.

M. Lafrenière : O.K. Puis je comprends, quand vous nous avez parlé tantôt des sommets, tout ça, mais je parle vraiment... Il arrive une crise, il y a une fuite de données du côté d'un de vos membres, l'association des banquiers. Est-ce que cette information-là que vous transmettez en 72 heures est transmise chez Desjardins et vice versa?

M. Prud'homme (Eric) : Bien, nos obligations sont de les transmettre au bureau, par exemple... au Commissariat à la protection de la vie privée du Canada. Dans certaines circonstances, ça touche les systèmes technologiques et la cybersécurité. Ça va être au Bureau du Surintendant des institutions financières. Après ça, dans les limites permises par la loi, on va transmettre des informations quand on le peut, quand c'est permis par la loi.

M. Lafrenière : Parfait. Et, si je résumais ça, entre Desjardins du côté provincial puis l'Association des banquiers, il n'y a pas de transfert d'information. J'ai bien compris?

M. Prud'homme (Eric) : On va avoir des discussions, on va avoir des dialogues, on va...

M. Lafrenière : Parfait. Autre question pour vous.

Mme Mason (Angelina) : Sorry, but can I assist? So there are operational components of our association where we would share information like that and we do share information like that with Desjardins.

What we have advocated for, under the privacy legislation, is broader powers to allow us to share for more than just fraud, but for financial crimes generally, to include cybersecurity. We have also advocated for changes in the law that help support more sharing in that context, in particular what we call a safe harbor, so that when you share information in that context, you're protected, so you don't lose privilege over documents that would otherwise be protected legally, so you're not accused of misrepresentation because of a potential actor that may have turned out not to be... a potential bad actor. But you are able to share in order to protect against the cyber threats.

M. Lafrenière : Parfait. Merci beaucoup. Tout à l'heure, vous nous avez parlé de meilleures pratiques que vous partagez, justement, dans vos sommets, dans les rencontres. Pour les employés du côté bancaire, on ne parlera pas de Desjardins du tout, mais, du côté bancaire, j'imagine qu'il y a des vérifications d'antécédents qui sont faites avant l'embauche.

M. Prud'homme (Eric) : Oui, tout à fait.

M. Lafrenière : Est-ce qu'il y en a qui sont faites pendant que l'employé est en entreprise?

M. Prud'homme (Eric) : Oui. Après ça, il faut voir est-ce que ces personnes-là ont accès ou non, dans le cadre de leur travail, à des informations confidentielles ou personnelles. Mais oui, ça peut se faire, oui.

M. Lafrenière : Vous m'avez répondu : Ça peut se faire.

M. Prud'homme (Eric) : Non, non, mais ça dépend. Par exemple, tous les gens qui sont en contact avec des données personnelles, c'est sûr qu'il y a des vérifications en continu qui sont effectuées. On a des systèmes aussi de sécurité en place, là, je ne les nommerai pas tous, là.

M. Lafrenière : ...

M. Prud'homme (Eric) : C'est ça.

M. Lafrenière : Comprenez-moi, la raison pour laquelle je vous pose ces questions-là, c'est parce qu'on apprend du passé. Je viens d'une organisation où, en 2011, on a vécu un grand bris de sécurité avec des vols de données, puis on sait que, par la suite, ce qui a été dit, c'est que, justement, le danger, c'est qu'on vérifie, on enquête beaucoup les gens avant qu'ils travaillent, mais, une fois en poste, on les oublie un peu. Là, vous m'avez dit : On peut.

Je veux juste vous mettre à votre attention que le danger, c'est d'avoir un employé pendant 20, 30 ans dans notre entreprise, puis c'est rarement les plus récents, les plus jeunes qui le font... Est-ce qu'il y a de la vérification qui se fait par la suite?

M. Prud'homme (Eric) : Oui, tout à fait, il y a des vérifications en place. Et, je veux dire, la protection de l'information confidentielle, c'est majeur. Peut-être, ma collègue voudrait compléter.

Mme Mason (Angelina) : It's a multilayered approach. So, part of it is the background check, part is how you train your employees, including monitoring their activities. So, it's not simply checking of their character, but also having checks and balances on what types of activities they're conducting. So, if you're conducting transactions and there's something unusual... you normally touch 10 to 15 accounts in a day, all of a sudden, there's a hundred accounts, there's flags for that. There're also physical types of monitoring, whether it's cameras in the branch or if you go to certain elements of our facilities, you can't even bring a device in with you. So, if you're in some of the most sensitive areas where information is stored, you're not even able to take a device in with you. So, there's a range of different types of checks and balances to ensure that, if there's any unusual activity, we detect it.

Le Président (M. Simard) : ...cher collègue.

M. Lafrenière : Oui, rapidement. Donc, j'ai bien compris qu'il y a de la journalisation qui se fait des recherches qui sont faites dans vos bases de données.

M. Prud'homme (Eric) : Oui. Comme ma collègue l'a expliqué, c'est qu'il y a différents niveaux, et tout ça, c'est imbriqué ensemble.

M. Lafrenière : En terminant, rapidement, il ne reste pas beaucoup de temps, on a parlé tantôt de supposition de personne, de vol d'identité. Vous avez entendu ce qui nous a été dit tout à l'heure, comment on peut aider ces gens-là qui sont victimes de vol d'identité. Ils doivent se présenter et retrouver leur crédit. On sait que c'est très difficile, ça prend plusieurs heures. De quelle façon les banques aident, justement, les victimes de vol d'identité?

M. Prud'homme (Eric) : Bien, tout à fait. Écoutez, moi, je vais vous parler au nom de l'Association des banquiers canadiens. On a écrit, justement, un livre blanc sur l'identification numérique et on supporte un système fédéré d'identification numérique à travers le Canada. Donc, tant le gouvernement fédéral que les gouvernements provinciaux, comme vous le savez, détiennent des informations. Au niveau fédéral, c'est pour les passeports, par exemple, c'est... et, au niveau provincial, c'est les permis de conduire, le numéro... au niveau fédéral, le numéro d'assurance sociale. Et, dans le secteur privé, on a en place des systèmes très solides d'identification numérique. Donc, les banques, donc, par exemple...

• *(16 h 20)* •

M. Lafrenière : ...question très précise. Une personne qui s'est fait voler son identité, qui se présente dans une banque, pour retrouver son score de crédit, vous allez l'aider?

M. Prud'homme (Eric) : Bien sûr. Bien sûr, on est dans une relation basée sur la confiance et à long terme, et donc c'est au coeur de...

M. Lafrenière : Je vous ai bien entendu, mais vous savez que, dans les recherches qui ont été faites sur le «dark Web», il y a aussi des données de banques canadiennes qui ont été trouvées, hein? Vous n'êtes pas à l'abri de ça, vous le savez aussi?

M. Prud'homme (Eric) : Même le gouvernement...

Le Président (M. Simard) : Peut-être en conclusion. Merci.

M. Prud'homme (Eric) : ...n'est pas à l'abri des...

Le Président (M. Simard) : Merci beaucoup. Merci. Mme la députée de Saint-Laurent, à vous la parole.

Mme Rizqy : On va continuer sur la même lancée si vous le permettez. Une personne qui se fait voler ses données chez Desjardins, qu'un prêt hypothécaire est contracté chez Banque Nationale, un prêt auto à Banque de Montréal, concrètement, qu'est-ce qu'il arrive? Comment vous l'aidez? À part le livre blanc, là, comment vous l'aidez pour rétablir son score?

M. Prud'homme (Eric) : Alors, bien, d'abord, ce qui est important, là... ma collègue a mentionné que, quand... il doit y avoir de l'échange d'information, et il y en a, tant que c'est permis par la loi, justement. Et, nous, justement, à l'Association des banquiers canadiens, on a mis de l'avant qu'il devait y avoir des possibilités, par exemple, pour élargir à certains niveaux la législation pour permettre à bien lutter au niveau de la cybercriminalité contre les crimes financiers qui pourraient arriver.

Mme Rizqy : Ce n'est pas une question de lutter, faire de la prévention. La question du député de Vachon, vous avez répondu que, oui, vous l'accompagnez, vous avez parlé d'un livre blanc.

Moi, je vous pose la question suivante avec un cas concret : Si on a une personne qui est chez Desjardins, s'est fait voler son identité, par la suite, deux prêts ont été contractés à son nom. Elle habite au Saguenay, elle veut blanchir son dossier de crédit. Vous avez répondu : Oui, on l'accompagne. Concrètement, vous l'accompagnez comment? Parce qu'en ce moment elle se trouve pas mal seule, la dame en question.

M. Prud'homme (Eric) : Bon, bien, écoutez, d'abord, tout ce qui est fait à l'intérieur d'une banque puis dans les limites, bien sûr, de ce qui est permis par la législation, ça va être fait, justement, parce qu'on est dans une relation à long terme. On veut garder ces clients-là et on va les accompagner dans la... justement, aussi, en travaillant avec des bureaux de crédit. Tout est fait, et on a des services de sécurité corporative. Il y a des politiques en place, dans chacune des banques, au niveau de la protection des données personnelles. Il y a des mesures qui sont en place, justement, pour pouvoir accompagner ces gens-là.

Mme Rizqy : Si je vous soumets respectueusement la solution suivante : Si on a des gens qui sont, par exemple, identifiés chez Desjardins, que leurs dossiers ont été volés et que, par la suite, ces gens-là vous le disent, là, à vous, l'ABC, qui regroupe 70 différentes institutions financières : Mon dossier a été volé, pourquoi vous n'avez pas mis en place une mesure accélérée de traitement qui permet d'automatiquement blanchir et d'éliminer les prêts qui ont été contractés, surtout lorsque la personne cogne aux banques puis dit : Voici le rapport de police?

M. Prud'homme (Eric) : Alors, moi, je peux vous parler de ce qu'on fait à l'Association des banquiers canadiens. On n'est pas directement au niveau des opérations, mais c'est une très bonne question. Tout ce qui touche aussi à l'éducation financière, la littératie financière pourrait aider aussi les gens à bien comprendre. Donc, deux fois par année, deux fois... non, mais c'est important, on est...

Mme Rizqy : Je comprends, mais, monsieur, la littératie numérique, je sais parfaitement c'est quoi. C'est superbien, j'en suis puis je suis moi-même professeure, j'adore la pédagogie. Mais, maintenant, on est le après, et, dans le après, c'est vrai que, dans le vol de données, ce ne sera pas tout le monde qui aura un vol d'identité. Là, j'arrive de façon beaucoup plus spécifique, le vol d'identité, où est-ce que, là, la vie bascule pour ces gens. Et c'est pour ça que...

M. Prud'homme (Eric) : ...oui, ce n'est pas des situations faciles.

Mme Rizqy : Là, je comprends qu'il y a un livre blanc, mais il n'y a pas véritablement un accompagnement pour blanchir le dossier, pour permettre rapidement, de façon accélérée, avec un rapport de police... Puis moi, je pense que, probablement, ça pourrait être une mesure, à l'avenir, qu'on pourrait voir avec vous, d'appliquer... parce que, sinon, les gens se retrouvent avec des délais déraisonnables et des scores de crédit qui sont grandement affectés et qui, par la suite, lorsqu'ils vont vouloir contracter un prêt hypothécaire, bien, soit qu'ils ne l'auront pas, soit ils vont le payer trop cher.

M. Prud'homme (Eric) : Moi, je peux vous dire qu'il y a des mesures en place, justement, puis les employés de banque sont présents, sont formés, puis ils vont accompagner les personnes qui vivent des situations difficiles. On le fait sur une base... à d'autres niveaux, là, pas nécessairement en matière de vol d'identité, mais... Oui, oui, mais on le fait aussi au...

Une voix : ...

M. Prud'homme (Eric) : Non, non, mais on le fait au niveau des vols d'identité, mais on le fait aussi au niveau... lorsque les gens, dans leur situation, leur vie quotidienne, ils ont des situations plus difficiles, on va les écouter puis on va mettre en place des solutions pour rencontrer leurs besoins du mieux possible. Peut-être que ma collègue voudrait ajouter quelque chose?

Mme Rizqy : Bien, j'ai compris votre réponse. Je vais passer, puisque le temps passe très rapidement... Ça peut arriver, auprès de vos institutions financières, évidemment, le vol interne par des employés. C'est quelque chose que vous faites face très souvent. Est-ce que vous rapportez tous les crimes dans une dénonciation policière ou il arrive que les crimes ne soient pas rapportés et, par conséquent, pas comptabilisés?

M. Prud'homme (Eric) : Bien, on travaille avec les forces policières puis on va rapporter... Quand il y a un crime, c'est rapporté aux forces policières. Et, d'abord, on travaille à plusieurs niveaux...

Mme Rizqy : Est-ce que la dénonciation policière va être devant les tribunaux ou... Justement, est-ce que vous allez dans une procédure publique ou pas?

M. Prud'homme (Eric) : Peut-être, ma collègue voudrait compléter... juste pour la traduction, le temps que ça se rende.

Mme Mason (Angelina) : ...will engage the authorities where appropriate, if you're talking about a theft. And we also... obviously, if there's any real risk of significant harm to individuals, we will notify them directly. When we're talking about assisting individuals who have suffered because of...

Mme Rizqy : This is not my question. ...my question back then but now my current question is : When you identify an employee who commit a wrongful action, when you go to the police, do you go after that public, do you go and press charges or sometimes you don't do it?

Mme Mason (Angelina) : I believe, in most cases, it would be... you involve the police. Whether or not it's followed through on is another question, but we definitely take measures.

Mme Rizqy : ...without follow through on, with that respect, is that not your responsibility to make sure there's going to be a follow-up with that? Because if we don't press charges, what's going to happen, is that the track that we have, the records that are going to show up is maybe that we don't have current numbers for the task force to see if we have enough people working against all the identity theft inside of the bank.

Mme Mason (Angelina) : I can say that we have shared volumes of information with the authorities. We do... as part of our association, we share information about fraud and about varied ranges of crimes and we share with the appropriate authorities, RCMP and others. We have been involved in multiple task forces, identifying when there has been identify theft fraud by organised crime. We have worked collaboratively with the RCMP on these initiatives. We definitely take measures to endeavor, to have these people prosecuted.

M. Prud'homme (Eric) : Tout est fait, justement, pour ne pas que ces situations comme ça se produisent, et, quand ça se produit, on travaille avec différents intervenants, tant les corps policiers et, justement, on trouve la meilleure approche, la meilleure solution pour que ces choses-là ne se reproduisent pas. Nos systèmes de sécurité sont en constante évolution, et ça comprend aussi ce dont vous parlez.

Mme Rizqy : Oui, parfait, mais c'est juste qu'on a certains experts qui mentionnent que ce n'est pas tous les crimes à l'intérieur des banques qui sont commis par certains employés, qu'on retrouve par la suite sur la place publique. Et là ça fait en sorte que c'est un peu ce qu'on appelle un «catch-22». C'est que, si on n'est pas devant un tribunal, on ne sait pas nécessairement combien de fois une banque s'est fait frauder à l'intérieur, qui s'est fait voler à l'intérieur, peu importe le montant, peu importe le nombre de dossiers. Ça fait en sorte que, par la suite, on ne peut pas prendre des mesures adéquates pour savoir si, oui ou non, on a assez de policiers qui travaillent en matière de fraude.

Puis je vais continuer sur une autre affaire, j'aimerais maintenant parler du ratio assurance. Vos banques, quel est le ratio d'assurance en termes... par exemple, Banque de Montréal, Banque Nationale, est-ce que vous savez si elles sont proprement assurées pour tous les vols de données, conformément à ce qu'il arrive maintenant aux États-Unis?

M. Prud'homme (Eric) : Moi, je peux répondre du point de vue d'un consommateur. Un consommateur qui serait victime d'un vol, qui aurait... disons, à l'intérieur d'une banque, s'il y avait, justement, une fuite de données, et un consommateur serait impacté, cette personne-là serait indemnisée.

Mme Rizqy : ...je ne vous demande pas si, par exemple, jusqu'à 100 000 $, un compte bancaire... Ça, c'est correct. Je vous demande en matière de poursuite. Habituellement, il y a des gestions de risque qui doivent être faites, les banques doivent contracter des assurances pour la gestion de risque. Quel est le ratio d'assurance en ce moment? Est-ce qu'on parle de 200 millions, 300 millions?

Puis je vous donne un ordre d'idée de grandeur. Dans le cas de Marriott, ils ont payé 162 millions d'amendes; dans le cas de Facebook, 500 millions; Equifax, 700 millions de dollars US. Alors, moi, je me pose la question, lorsque vous vous réunissez une fois par année, est-ce que vous parlez de la gestion de risque? Parce que c'est... Présentement, le plus gros risque, c'est ça, c'est les risques de poursuite. Aujourd'hui, Desjardins fait face à 4,8 milliards de recours collectifs. Moi, je me demande si nos banques sont assez assurées.

• *(16 h 30)* •

M. Prud'homme (Eric) : Bien, moi, je vous dirais... Vous parlez de gestion de risque. Bien sûr, j'ai parlé de certaines lignes directrices du Bureau du Surintendant des institutions financières. Il y en a plusieurs, lignes directrices, et la gestion du risque, c'est au coeur aussi des opérations bancaires. Bien sûr, c'est un enjeu, la gestion du risque. Il y a des discussions qui ont lieu entre la haute direction, les conseils d'administration, les hauts dirigeants. Donc, c'est au coeur, la gestion du risque. Il y a même, vous le savez sûrement, une ligne directrice sur la bonne gouverneure de l'entreprise.

Mme Rizqy : Et quel est le montant que vous suggérez à vos banques pour être assurées?

Mme Mason (Angelina) : ...into the particular insurance profiles of any particular member. I can tell you that cybersecurity is a significant risk that our banks manage in consultation with the Superintendent of financial institutions. They deal with everything from the resiliency of the bank, how they would manage if there was to be an incident, tabletops, you name it. They go... they apply significant efforts in this area to ensure that this risk is properly managed. And I would come to the fact that this is not a risk that is isolated to the banking industry, this is a risk to society, both governments, you're dealing with it across sectors, which is why I just want to take a moment to say, we have been in this area, ahead of... leaders in this space...

Le Président (M. Simard) : Très bien.

Mme Mason (Angelina) : ...and we've been advocating for cybersecurity standards.

Le Président (M. Simard) : Merci, madame.

Mme Mason (Angelina) : Yes. Thank you.

Le Président (M. Simard) : Merci, beaucoup. M. le député de Gouin.

M. Nadeau-Dubois : Merci, M. le Président. Bonjour, M. Prud'homme et Mme Mason. J'ai peu de temps, ça fait que je vais vous demander de faire des réponses brèves dans la mesure du possible.

Vous avez répondu, tout à l'heure, à une question d'un collègue en confirmant que Capital One est membre chez vous. Vous n'êtes pas sans savoir que cette institution-là a fait face assez récemment à une fuite de données importantes, 6 millions de Canadiens touchés. On parle de noms, d'adresses, de numéros de téléphone, courriels, revenus, dates de naissance, cotes de crédit, soldes bancaires, et, dans 1 million de cas, les numéros d'assurance sociale. Qu'est-ce que votre... qu'est-ce que Capital One a fait ou a pris comme mesures pour protéger ces gens-là par la suite?

M. Prud'homme (Eric) : D'abord, moi, je vais vous parler au nom de l'industrie en ce qui concerne... dans l'ensemble de l'industrie, qu'est-ce qu'il se fait à partir du moment où il y aurait une fuite d'information qui est détectée. D'abord, c'est sûr, comme je l'ai mentionné tantôt, ce n'est vraiment pas facile quand une situation arrive sur le plan personnel, ce type de situation là, puis on en est très conscient. Encore une fois, il faut comprendre que ces choses-là, c'est hyper malheureux quand ça arrive, mais ça arrive dans différents secteurs aussi. Alors, nous, comme association, on a participé aux consultations au niveau du gouvernement fédéral, et on échange aussi de l'information avec le Centre canadien de cybersécurité, justement, qui réunit plusieurs experts dans le domaine de la cybersécurité, justement, pour qu'on développe au niveau pancanadien d'un solide système d'écosystèmes pour tout protéger.

M. Nadeau-Dubois : Que font vos membres concrètement pour aider concrètement leurs clients qui, concrètement, font face... sont victimes d'une fuite de données comme celle-là?

M. Prud'homme (Eric) : Bon, à partir du moment où y a une fuite de données qui serait détectée, il y a un suivi, un monitoring, excusez-moi, là, qui est fait des comptes qui pourraient être affectés. Donc, on a toujours des équipes de spécialistes qui travaillent sept jours sur sept, 24 heures sur 24 à faire des suivis. Ma collègue a mentionné, justement, si jamais on détecte des activités qui sortent de l'ordinaire, il y a des drapeaux rouges qui sont levés à ce moment-là, il y a des actions précises qui sont prises, et on va accompagner et on va indemniser les gens qui pourraient être touchés dans ces situations-là.

Le Président (M. Simard) : En conclusion.

M. Nadeau-Dubois : Vous redonnez l'argent, mais les données, elles, quelle responsabilité est-ce que vos membres assument en ce qui a trait à la portion des données qui, elles, sont en circulation?

M. Prud'homme (Eric) : Bien, s'il faut, on va travailler avec des bureaux de crédit pour, justement, faire un suivi sur une... si jamais il y avait une utilisation de ces données-là.

Le Président (M. Simard) : Très bien. Merci, monsieur. M. le député de Jonquière.

M. Gaudreault : Merci. Merci beaucoup de votre présence. La fuite concernant Capital One, qui est un nouveau membre, concerne 106 millions de clients aux États-Unis... bien, la source, c'est-à-dire, de la fuite viendrait aux États-Unis, mais, sur ces 106 millions, il y a en 6 millions qui seraient des Canadiens. Comment on gère ça entre deux législations, là, complètement différentes, la législation américaine, la législation canadienne? On a des gens qui vivent au Québec aussi. Je vois que, dans vos membres, vous avez la Banque de Chine, il y a des institutions internationales, alors là, les règles ne sont pas les mêmes, là. Et la source de la fuite vient des États-Unis, mais pourtant il y a des clients canadiens.

M. Prud'homme (Eric) : Bien, dans... Oui?

Une voix : ...

M. Prud'homme (Eric) : Ah! vas-y. Je vais laisser ma collègue répondre.

Mme Mason (Angelina) : Regardless of where the information is housed, the fact that it is Canadian... that these are consumers in Canada, the legislation of PIPEDA applies. So, our banks are accountable, so they're responsible for ensuring for the security of that information and ensuring our laws are followed with respect to notifying individuals and ensuring that they have the appropriate information if there is any real risk of harm. And that's what happens in these cases. So, even though the breach happened in the U.S., notification procedures in all laws of Canada applied in that circumstance.

M. Gaudreault : C'est vrai. Mais, si on veut être capable de mieux protéger les données personnelles des clients, on a des institutions maintenant qui sont internationales... je comprends qu'il peut y avoir des procédures après, une fois que la fuite est arrivée, mais, si on veut agir en amont, est-ce qu'il y a des solutions qui se posent ou des instances internationales qui peuvent être interpelées?

M. Prud'homme (Eric) : Bien, l'Association des banquiers canadiens, on est membres de différentes organisations au niveau international où il y a des forums de discussion sur différents sujets qui touchent l'industrie bancaire, justement, pour rester à l'affût tant au niveau international que canadien, bien sûr, de qu'est-ce qu'il se fait en termes de meilleures pratiques.

M. Gaudreault : Merci.

Le Président (M. Simard) : Merci. Merci à vous, M. le député de Jonquière. Alors, sur ce, nous vous remercions beaucoup pour votre présence parmi nous.

Nous allons suspendre temporairement nos travaux afin de faire place à l'Office de la protection du consommateur.

(Suspension de la séance à 16 h 37)

(Reprise à 16 h 39)

Le Président (M. Simard) : À l'ordre, s'il vous plaît! Nous allons reprendre nos travaux. Alors, mesdames, monsieur, bienvenue. Auriez-vous d'abord l'amabilité de vous présenter? Et vous savez que vous disposez d'une période de 10 minutes pour votre exposé.

Office de la protection du consommateur (OPC)

Mme Champoux (Marie-Claude) : Alors, bonjour. Mon nom est Marie-Claude Champoux. Je suis présidente de l'Office de la protection du consommateur. Laissez-moi vous présenter ceux qui m'accompagnent : d'abord, Mme Marjorie Théberge, la vice-présidente à l'office, de même que Me André Allard, directeur des affaires juridiques à l'office également. En fait, j'aurais dû dire Me Marjorie Théberge.

Alors, je vous remercie de l'invitation qui nous a été lancée. En tant que présidente de l'Office de la protection des consommateurs, je ne peux demeurer insensible à la situation des millions de Québécois touchés par la fuite de renseignements personnels chez Desjardins.

La protection des renseignements personnels est, de toute évidence, un sujet qui préoccupe l'office, bien qu'il ne fasse pas partie de sa mission première. C'est en effet la Commission d'accès à l'information qui assume cette responsabilité. Malgré tout, au bénéfice des consommateurs, l'office agit de manière préventive en matière de protection des renseignements personnels, et je peux vous dire qu'on intensifiera nos efforts. On envisage d'insister sur le message de vigilance qui suit, très général mais tout de même essentiel : Il faut éviter de donner des renseignements personnels quand ce n'est pas nécessaire. D'ailleurs, ce matin, l'office a modifié son site Internet afin que la section Protection des renseignements personnels soit visible sur sa page d'accueil afin d'en faciliter l'accès.

L'office profite d'une excellente notoriété auprès de la population québécoise. Les consommateurs se tournent vers l'organisme pour des sujets qu'il ne couvre pas, dont, parmi tant d'autres, la protection des renseignements personnels. L'office se sert ainsi des tribunes dont il dispose pour véhiculer des messages préventifs dans les médias ou dans son site Web, entre autres. D'ailleurs, dans son site, l'office invite déjà les consommateurs à protéger leur numéro d'identification personnelle, le NIP, de leur carte de crédit. On les incite à vérifier si leur dossier de crédit contient des renseignements exacts et à jour. On les prévient aussi de se méfier des courriels provenant supposément d'une institution financière dans lesquels l'expéditeur demande des renseignements bancaires ou personnels. Ce ne sont ici que quelques exemples.

• *(16 h 40)* •

Je signale au passage que la Loi sur la protection du consommateur prévoit, selon les circonstances, une exonération ou une limite de responsabilité pour le consommateur en cas d'utilisation non autorisée de sa carte de crédit par un tiers. On peut ici penser à une fraude, au vol ou à la perte d'une carte. Cette protection a très certainement sauvé bien des gens de malheurs. En revanche, elle ne s'applique pas lorsqu'il est question d'une nouvelle carte de crédit qui aurait été obtenue par un tiers malveillant au nom du consommateur avec des renseignements personnels obtenus illégalement.

Je poursuis en vous parlant de la Loi sur la protection du consommateur, l'une des quatre lois dont l'office est responsable. Elle régit les relations entre les consommateurs et les commerçants, entre autres, en matière de crédit. Une importante partie de cette loi touche en effet les contrats de carte de crédit, de marge de crédit, de prêt d'argent, de vente à tempérament, etc.

Une fuite de données, quelle qu'elle soit, peut ultimement, dans les situations les plus critiques, se traduire par un vol d'identité. Je ne vous apprends rien ici. Et le vol d'identité a des conséquences majeures dans la vie du consommateur, car il peut entraîner des inscriptions à son dossier de crédit qui lui sont défavorables, des transactions faites en son nom par une autre personne; c'est assez catastrophique, vous en conviendrez.

On peut se demander quelles sont les conséquences d'un vol d'identité. On en connaît plusieurs. Elles sont nombreuses. Ce qui nous préoccupe particulièrement à l'office, ce sont les traces qui se répercutent dans le dossier de crédit du consommateur. Pourquoi? Parce que le dossier de crédit, c'est un élément central dans la vie d'un consommateur. Concrètement, une note défavorable peut grandement lui nuire s'il demande une carte de crédit, s'il veut emprunter de l'argent ou s'il souhaite profiter d'un plan de financement. Mais ce n'est pas tout. Une note défavorable au dossier de crédit d'une personne peut aussi lui nuire dans plusieurs sphères de sa vie citoyenne : souscrire une assurance, louer un véhicule ou même obtenir un emploi.

Présentement, il n'est pas si simple pour le consommateur d'accéder à son dossier de crédit, d'autant plus que des frais peuvent lui être exigés. Une inscription peut être faite, une nouvelle transaction peut y figurer, une modification peut y être apportée sans que le consommateur en soit informé. Une autre personne pourrait aussi accéder à son dossier, le tout à son insu. Ces faits sont troublants, surtout quand on considère que tous les renseignements que contient le dossier de crédit d'une personne sont des renseignements qui la concernent. Un peu plus de transparence ne pourrait qu'être positif.

Peut-être le savez-vous, tout consommateur a la possibilité de contester une note à son dossier de crédit, notamment s'il est victime d'un vol d'identité. Au moment où je vous parle, une note, bien que contestée, influence la cote de crédit d'un consommateur, et ce, jusqu'à ce qu'il fournisse des preuves. Entre-temps, c'est le consommateur qui en paie le prix. Par exemple, s'il souhaite conclure un contrat de crédit, peut-être aura-t-il accès à un montant moindre, peut-être ne pourra-t-il obtenir de crédit, acheter la voiture dont il a besoin pour se rendre au travail. C'est le consommateur qui porte le fardeau de la preuve, un fardeau lourd et stressant. Encore ici, peut-être faudrait-il réfléchir à changer les règles du jeu pour mieux servir les consommateurs.

J'ouvrirai maintenant une courte parenthèse. À l'office, il arrive qu'un consommateur communique avec nous parce qu'un créancier, disons un commerçant, lui exige une somme d'argent qui n'est pas due. Ça peut arriver, et je vous donne un exemple. Si le consommateur annule un contrat avec un commerçant itinérant dans les 10 jours de sa conclusion, dans un tel cas, l'annulation est faite en tout respect de la Loi sur la protection du consommateur et le commerçant ne peut plus exiger cette somme du consommateur. Mais, dans une situation comme celle-là, nous sommes bien au fait que certains commerçants menaceraient le consommateur de porter une inscription à son dossier de crédit s'il ne paie pas, et c'est regrettable, mais plusieurs vont payer pour ne pas voir leur dossier entaché. Avec tout ça, je veux seulement démontrer que les solutions qui pourraient être amenées relativement au dossier de crédit et au vol d'identité seraient aussi à même de venir en aide aux consommateurs dans un autre contexte, soit quand le consommateur ne doit pas la créance qui lui est exigée.

Pour en revenir au sujet qui nous intéresse plus précisément, je souhaite mettre aussi en lumière les faits qui suivent. Actuellement, le commerçant, par exemple, une institution financière qui consulte un dossier de crédit pourrait très bien n'avoir aucune indication quant au fait que le consommateur s'est possiblement fait voler son identité. Comme je l'ai rapidement expliqué plus tôt, le contenu du dossier pourrait faire en sorte que l'institution financière n'accorde pas de prêt à cette personne ou accorde le prêt mais à des conditions moins favorables, exemple, un taux de crédit plus élevé, sur la base d'un dossier de crédit comprenant des transactions faites par un être mal intentionné. Les heurts du vol d'identité se répercutent dans la cote de crédit du consommateur sans que cette institution financière le sache, mais surtout sans que le consommateur le sache. Il ne saura donc pas que le prêt lui a été accordé à des conditions moins favorables que ce qu'il aurait pu obtenir.

Je ne vous apprendrai rien, la notion de protection des renseignements personnels est plus que complexe. Elle touche la cueillette de renseignements, leur conservation, leur utilisation, leur communication, leur destruction. À l'office, la question qu'on se pose, c'est : Comment pouvons-nous faire pour réduire les conséquences d'un vol d'identité sur les consommateurs québécois? Nous devons y répondre tous ensemble et continuer à explorer toutes les avenues possibles. Bien entendu, nous nous réjouirons si des mesures sont proposées pour mieux outiller les consommateurs en matière de protection des renseignements personnels et pour mieux les protéger en cas de vol d'identité. Les pistes d'amélioration sont nombreuses, on le sait, on l'a vu dans les derniers mois, plusieurs ont déjà été avancées.

Je termine en vous rassurant qu'à l'Office de la protection du consommateur nous accueillerons avec enthousiasme toute solution, dont toutes celles qui, particulièrement, viendront soutenir le consommateur québécois victime d'un vol d'identité de la part d'un individu malveillant. Alors, je vous remercie toutes et tous de votre attention.

Le Président (M. Simard) : Merci à vous, Mme Champoux. Donc, avant de poursuivre nos travaux, je vous indique qu'afin d'entrer dans nos temps le gouvernement dispose d'une période de 14 min 45 s, l'opposition officielle, d'une période de 9 min 50 s, et les deuxième et troisième groupes d'opposition, d'une période de 2 min 27 s. Je cède maintenant la parole au député de Vachon.

M. Lafrenière : Merci beaucoup. Merci, mesdames, monsieur. Merci d'être là avec nous. En passant, avec votre présentation, vous avez changé complètement les questions que j'avais pour vous. Je suis persuadé que ma collègue de Saint-Laurent a entendu de la musique à ses oreilles. On a parlé beaucoup aujourd'hui des questions pour retrouver la cote de crédit pour les citoyens qui vivent ça. Parce que je vais me permettre de dire que c'est un calvaire, ces gens-là se retrouvent tout seuls, c'est très difficile, puis j'aurais le goût de vous entendre là-dessus, puis je vais vous parler vraiment juste de ça parce que je trouve ça hyperimportant.

Aujourd'hui, on a entendu des gens d'Equifax, et ce qu'on s'est fait dire par plusieurs citoyens qui l'ont vécu, lorsqu'il arrive un vol d'identité, donc des transactions frauduleuses, problèmes avec leur crédit, ils se présentent devant l'entreprise puis ils se font dire : Bien, écoutez, vous ne pouvez pas changer votre cote, puis ça ne fonctionne pas, ils se retrouvent à aller devant la Commission d'accès à l'information. Pouvez-vous nous en parler un peu? Est-ce que c'est quelque chose que vous connaissez?

Mme Champoux (Marie-Claude) : Oui, c'est quelque chose dont on entend parler beaucoup, effectivement, le fardeau de la preuve est toujours sur le dos du consommateur. Alors, effectivement, oui, c'est difficile pour un consommateur de changer son dossier de crédit.

M. Lafrenière : Puis, selon vous, à l'OPC, quelle serait l'obligation de... puis je parle d'une firme, on aurait pu convoquer une autre agence, je pense qu'on aurait eu le même résultat. Quelle serait la responsabilité de cette agence-là? Parce que, de ce que je comprends, c'est que le citoyen est laissé à lui-même, il n'y a pas personne qui remet un guide en disant : Bien, regardez, vous avez été victime de vol d'identité, votre crédit, votre score de crédit a été affecté, voici ce que vous devez faire. Moi, ce que les gens m'ont rapporté, c'est qu'ils doivent se dépêtrer eux-mêmes, puis aller devant la Commission d'accès à l'information, puis ce qu'on se fait dire, c'est près de 80 heures de travail acharné pour réussir à s'en sortir. Est-ce qu'il y a une obligation qui demande à ces agences-là de remettre, justement, des indications, quoi faire?
• (16 h 50) •

M. Allard (André) : Oui, si vous permettez. D'abord, la réponse à cette question-là supposerait qu'on formule des recommandations, puis on n'est pas ici pour formuler des recommandations, on est plutôt ici pour faire l'état des lieux dans la perspective d'un consommateur. Il faut aller en amont, en amont de tout le processus d'inscription, même des annotations dans les dossiers de crédit. Ce sont des annotations qui sont inscrites par les entreprises sans qu'elles vérifient. Par exemple, lorsque le consommateur voit que son inscription lui est défavorable, il s'aperçoit effectivement qu'il y en a une, inscription, c'est le premier défi qu'il doit relever. Et il se peut qu'il conteste l'exactitude de cette inscription ou même la légitimité de cette inscription. La présidente, tout à l'heure, a mentionné un exemple où, dans certains cas, les entreprises inscrivent des annotations défavorables, alors que le consommateur a exercé un droit qui lui était conféré par la loi. Donc, elle est litigieuse, il s'agit d'une dette litigieuse qui a été inscrite au dossier de crédit. Donc, il s'agit donc d'une inscription dont l'entreprise décide elle-même de son bien-fondé. Donc, ça, c'est un premier problème, parce que contester une telle annotation est très difficile. À la limite, on souhaiterait être poursuivi pour qu'on puisse faire la preuve qu'on n'a pas contracté cette dette-là. Mais les entreprises ne nous poursuivent pas, elles inscrivent au dossier une annotation défavorable avec les...

M. Lafrenière : Je m'excuse, c'est parce que le temps est très compté ici.

M. Allard (André) : Je suis désolé.

M. Lafrenière : Non, non, vous n'avez pas à être désolé, voyons. Et c'est quoi, le recours, pour le consommateur, à ce moment-là?

M. Allard (André) : Dans le pire cas, il devra saisir lui-même les tribunaux pour poursuivre à la fois l'agence et l'entreprise, pour pouvoir contester... l'inexistence d'une dette, ce qui représente un défi colossal.

M. Lafrenière : Question pour vous. Des agences de crédit, on en a entendu une, tout à l'heure, Equifax, dans le dossier de Desjardins : Est-ce que vous avez eu beaucoup de plaintes, à l'OPC, pour l'accès aux services ou l'accès dans la langue de leur choix, c'est-à-dire en français? Est-ce que c'est le genre de plaintes que vous avez reçues? Sans tomber dans des chiffres, est-ce que vous avez reçu des plaintes?

Mme Champoux (Marie-Claude) : Très peu de plaintes chez nous. Bien, pour la langue, pas du tout, c'est probablement plus à l'Office québécois de la langue française, s'il y en a eues, mais, chez nous, il n'y a pas eu de plainte concernant la langue. Puis on a eu quelques appels suite à la fuite, en fait, suite aux nombreuses fuites des derniers mois, on a eu quelques appels, mais quelques dizaines à peine à l'office, qu'on a référés soit à l'Autorité des marchés financiers ou, justement, la Commision d'accès à l'information, là, parce que, comme ce n'est pas une loi qui est sous notre gouverne, là, on n'y répondait pas, mais c'est... Nous, on reçoit 150 000 appels par année, à l'office, sur des sujets divers, alors quelques dizaines, c'est vraiment très, très peu.

M. Lafrenière : Dans la minute qui me reste... Tout à l'heure, on parlait du dossier de crédit. On sait que les commerçants ont accès au dossier de crédit, ils peuvent aller le consulter. Selon vous, les mesures de sécurité qui sont appliquées pour savoir, justement, qui l'a consulté, le dossier de crédit puis qu'est-ce qu'il en a fait, est-ce que vous êtes... Est-ce que c'est une connaissance que vous avez, à l'OPC? Je prends une chance.

M. Allard (André) : En fait, la situation que vous évoquez, c'est que, lors d'une transaction entre un commerçant et un consommateur, la personne qui connaît mieux la situation financière du consommateur, c'est l'entreprise. Le consommateur n'a pas accès, en temps réel, de façon continue, à son dossier de crédit, alors que son information personnelle, relativement à sa situation financière, qu'il ignore puisqu'elle est mesurée avec une cote qu'on ne lui communique jamais... c'est l'entreprise qui connaît le mieux la situation financière du consommateur. Le consommateur est donc, encore une fois, dans une situation défavorisée, ne sachant pas pourquoi ou sur quelle base la négociation ou la discussion du contrat va se tenir.

M. Lafrenière : Merci beaucoup. Merci, je vais laisser la parole.

Le Président (M. Simard) : Merci à vous, M. le député de Vachon. M. le député de Vanier.

M. Asselin : Merci beaucoup, M. le Président. Mme Champoux, Mme Théberge, Me Allard. J'ai bien compris que vous n'avez pas reçu beaucoup de plaintes suite aux incidents de chez Desjardins.

Mme Champoux (Marie-Claude) : Oui, vous avez effectivement bien compris, on a... en fait, on n'a pas eu de plainte, on a eu quelques appels qui sont entrés dans notre système téléphonique, mais des appels que nous avons redirigés.

M. Asselin : Si un membre de chez Desjardins appelait chez vous, qu'est-ce que vous lui conseillerez?

Mme Champoux (Marie-Claude) : Ça dépendait probablement de la nature du sujet, mais on le référait soit à l'Autorité des marchés financiers, soit à la Commision d'accès à l'information, soit à la police, dans le fond, On n'est pas... À l'office, on gère quatre lois.

M. Asselin : La fuite de données vous concerne quand même, non?

Mme Champoux (Marie-Claude) : On gère quatre lois, à l'Office de la protection du consommateur, et la loi sur la protection des renseignements personnels n'en est pas une. Alors, oui, on a une préoccupation parce que les consommateurs sont affectés par ça, mais on ne gère pas cette loi-là, donc.

M. Asselin : Est-ce que, dans vos outils de communication, vous avez modifié l'information qui vous concerne sur vos sites?

Mme Champoux (Marie-Claude) : Oui. Bien, comme je le disais en introduction, on a quand même un onglet Protection des renseignements personnels sur notre site Web, onglet qui était un petit peu plus difficile à trouver jusqu'à ce matin mais qu'on a effectivement ramené en page d'accueil pour que l'information soit plus accessible. Dans nos activités de communication, dans nos ateliers, oui, on fait des activités de prévention pour la protection des renseignements personnels auprès des consommateurs, mais je réitère que ce n'est pas une loi qui est sous notre responsabilité.

M. Asselin : Actuellement, quelles sont les activités de sensibilisation que vous conseillez aux gens concernant ce qu'il est arrivé?

Mme Champoux (Marie-Claude) : On ne fait pas d'activité de sensibilisation sur ce qu'il est arrivé, on fait des activités générales de sensibilisation dans une... Pour que le consommateur soit bien protégé dans l'ensemble de son dossier, on lui procure certains conseils sur la protection des renseignements personnels, mais ce n'est pas en lien avec les fuites qui ont eu lieu.

M. Asselin : O.K. Merci.

Le Président (M. Simard) : Merci beaucoup. Mme la députée de Charlevoix—Côte-de-Beaupré.

Mme Foster : Bonjour. Merci d'être ici aujourd'hui. À l'Office de la protection du consommateur, est-ce que vous avez des spécialistes de la protection des données personnelles parmi vos employés?

Mme Champoux (Marie-Claude) : En fait, on a une personne qui est responsable de la protection des renseignements personnels de l'office, mais on n'a pas de conseiller pour les consommateurs, par exemple,

Mme Foster : Est-ce que vous croyez, suite aux événements, que ça pourrait être une bonne idée? Parce que ce qu'on entend depuis ce matin, c'est que c'est un problème qui va aller en augmentant, et ce, dans toutes les sphères de la société.

Mme Champoux (Marie-Claude) : Je ne sais pas. Est-ce que vous demandez s'il devrait y avoir plus de conseillers? À ce moment-là, ça serait peut-être plus à la Commission d'accès à l'information, qui est responsable de la loi sur la protection des renseignements personnels, ou je ne sais pas si vous voulez que l'office devienne responsable de la loi sur la...

Mme Foster : Non. Ce n'est pas ce que j'ai dit, ce n'est pas ce que j'ai dit. Dans votre rapport annuel de gestion, vous mentionnez accorder une importance primordiale au fait d'informer les consommateurs sur leurs droits, leurs recours, leurs responsabilités. Qu'est-ce que vous avez fait pour informer les membres de Desjardins? Tantôt, on parlait un peu de... tu sais, vous dites que vous n'êtes pas allé dans la sensibilisation, c'est plus en allant sur le site Web ou en vous contactant que, là, on peut avoir des renseignements, mais est-ce qu'il y a autre chose qui a été fait de façon proactive?

Mme Champoux (Marie-Claude) : De façon proactive pour les membres Desjardins en particulier, non, mais, auprès de la population, oui, on fait des activités de sensibilisation et de prévention.

Mme Foster : Oui, O.K. Puis également, dans votre rapport annuel, vous mentionnez que vous exercez des actions de sensibilisation pour rappeler aux commerçants leurs obligations.

Mme Champoux (Marie-Claude) : Oui.

Mme Foster : Est-ce qu'il y a des actions de sensibilisation qui ont été faites auprès des entreprises bancaires pour leur rappeler leurs obligations, par exemple?

Mme Champoux (Marie-Claude) : Bien, on a des rencontres assez régulières avec les entreprises, effectivement, entre autres, parce que nous sommes responsables des dossiers de crédit. Comme vous savez peut-être, on a lancé un document de consultation, le printemps dernier, sur une modernisation de la loi sur le crédit. Alors, oui, on a des rencontres, mais pas au niveau de la protection des renseignements personnels, parce que, au risque de me répéter, ce n'est pas une loi qui est sous notre responsabilité.

Mme Foster : Qui est sous votre responsabilité. À votre avis, ce serait quoi, le meilleur moyen pour que les Québécois se protègent? Parce que, tout à l'heure, vous avez parlé de renverser le fardeau de la preuve — parce que, on le sait, c'est

un processus qui est lourd quand on est victime, on en a parlé un peu tantôt, vous avez parlé de renverser le fardeau de la preuve — mais quel changement, là, nous, on pourrait faire ici, comme législateurs, qui pourraient en arriver à ce résultat-là?

Mme Champoux (Marie-Claude) : Comme j'ai dit, nous, on... je pense que Me Allard le disait tout à l'heure, on n'est pas là pour vous faire des propositions, on fait tout simplement état de ce qui est présentement les faits. On va accueillir, évidemment, les recommandations et les propositions des membres de l'Assemblée nationale, puis on se conformera avec plaisir, mais effectivement nous, on est là pour vous présenter la situation des consommateurs telle quelle.

Mme Foster : État de la situation et non pas mode recommandation. Parfait. Merci.

Le Président (M. Simard) : Merci à vous, Mme la députée. M. le député de Vachon, il vous reste 4 min 9 s.

M. Lafrenière : Je m'excuse, je vous ai menti tout à l'heure. Je vous ai dit que j'avais des questions juste là-dessus, mais vous m'avez guidé sur d'autres choses. Vous avez parlé des commerçants, et je voulais savoir si vous aviez reçu des plaintes à l'OPC concernant l'utilisation de bases de données, c'est-à-dire les fameux dossiers de crédit, de la part de commerçants. Je ne veux pas parler de côté criminel, ce n'est pas votre cour, je comprends bien ça, mais est-ce que vous avez reçu des plaintes à l'OPC quant à l'utilisation par des commerçants? On va mettre ça clair, là, un commerçant qui utiliserait la base de données à d'autres fins, comme du marketing, comme des ventes différentes, est-ce que vous avez déjà reçu des plaintes comme ça chez vous?

Mme Champoux (Marie-Claude) : Je peux vous le garantir, que ce n'est pas dans les tops de nos plaintes, mais je ne peux pas vous garantir qu'on n'a jamais eu aucune. Moi, je n'en ai pas entendu parler, qu'il y ait eu des plaintes, mais évidemment je n'ai pas nécessairement chacune des plaintes, là. C'est une information, toutefois, que je pourrais fournir à la commission plus tard, là, quand on aura fait le décompte, mais c'est certain que ce n'est pas une plainte qui arrive souvent. Ça, ça serait allé sous mon radar.

M. Lafrenière : Sans aller dans les recommandations, on va rester loin de ça, cependant, est-ce qu'il y a de la sensibilisation qui peut être faite de votre part auprès des commerçants quant à leurs rôles et responsabilités en utilisant cette base de données? Puis là je vais mettre ça clair, là, pas de cachette, sans présumer que certains commerçants pourraient le faire, c'est arrivé récemment, on a vu des cas dans les médias tout, tout, tout récemment, de leur rappeler que l'utilisation de cette base de données, quand on parle de la base de crédit, doit être faite dans le cadre d'une transaction initiée par un consommateur, et non pas pour faire du marketing ou d'autre chose. Est-ce que c'est le genre de communication, de prévention, ça, que vous pourriez faire à votre niveau?

• *(17 heures)* •

Mme Champoux (Marie-Claude) : Certainement. C'est certainement des communications qu'on pourrait faire. Évidemment, l'office a un petit budget, a de petits moyens. Alors, des fois, il faut faire des choix sur quels sont les campagnes puis les moyens de communication qu'on utilise, mais c'est effectivement quelque chose qui pourrait être dans notre palette.

Le Président (M. Simard) : Merci beaucoup. Il vous reste deux minutes, cher collègue.

M. Lafrenière : Sur la même lancée, est-ce que les agences de crédit pourraient se retrouver à avoir les mêmes recommandations de votre part sur comment aider, comment guider les consommateurs qui se retrouvent dans le trouble?

Mme Champoux (Marie-Claude) : Je ne sais pas si nous sommes des spécialistes de consommateurs sur le... pour les guider dans un processus législatif ou un processus... juridique, pardon, mais d'adopter des bonnes pratiques, oui, ça pourrait être effectivement des conseils qu'on peut donner.

M. Lafrenière : Parce que, bien honnêtement, les gens qu'on a entendus aujourd'hui, il n'y a pas personne qui semblait vraiment les diriger à la bonne place, sans méchanceté, là. Puis, pour le citoyen, le consommateur, je me dis : Écoute, on se retrouve dans un cul-de-sac, on se fait dire : Ce n'est pas chez nous. Ta cote de crédit est affectée? «Too bad», en bon français. Attends, ça va revenir, un jour, correct.

Alors, je me dis, il y a sûrement quelqu'un qui peut les aider. Puis je ne demande pas de le prendre par la main puis d'aller lui faire faire les démarches, mais, au moins, d'aviser. Parce que, de ce que j'ai compris tout à l'heure, même de la part d'Equifax, on leur dit : Nous, on ne peut pas rien faire. On ne les guide même pas vers la Commission d'accès, qui est quand même assez lourde.

Mme Champoux (Marie-Claude) : On pourrait probablement le regarder, là. Je ne sais pas, est-ce que ça prendrait la forme d'un guide? Est-ce que ça... des bonnes pratiques qu'on pourrait partager avec les agences de crédit? Ce n'est pas quelque chose sur lequel l'office s'est penché, mais on pourrait certainement le regarder, là.

M. Lafrenière : Sans tomber dans les recommandations, seulement une idée, comme ça.

Mme Champoux (Marie-Claude) : On vous écoute et on vous répond.

M. Lafrenière : Merci beaucoup. Bien gentille, merci.

Le Président (M. Simard) : Merci, M. le député de Vachon. M. le député de Robert-Baldwin.

M. Leitão : Très bien. Merci beaucoup, M. le Président. Alors, bonjour. Merci d'être là. On va rester dans les enjeux soulevés par le collègue de Vachon. Moi, ce qui m'intéresse beaucoup, c'est la question de l'accès au dossier de crédit.

Donc, de la façon dont le système fonctionne présentement, un commerçant, banque ou autre, un commerçant a un accès direct au dossier de crédit d'un consommateur. Il n'a qu'à entrer un code et il a accès directement à ça. Il peut non seulement aller retirer des informations, mais il peut aussi inscrire des informations. Est-ce qu'un consommateur, lui aussi, a le droit d'accéder à son propre dossier de crédit?

Mme Champoux (Marie-Claude) : En fait, le consommateur a accès à un dossier de crédit résumé, si je peux me permettre l'expression. Ce n'est pas un dossier complet. La plupart du temps, pour avoir le dossier complet, il y a des frais.

M. Leitão : Très bien. Est-ce que vous pensez... Est-ce que l'office pense que, justement, cette information-là, en fin de compte, appartient au consommateur? C'est mon information. Ça résume les emprunts et les choses que moi, j'ai faites, comme consommateur. Vous ne pensez pas que ça devrait être l'inverse? Donc, le consommateur, lui, il peut et il devrait avoir accès en tout temps à son dossier de crédit, et ça serait aux autres, aux commerçants, d'obtenir une autorisation pour avoir accès au dossier de crédit.

Mme Champoux (Marie-Claude) : Disons, sans commenter sur la façon, il est évident que l'Office de la protection du consommateur souhaite plus de transparence pour les consommateurs versus leur dossier de crédit.

M. Leitão : Merci. Parce que c'est une question de transparence, mais c'est aussi une question d'accès, parce que ça... S'il y a des choses à corriger, comme Me Allard a dit, c'est extrêmement complexe de corriger, et on renverse complètement le fardeau de la preuve, ce qui n'est pas du tout la situation normale dans notre système juridique. Et puis, en plus, si on veut faire ça, évidemment, ça implique toutes sortes de frais additionnels.

Alors, ma question est : Pour vous, en tant qu'Office de protection du consommateur, est-ce que vous pensez que ça serait dans votre mission, d'émettre des recommandations ou des «guidelines», enfin, quelque chose pour sensibiliser les autorités réglementaires à faire ce renversement de situation où le dossier de crédit appartient au consommateur, et c'est à lui et lui seul à donner accès à cette information à des commerçants ou autres?

Mme Champoux (Marie-Claude) : Comme je vous dis, sur la façon, lui seul... Je ne commenterai pas sur la façon que ça doit être fait, mais effectivement l'Office de la protection du consommateur souhaite que le consommateur ait un meilleur accès à son dossier puis, en fait, dans un souci de transparence et d'accessibilité pour son dossier, tout à fait.

M. Leitão : O.K. Merci. Aussi, en termes de protection du consommateur, on a entendu ce matin d'Equifax, et je suis sûr que c'est la même chose avec d'autres agences de crédit, qu'ils offrent toute une série de services additionnels, des services de protection. Et ces services-là, bien sûr, ne sont pas gratuits. Ça implique des frais, donc quelqu'un doit payer pour ça. Encore une fois, est-ce que ces frais-là... est-ce qu'ils sont... Bien, ils sont dans le droit de charger, oui, mais est-ce que vous pensez que ces frais-là ne devraient pas exister, qu'en fin de compte ça devrait faire partie du service de base ou du service courant de l'agence de crédit, non seulement de gérer la banque de données, mais aussi de fournir des services de protection? Ça devrait faire partie du package?

Mme Champoux (Marie-Claude) : Je ne sais pas quels sont les services supplémentaires dont Equifax parlait, alors c'est difficile pour moi de dire... Est-ce que tous les services devraient être gratuits? Je l'ignore, je ne suis pas une spécialiste. Alors, c'est sûr que moi, je pense que l'accès pour le consommateur, certainement, devrait être plus facile. Mais, pour ce qui est des services de protection, je ne les connais pas, ça fait que je suis incapable de vous répondre.

M. Leitão : D'accord. Parce que la façon dont le système fonctionne présentement, Equifax se fait... enfin, va chercher ses revenus, pour la plupart, chez les commerçants. Donc, le commerçant, quand il consulte le dossier d'Equifax — je mentionne Equifax, ça peut être un autre — donc c'est là qu'ils font leurs revenus. Très bien.

Mais aussi, en offrant des services directement aux consommateurs, des services de notification, des services de «credit monitoring», etc., ils chargent aussi des frais et là directement aux consommateurs. Là, je pense que l'office a un rôle à jouer, d'indiquer, de lever un drapeau. On disait : Mais non, ces services-là que vous chargez aux consommateurs, en fin de compte, devraient faire partie de votre offre de services standard pour tout le monde.

M. Allard (André) : En fait, le seul commentaire que j'aurais le goût de formuler, c'est que les dossiers de crédit, ce sont des outils que se sont donnés les entreprises pour évaluer la solvabilité et mesurer le risque lorsqu'ils font affaire avec un consommateur. C'est un outil qu'ils se sont donné, à eux, pour pouvoir faire leur travail correctement, de façon responsable.

M. Leitão : O.K. Bon, c'est un peu particulier, mais bon...

Sur un autre ordre d'idées, mais on reste toujours dans ce domaine-là, est-ce que vous pensez que c'est toujours pertinent qu'un consommateur, d'une façon pas... excusez-moi, qu'un commerçant, d'une façon presque routinière, pour la moindre des transactions, ait accès à une enquête de crédit? Est-ce que c'est toujours pertinent de procéder avec une

enquête de crédit? Sachant très bien que le plus qu'on a d'enquêtes de crédit, évidemment, ça va avoir un effet sur le score de crédit.

Mme Champoux (Marie-Claude) : Mais on demande au commerçant d'évaluer la capacité de crédit avant de faire un prêt à un consommateur. Puis ça, c'est la Loi sur la protection du consommateur qui prévoit ça. On leur donne... Oui, bien, quand on parle de crédit, c'est nécessairement soit un achat à crédit ou un prêt d'argent. Alors, on donne cette obligation au commerçant de vérifier le crédit. Alors, c'est sûr que...

M. Leitão : D'accord. Je n'ai pas de problème avec ça. La question que je me pose et que, donc, je vous pose : Est-ce que cet outil-là est utilisé par des commerçants dans des cas où il n'y a pas vraiment nécessité de procéder à une enquête de crédit?

M. Allard (André) : Bien, on a assisté, depuis quelques années, à cette propension des entreprises à vérifier le dossier de crédit, même si ce n'est pas en vue de consentir du crédit. Alors, les assureurs, pour se louer un logement, par exemple, ou... enfin, d'autres transactions qui sont étrangères à un contrat de crédit. Oui, c'est de plus en plus utilisé.

M. Leitão : Et ça serait peut-être intéressant et utile que l'office dise quelque chose là-dessus, parce qu'il me semble que ce n'est pas pertinent, donc ce n'est pas dans l'intérêt public. Et je passe la parole à ma collègue parce que, sinon, je vais...

Le Président (M. Asselin) : Mme la députée de Saint-Laurent, il vous reste encore deux minutes.

• *(17 h 10)* •

Mme Rizqy : Parfait. Mais je reste là-dessus, parce que je comprends que tout le monde parle d'éduquer les citoyens, mais les citoyens ne savent pas qu'à chaque fois qu'il y a une demande de crédit leur score est affecté. Est-ce que ça, vous ne pensez pas que ça devrait être divulgué de façon claire à chaque fois qu'il y a une demande qui est faite, que ce soit pour le logement, le prêt auto ou les achats crédit-bail, là? Est-ce que vous ne pensez pas qu'on devrait le dire clairement aux citoyens puis avoir leur consentement, à ce moment-là, un consentement éclairé?

Me Allard, je sais que vous ne voulez pas faire de recommandation, mais l'article 292 de la loi est quand même assez clair. Vous avez aussi, dans votre mission, un devoir d'éduquer la population. Alors, je vous demande, à titre d'avocat, pouvez-vous, s'il vous plaît, nous faire un éclairage, en ayant en tête qu'il y a des gens qui nous écoutent à la maison, puis on doit faire aussi de l'éducation citoyenne?

M. Allard (André) : Bien, ça nous ferait plaisir de faire des recommandations dans un contexte où on va travailler sur une proposition qui pourrait être formulée. En fait, notre présence ici, encore une fois, puisqu'on parlait initialement, là, de la fuite de Desjardins et donc des conséquences, nous, on est là pour éclairer peut-être les parlementaires sur les conséquences que peut avoir une fuite lorsque les données sont utilisées par des personnes malveillantes pour des fins autres ou des fins illégitimes. Alors, voilà, simplement un état des lieux.

Mme Rizqy : Vous comprendrez qu'on ne vous reçoit pas juste pour nous faire un état des lieux. On essaie de... À la fin, nous, on a un travail à faire de parlementaire. Puis je pense qu'on n'est pas mal assez éclairés autour de la table. Dites-moi... Tantôt, vous avez dit : Il faut changer les règles du jeu. Quelles règles voulez-vous changer?

M. Allard (André) : En fait, les règles, on l'a mentionné, on se retrouve dans une situation où le consommateur ignore sa cote de crédit. S'il veut le faire, il doit payer, et là j'ai vérifié ce matin, entre 12 $ et 30 $ par mois pour avoir la même information que l'entreprise avec laquelle il transige possède à son égard. Donc, c'est une situation qui peut effectivement être susceptible ou être préoccupante. Et je terminerais simplement en disant que, s'il y avait un seul élément positif dans cette controverse avec Desjardins, c'est qu'il y a 4,2 millions de personnes qui ont soudainement accès...

Le Président (M. Simard) : Très bien. Merci, monsieur.

M. Allard (André) : ...à son dossier de crédit avec tout ce que les...

Le Président (M. Simard) : Merci. M. le député de Gouin.

M. Nadeau-Dubois : Merci beaucoup d'être ici cet après-midi. Pas que je n'aime pas les banquiers, mais je dois... Je suis capable de leur trouver des qualités, mais c'est bien d'avoir des gens qui, avant tout, se préoccupent de la protection des consommateurs. Vous dites être ici pour faire un état des lieux.

Est-ce que je comprends bien si je dis qu'on a actuellement, d'une part, des entreprises qui veulent offrir du crédit, d'autre part, des institutions financières qui sont aussi des entreprises... souvent, des très grandes entreprises, qui veulent connaître les scores de crédit des individus? Et, au milieu, on a les agences de crédit qui sont, elles aussi, on l'a vu tantôt, de très grandes entreprises, des grandes multinationales. On a tous des grands joueurs très puissants économiquement, qui ont, tous, des intérêts. Les agences de crédit donnent des services non pas aux individus, mais aux entreprises. C'est surtout un intermédiaire entre différentes entreprises.

Qui est là, dans le système actuel, pour protéger les consommateurs, les consommatrices? J'ai l'impression qu'on a plein de grandes entreprises qui se donnent des services entre elles. Qui est là pour protéger les gens ordinaires?

Mme Champoux (Marie-Claude) : Je pense qu'il y a nous, en partie, l'Office de la protection du consommateur. Je pense qu'effectivement la Commission d'accès à l'information peut être là aussi pour la protection des renseignements personnels. Je connais moins l'état des lieux chez eux, mais c'est sûr que nous, c'est notre mission première, la protection des consommateurs, puis on tente de le faire au meilleur de nos ressources et de nos capacités.

M. Nadeau-Dubois : Est-ce que vous jugez que les consommateurs... puis ce n'est pas un critique de votre rôle, là, comprenez-moi bien. Est-ce que vous jugez que les consommateurs, les consommatrices au Québec, actuellement, sont suffisamment protégés?

Mme Champoux (Marie-Claude) : Je dirais qu'à l'Office de la protection du consommateur on souhaite toujours une meilleure protection des consommateurs.

M. Nadeau-Dubois : Est-ce que vous jugez qu'actuellement l'office a tous les outils pour faire son travail?

Mme Champoux (Marie-Claude) : Vous me mettez dans une drôle de position. Je pense qu'à l'office on fait des miracles avec la petite équipe et le petit budget que nous avons.

Le Président (M. Simard) : Merci beaucoup, Mme Champoux. M. le député de Jonquière.

M. Gaudreault : Oui. Merci beaucoup de votre présence. Desjardins, ce matin, a plaidé à plusieurs reprises pour développer ou construire une identité numérique des Québécois et des Québécoises. Comment vous voyez ça? Est-ce que vous avez réfléchi là-dessus? Avez-vous des idées à nous proposer? Et comment cette identité numérique pourrait garantir une plus grande protection des consommateurs?

Mme Champoux (Marie-Claude) : Je dois vous avouer que je n'ai pas l'expertise et je ne pense pas qu'à l'office nous avons l'expertise pour juger de la pertinence ou de l'efficacité d'une identité numérique. On n'a pas cette expertise-là à l'office.

M. Gaudreault : O.K. Mais seriez-vous ouverts à recevoir le mandat, par exemple, du gouvernement, au moins, pour aller chercher les bonnes pratiques à cet égard à l'étranger, toujours dans un souci de protection du consommateur, là?

Mme Champoux (Marie-Claude) : C'est certain que, si le gouvernement ou l'Assemblée nationale nous donnait le mandat, ça nous ferait plaisir de le prendre puis de collaborer avec les experts puis ceux qui connaissent ça définitivement mieux que nous.

M. Gaudreault : Oui, parce qu'il y différentes manières de prendre le problème, mais moi, je pense qu'une des bonnes manières de prendre le problème qu'on a devant nous, c'est vraiment sous l'angle du consommateur, donc sous l'angle de la personne, sous l'angle du citoyen un peu perdu à travers l'ensemble des données et des institutions avec qui il fait affaire et qui sont parfois gigantesques, là, à côté de lui.

En tout cas, on retient ça pour l'instant. Avec le temps qu'il me reste, d'autres collègues l'ont abordé un peu tantôt, mais, si vous aviez une suggestion à nous faire immédiatement... je sais que vous ne voulez pas trop embarquer dans les recommandations, mais je vous demande de le faire pareil. Vous avez parlé de renverser le fardeau de la preuve, d'autres ont parlé de modifier la loi, là, pour s'assurer d'une divulgation obligatoire des incidents, là, de vol de données. Vous iriez où, là, dans tout ça?

Mme Champoux (Marie-Claude) : Je vais réponde ce que nous avons répondu depuis le début. Je suis désolée, mais effectivement on ne fera pas de recommandation ou suggestion, mais ça va nous faire plaisir de travailler avec...

M. Gaudreault : Je vais formuler ma question différemment.

Le Président (M. Simard) : Très succinctement, cher collègue.

M. Gaudreault : Oui. Une divulgation obligatoire des incidents, est-ce que ça permettrait de protéger davantage les consommateurs?

Mme Champoux (Marie-Claude) : Certainement que la transparence, c'est toujours bon pour les consommateurs.

Le Président (M. Simard) : Très bien. Merci beaucoup pour votre participation à cette commission.

Sur ce, nous allons momentanément suspendre nos travaux pour faire place au professeur José Fernandez.

(Suspension de la séance à 17 h 17)

(Reprise à 17 h 20)

Le Président (M. Simard) : À l'ordre, s'il vous plaît! Nous allons reprendre nos travaux.

Nous recevons M. Fernandez, qui est professeur titulaire au département de génie informatique et génie logiciel à Polytechnique Montréal. Cher monsieur, bienvenue parmi nous. Vous savez que vous disposez d'une période de présentation de 10 minutes. Alors, à vous la parole.

M. José Fernandez

M. Fernandez (José) : Merci. Je me présente, donc, José Fernandez. Merci de m'avoir présenté.

Je suis ici en représentation du réseau de chercheurs pancanadiens en cybersécurité, le SERENE-RISC, qui est dirigé par mon collègue le professeur Benoît Dupont, qui s'excuse de ne pas pouvoir être venu présenter les propos de ce réseau.

Comme vous savez, je suis professeur à l'école polytechnique, chercheur en cybersécurité depuis 15 ans, membre de l'Ordre des ingénieurs, et, en tant que professeurs et en tant que chercheurs, nous maintenons plusieurs liens de collaboration avec les agences du gouvernement, l'industrie et, bien sûr, comme vous l'avez sûrement entendu parler, avec le groupe Desjardins, avec lequel nous maintenons des liens de collaboration en termes de recherche et développement en cybersécurité, et ce, depuis 2017.

Donc, vous comprendrez que je ne prendrai pas position sur qu'est-ce qu'il s'est passé à Desjardins en concret, pour la simple raison que je n'ai pas les informations nécessaires, en tant qu'expert, pour analyser le dossier. En temps et... Je crois comprendre aussi que c'est encore sous enquête. En temps et lieu, ces faits ou les résultats de cette enquête pourront être interprétés par des experts dans le domaine, et ce ne sera certainement pas moi.

Ce sur quoi je veux vous parler aujourd'hui, c'est le phénomène généralisé. En tant qu'experts, nous nous sommes tous mis d'accord sur qu'est-ce qu'une fuite de données. Il est important de, en tant que bon professeur d'université, bien clarifier les choses. Quand on parle d'une fuite de données dans un contexte informatique, il y en a deux types. Il y a ce qu'on appelle un incident, et, lorsque l'incident... lorsqu'on a une preuve ou lorsqu'on a un indice qu'il y a eu une pénétration des systèmes informatiques, après ça, il y a une brèche lorsqu'on a vraiment preuve que les informations se sont retrouvées dans les mains d'une personne non autorisée.

Alors, on a deux types d'incidents ici: un dans lequel l'incident se doit à la pénétration des systèmes par quelqu'un de l'extérieur, un accès non autorisé à travers une faille informatique, dans les systèmes ou autre, et l'autre type d'incident, dans lequel on a une menace interne, quelqu'un à l'intérieur, en bon anglais, un «inside job» ou un «inside threat». Un employé ou quelqu'un de proche de l'organisation, à qui on avait donné accès à ces informations-là, va prendre ces informations pour des fins non autorisées.

Alors, les deux cas se retrouvent. Alors, je vais vous citer, par exemple, trois études publiées récemment : un rapport de la compagnie Verizon en 2019, qui fait l'analyse de 40 000 incidents, dont 2 000 sont des brèches confirmées, et on va trouver que, dans ces 2 000 brèches là, dans différentes... trois quarts de ces incidents-là sont dans le secteur bancaire. À peu près entre 20 % à 40 %, selon l'année, sont des «inside threats», des menaces internes, des gens qui sont partis avec des données, qui avaient accès à ces données-là de façon légitime.

Le rapport récent du commissionnaire à la vie privée du gouvernement fédéral... fait possible... justement, par la nouvelle loi qui oblige les compagnies à dévoiler ces informations-là, fait état de statistiques similaires. À peu près 30 %, à peu près un tiers des incidents sont des menaces internes. Également, un rapport publié par nos collègues à l'Université Carnegie Mellon fait état aussi de ce constat-là.

Alors, ce qu'il faut dire ici, c'est qu'en termes de technologie et en termes de procédés, d'arrêter ou de... Quand on parle d'une brèche informatique de quelqu'un de l'externe, on parle surtout de contre-mesures technologiques, des contre-mesures procédurales qui sont là pour surtout prévenir l'entrée non autorisée, alors que, lorsqu'on parle de détecter que quelqu'un va vouloir prendre les informations et les vendre à l'extérieur, là, on est dans les intentions, et c'est très difficile, parce que, là, il faut, à quelque part, l'intention de la personne, et là on est surtout dans les méthodes de détection. Il y a quand même certaines méthodes de détection, mais elles sont très primitives. C'est beaucoup moins mature dans l'industrie, autant en termes de technologies, que de procédés, que la prévention d'attaques externes.

Alors, cette distinction-là est à faire, et lorsque vous serez plus avancés dans vos travaux, et lorsque les faits seront sortis, il faut considérer qu'il y a deux poids, deux mesures, parce que c'est deux choses très différentes, avec des technologies et des procédés très différents.

La raison pour laquelle j'ai accepté de remplacer M. Dupont et venir vous témoigner ici, malgré le fait que je travaille avec Desjardins, c'est parce que je trouvais très important, à ce stade-ci, de souligner quelque chose sur lequel j'ai déjà sorti dans les médias peu après l'incident... enfin, peu après l'incident, j'ai attendu quand même quelques semaines. C'est le vrai problème, ce que je considère être le vrai problème. Je ne suis pas seul, puis beaucoup d'autres experts, entre autres, mes collègues dans le DIACC, le conseil canadien de l'identité et des accès digitaux... C'est le fait qu'en ce moment, au Canada, on n'a pas... ni au Québec, on n'a pas de mécanisme de ce qu'on appelle identité numérique.

Alors, quand on parle d'identité numérique, il faut faire attention. Identité numérique, c'est une chose, c'est de savoir qui est cette personne, mais de savoir à tout coup que cette personne-là n'est pas un imposteur. On parle bien d'authentification, de méthode d'authentification. Alors, aujourd'hui, sur les pages Web, sur l'Internet, ce serait l'usager, mot de passe. Cependant, cette méthode d'authentification n'est bonne que pour les pages Web. Elle ne me permet pas de m'authentifier en personne, elle n'est aussi pas très sécuritaire. Alors, c'est pourquoi il y a maintenant, dans d'autres pays, tel qu'en Europe, surtout, en Estonie, en Belgique, en Espagne, même en Afrique maintenant, le Sierra Leone, la Tunisie... commencent à se doter de moyens pour avoir cette identité numérique ou plutôt des moyens d'authentification. On parle surtout de cartes

d'identité, et ces cartes d'identité permettent maintenant de s'authentifier autant en personne qu'à travers l'Internet, le Web, potentiellement par téléphone aussi pour des transactions avec le gouvernement, mais aussi des transactions dans le secteur privé.

Ce qu'il est important de comprendre, c'est que la technologie derrière ces méthodes d'authentification numérique est la même, essentiellement, que celle des cartes de crédit aujourd'hui. Au Canada, nous avons été innovateurs, en tout cas plus que les Américains, dans la transition vers des cartes à puce dans le secteur bancaire et les cartes de crédit. C'est ce qui fait qu'il y a eu une réduction des fraudes avec les cartes assez importante. Et ce que la plupart des experts se pointent à dire, c'est que, si on pouvait étendre cette même technologie, ce même savoir dans les transactions avec le gouvernement et les autres transactions non bancaires, non financières, on aurait probablement une réduction de ces incidents de vol d'identité. Parce que le problème aujourd'hui, c'est qu'en 2019, excusez-moi, mais c'est tout à fait ridicule que, lorsque j'appelle un fournisseur de services, on me pose comme question de sécurité : Quel est le nom de jeune fille de votre mère? Le nom de jeune fille de votre mère, c'est Tardieu — bonjour, maman — parce que c'est dans ma carte d'assurance maladie. Mon baptistère, ici, en bas de la côte, là, à la paroisse Notre-Dame-de-Foy, ça dit «José Manuel Fernandez Tardieu». Tous mes documents officiels le contiennent. C'est ridicule qu'en 2019 j'aie à cacher ma date d'anniversaire et j'aie à cacher mon adresse, alors qu'elle est sur le CIDREQ, sur le registre des entreprises. Et c'est ça, le problème, on est littéralement encore à l'âge de pierre, et c'est d'autant plus dommage que la technologie derrière ça, en grande partie, a été inventée et développée au Canada.

Alors, c'est sur ça que je vous laisse. Ce désir d'aller vers une meilleure infrastructure d'authentification numérique, ce n'est pas nouveau. Ça fait une trentaine d'années que la technologie existe. On était à la veille de faire ce changement-là au Canada au début des années 2000. Je pense qu'une des raisons pour lesquelles j'ai accepté de venir témoigner ici devant vous, MM. les parlementaires, c'est pour souligner le message que c'est le temps qu'on fasse ce changement-là.

Ce n'est pas seulement une question de sécurité — je veux finir avec ça — c'est aussi une question de développement économique. À partir du moment qu'on a une infrastructure de confiance sur l'identité des personnes, on peut se permettre de faire beaucoup plus en ligne, on peut se permettre de faire beaucoup plus de transactions bancaires, de commerce de façon beaucoup plus efficace, et ça, c'est un accélérateur économique. Il ne faut pas négliger cet effet-là positif de cette transition. Alors, je termine là-dessus, M. le Président.

Le Président (M. Simard) : Merci à vous, M. Fernandez. Je cède maintenant la parole au groupe gouvernemental en vous annonçant une bonne nouvelle, on a majoré légèrement le temps. Vous disposez de 15 min 30 s, tandis...

Une voix : Vous êtes généreux, M. le Président.

Le Président (M. Simard) : Que voulez-vous, ça m'arrive parfois, mais aussi pour l'opposition officielle, qui... étant donné votre grande gentillesse, vous disposez de 10 min 20 s, les deuxième et troisième groupes d'opposition disposent de 2 min 35 s.

Je cède maintenant la parole au député de Charlevoix—Côte-de-Beaupré...

Mme Foster : ...

Le Président (M. Simard) : ...Île d'Orléans. À vous, chère collègue.

Mme Foster : Merci. Merci beaucoup. Merci d'être ici. Puisque vous êtes ici, nous allons profiter de votre expertise. Je comprends que vous ne voulez pas parler de Desjardins. Maintenant, je ferais appel à votre expertise universitaire vaste et large dans le domaine.

On a entendu parler d'un phénomène qui revient tout le temps. On entend parler souvent de ce fameux «dark Web». Est-ce que vous pouvez nous démystifier ça un peu? Comment les données qui proviennent de vols et de fuites circulent sur le «dark Web» après un vol? Quelles sont les possibilités de fraude? Est-ce que ce sont les fraudes... Les fraudes les plus probables sont-elles d'être capables d'ouvrir un compte bancaire ailleurs ou encore d'ouvrir un compte Vidéotron? Vous comprenez un peu, là. Ça mène à quel type de fraude?

M. Fernandez (José) : Oui, vous avez posé plusieurs questions.

Mme Foster : Oui, il y en a deux en une, là, oui, oui, oui.

• *(17 h 30)* •

M. Fernandez (José) : Je vais les prendre une à une. En ce qui concerne le «dark Web», c'est quoi? Le «dark Web», c'est un Internet parallèle qui n'est pas recensé par les moteurs de recherche, par Google. Donc, il est là, ça utilise une technologie très similaire à l'Internet normal, des fureteurs, mais il n'est pas recensé. Donc, à moins que vous sachiez où trouver l'information, ce n'est pas nécessairement très évident de la trouver. Alors, une des conséquences, c'est que c'est difficile pour les corps policiers de retrouver qu'est-ce qui se passe. Et donc c'est un moyen qui est utilisé à des fins tout à fait louables, par exemple, pour éviter la censure dans des pays où c'est moins démocratique, pour pouvoir protéger la vie privée des personnes. Mais aussi des criminels, effectivement, l'utilisent pour pouvoir transiger toutes sortes de choses, de la drogue en ligne, mais pourquoi pas aussi des informations volées en ligne, que ce soient des informations personnelles ou autres.

Le deuxième volet de votre question, et ça revient un peu à mon propos, ce n'est pas seulement les institutions financières qui utilisent les informations personnelles comme mode d'identification. Je vous dirais aujourd'hui que, si je

veux ouvrir un compte dans la plupart des institutions financières, il faut que je me présente, que je présente des pièces d'identité. Mais c'est souvent ce que je... la partie plus «soft», peut-être moins bien protégée, mais qui est aussi dérangeante, c'est effectivement les fournisseurs de services, les Vidéotron, les Hydro-Québec, qui... M. Fernandez, pour des fins de sécurité, pouvez-vous répondre à quelques questions? Et alors est-ce que, là... Bon, bien sûr, dans certains cas, l'impact sera moindre parce qu'il n'y a pas nécessairement de transaction financière, mais ça peut être dérangeant de se faire couper son compte Hydro ou se faire couper son compte téléphone ou autre.

Et, je vous dirais, ça, le point téléphone, c'est important, ça, parce qu'il y a... Une des façons qui a été utilisée pour défrauder, pour faire des attaques ciblées sur des personnes, c'est, justement, d'utiliser ces informations personnelles pour se faire passer par la personne ciblée auprès des compagnies de téléphone, et, à partir de ce moment-là, on peut prendre le contrôle du téléphone et envoyer tous les codes de sécurité. Et ça, c'est quelque chose qui doit changer.

Mme Foster : Equifax donne une protection qui se limite à cinq ans pour ce qui est... l'espèce de surveillance du crédit. Selon votre expertise, est-ce que c'est suffisant ou est-ce que des données peuvent être utilisées largement... parce que ce sont des données intemporelles... que sont le numéro d'assurance sociale, le nom de famille de la... le nom de jeune fille de la mère, bon. Est-ce que, selon vous, cinq ans, c'est suffisant pour ce qui est de la surveillance du crédit?

M. Fernandez (José) : Écoutez, en ce moment, la plupart des informations qui sont utilisées pour l'authentification, donc les données personnelles, presque toutes sont des données permanentes, O.K. : votre nom, votre numéro d'assurance sociale, votre date de naissance. Après ça, il y a l'adresse, etc. Donc, je ne veux pas me prononcer sur — parce que je ne suis pas un expert en fraude bancaire, je comprends bien, mais je ne suis pas un expert — est-ce que cinq ans est suffisant.

Mais ce que je peux commenter, c'est qu'un des problèmes d'utiliser une information personnelle pour l'authentification, c'est qu'on ne peut pas la changer. Et c'est là que, justement, il faut aller à des technologies... au minimum, usager, mot de passe, parce que le mot de passe, on peut le changer. Une carte d'identification, ce n'est pas basé sur la biométrie, on peut la changer. Je la perds, je me la fais voler... C'est ce qu'il arrive en Espagne ou en Belgique, vous perdez votre carte... la faire voler, vous allez voir les corps policiers, ils vous en donnent une autre. Il n'y en a pas, de problème, parce qu'on peut la changer. Et un des problèmes d'utiliser ça, c'est le fait que ce sont des informations pérennes. C'est ça qui fait que... Il y a des gens qui l'ont demandé, mais on ne peut pas vraiment changer son numéro d'assurance sociale.

Mme Foster : O.K. Est-ce qu'on a des moyens de mesurer quelle proportion des victimes de vol, d'incidents, là, de vol de données... qui subissent, effectivement, par la suite, des vraies fraudes ou des vrais vols d'identité? Est-ce qu'on a un moyen?

M. Fernandez (José) : Je suis très content que vous posiez cette question-là. C'est une question qui nous a troublés, moi et mes collaborateurs au Département de criminologie à l'Université de Montréal. M. Dupont... C'est une question qu'on s'est posée puis qu'on essaie d'établir depuis plusieurs années. Et puis on a même essayé de faire des modèles économétriques là-dessus. C'est difficile, O.K., parce qu'on n'a pas une vision globale des marchés noirs de vente. Mais ce qui était le cas et ce qu'on peut voir... ce qu'on a vu, dans les études qu'on a faites il y a quelques années, c'est que le pourcentage reste relativement bas, O.K.? On parle d'entre... les meilleures estimations, entre... peut-être 1 %, mais, au maximum, dans le 5 %. Les taux de... le nombre de mots de passe, de NIP de cartes qui ont été volés, on parle, potentiellement, aux États-Unis, de 10 % à 20 % de tous les numéros de cartes bancaires. Maintenant, quel pourcentage de ceux-là se font frauder? C'est peut-être moins de 1 %, oui. Mais, encore une fois, c'est une science très inexacte.

Mme Foster : O.K.

Le Président (M. Simard) : Merci beaucoup. M. le député de Richelieu.

M. Émond : Merci beaucoup, M. le Président. M. Fernandez, bonjour. Bienvenue parmi nous. Vous l'avez dit d'entrée de jeu, vous êtes ici en remplacement de votre collègue M. Dupont. Et je me dois de préciser que votre présence a été acceptée, consentie par tous les partis qui sont présents ici, à cette commission. Je m'excuse pour cette façon très maladroite, mais très parlementaire, de vous souhaiter la bienvenue parmi nous.

Et puis je comprends que vous ne souhaitez pas parler de Desjardins, puis c'est correct, mais on va plutôt parler de votre expertise. Vous avez parlé d'identité numérique tantôt — très intéressant — de méthodes d'authentification. Vous avez parlé des meilleures pratiques en Belgique, en Espagne, avec un système de cartes d'identité. J'aimerais vous entendre davantage sur cette méthode d'authentification parce que croyez-vous que... On a entendu les gens d'Equifax tantôt qui nous parlaient... Trouvez-vous que les méthodes d'identification pour se connecter à leur service... est-ce que vous les jugez, présentement, suffisamment sécuritaires? Je l'ai fait moi-même tantôt pendant la pause pour accéder à mon propre compte puisque j'ai été parmi les victimes de la fuite de données chez Desjardins puis je vais vous dire que c'est quand même... bien, moi, ça ne me rassure pas vraiment, mais c'est ce qui nous est offert.

Mais j'aimerais vous entendre sur l'identité numérique, comment on pourrait l'améliorer. Parlez-moi davantage de votre carte, ce qu'on retrouve en Belgique, en Espagne, de quelles méthodes... Qu'est-ce qu'on pourrait faire au Québec pour se tourner vers de type d'identité numérique?

M. Fernandez (José) : Alors, moi aussi, je suis un client d'Equifax, étrangement depuis avant la brèche, et moi aussi, je suis un client de Desjardins, et je suis dans la liste fameuse. Donc, effectivement, Equifax utilise une méthode

d'authentification par usager, mot de passe. Je vous dirais que c'est dans les bonnes pratiques, là. Ça, en termes d'un professeur d'université, c'est un C+, là, c'est la moyenne de classe.

Mais je pense qu'au Québec, étant donné qu'on se veut être un leader en termes de hautes technologies, on se veut être un leader aussi en termes de cybersécurité, étant donné le savoir qu'on a, il y a plusieurs universités qui oeuvrent dans le domaine, un écosystème vibrant de start-up et de fournisseurs de services dans ce domaine-là. Je pense qu'étant donné qu'on est aussi dans un contexte canadien, je pense qu'on doit oser avoir meilleur que juste un C+, les moyennes de classe. Et c'est dans ce contexte-là que je pense qu'effectivement on devrait aller vers une authentification numérique.

Alors, l'authentification numérique, c'est quoi? C'est une information secrète qui est sur votre carte numérique, une carte d'identification. Ça peut être un permis de conduire avec une puce. C'est comme une carte de crédit, mais il y a votre photo dessus. Et l'information secrète qui est à l'intérieur de cette puce-là est inviolable. On ne peut pas la sortir. Et il y a un processeur sur cette carte à puce qui fait une opération mathématique, et le résultat de cette opération mathématique là prouve à quiconque le veut que vous êtes vraiment José Fernandez. Et, de plus est, le résultat de ce calcul-là ne peut être utilisé qu'une seule fois.

Donc, si j'ai prouvé à la SAAQ que j'étais José Fernandez pour vendre une auto, cette information-là que la SAAQ aurait temporairement pour vérifier que c'est moi, elle n'est plus valable plus tard pour faire une autre transaction. Donc, si j'avais un «insider», justement, à la SAAQ qui aurait eu accès à ce code mathématique et voudrait faire une transaction frauduleuse plus tard, il ne pourrait pas. Alors, la sécurité de cela se base sur la technologie des cartes à puce.

L'autre possibilité, c'est de mettre ses identifiants sur des téléphones cellulaires, ce qui, dans certains cas, peut être acceptable, mais il y a des risques importants de les mettre sur les téléphones cellulaires étant donné qu'il y a plein d'autres logiciels qu'on installe sur nos portables qui feraient en sorte que ça puisse être dangereux. Mais, dans certains contextes, pour certains types de transactions, ça pourrait être acceptable, comme on le fait aujourd'hui, d'ailleurs, déjà avec nos cartes de crédit puis nos cartes de débit qu'on peut mettre sur nos téléphones.

M. Émond : O.K., merci, tout à fait. Puis, pour information, le gouvernement a mandaté le Centre québécois de l'excellence numérique pour travailler déjà sur l'identité numérique. Ça, c'est ce qui s'en vient, c'est l'après. Mais, dans le maintenant, il y a quand même plusieurs préoccupations qui demeurent. Les gens d'Equifax tantôt... Les personnes qui se sont fait dérober leur identité, dans le cas qui nous occupe aujourd'hui, se sont fait offrir de s'inscrire sur Equifax.

Puis là je me rapporte à des cas très personnels dans ma circonscription, mais que je suis certain qui ont touché l'ensemble des collègues, entre autres, avec les personnes âgées qui ont eu beaucoup de difficultés... Et je ne vais pas revenir sur le fait que le français n'était pas toujours... ou complètement absent du processus, là, mais bien dans le processus lui-même, où c'est la personne qui doit absolument, lui-même, s'inscrire et passer au travers du processus, qui est, pour certaines personnes, pas si simple. Moi, des personnes âgées dans mon comté qui ont eu beaucoup de difficultés puis qui ont effectué un va-et-vient entre le téléphone, la caisse populaire elle-même... puis, dans ce processus-là, personne ne pouvait intervenir à leur place pour les aider dans le processus. Personne, au Mouvement Desjardins, ne pouvait pas, par exemple, procéder à l'inscription avec eux pour les accompagner. Probablement pour des notions de sécurité, là, la personne devait le faire elle-même.

Mais quelles seraient les bonnes pratiques pour être en mesure d'accompagner les Québécois et les Québécoises plus vulnérables ou moins performants pour être capables de faire eux-mêmes l'inscription auprès d'Equifax? Est-ce qu'il existe des méthodes qui permettent d'aider les gens sans entrer dans de nouvelles brèches de sécurité?

• *(17 h 40)* •

M. Fernandez (José) : C'est une excellente question. Et, d'ailleurs, ça, c'est un sujet de recherche qui nous touche beaucoup. Dans le réseau SERENE-RISC, c'est ce qu'on appelle l'utilisabilité de la sécurité. Il y a des chercheurs, comme Sonia Chiasson, à l'Université Carleton, et qui sont des spécialistes dans ce domaine-là, qui disent : Il ne faut pas juste créer des solutions de sécurité qui ne seront pas utilisables, mais il faut aussi regarder le côté psychologique, humain.

Et je vous rejoins là-dessus, sans commenter directement sur la question Equifax, moi aussi, j'ai des parents âgés, et eux, ils sont chanceux, à chaque...ils ont quelqu'un pas loin qui connaît bien ça, qui peut les aider. Mais je suis tout à fait sensible à cette question-là. Et c'est un défi pour nous, les chercheurs, mais, je pense, aussi pour vous, les parlementaires, de s'assurer que les décisions et les programmes qui sont mis de l'avant seront inclusifs de ce type... de cette population-là qui est peut-être moins confortable avec la technologie, effectivement.

M. Émond : Parfait. Merci beaucoup. Je vais passer la parole à un collègue, M. le Président.

Le Président (M. Simard) : M. le député de Saint-Jérôme, à vous la parole. Il vous reste 3 min 20 s.

M. Chassin : Alors, je ne vous demanderai pas votre téléphone pour le passer à ma mère, M. Fernandez. Vous êtes certainement mieux équipé que moi.

Ceci étant dit, je veux revenir... Dans votre présentation, vous avez parlé d'un certain nombre de données que je n'ai pas prises en note, mais où des institutions financières représentaient le trois quarts des cas. Et là, donc, j'essaie de réfléchir à des hypothèses. Pourquoi est-ce que le secteur bancaire semble plus touché par des fuites de données? Est-ce que c'est parce qu'ils sont plus négligents? Est-ce que c'est parce que la valeur des données est plus élevée, et donc peut-être que ce secteur est plus attaqué, ou peut-être parce qu'il détecte davantage les attaques, alors que d'autres entreprises, par exemple, peuvent se faire voler et dérober des données sans nécessairement le réaliser?

C'est des hypothèses que je lance. Dites-nous, selon vous, quelles seraient les hypothèses intéressantes.

M. Fernandez (José) : ...répondre. Alors, je ferai suivre à Mme la secrétaire les références des rapports que j'ai mentionnés, si ça vous est utile.

Alors, le rapport de Verizon a concrètement fait état du fait que la raison principale, hein, ils ont bien regardé en détail ces fraudes-là, c'est parce que ces fraudes-là sont... derrière ces vols d'information, il y a des fraudes bancaires. C'est dans le but de faire de la fraude bancaire. Et, surtout aux États-Unis, c'est commun. Le type de fraude le plus commun, c'est de, tôt dans la saison des impôts, faire des faux retours d'impôt où est-ce qu'on demande un retour d'impôt et on envoie le chèque à une autre adresse, ou on va voler le chèque, ou on fait directement un dépôt direct. Alors, c'est parce qu'on fait de l'argent avec.

Une voix : ...

M. Fernandez (José) : O.K., oui. Maintenant, je veux me permettre un commentaire pas par rapport à Desjardins, mais à l'ensemble des institutions financières au Canada, parce qu'effectivement, dans ses liens industriels, on en a eu d'autres avec d'autres institutions financières au Canada, pas juste Desjardins, mais d'autres, des banques à charte et autres. Et je pense qu'il y a quelqu'un autour de la salle qui pourrait peut-être faire écho là-dessus sans le nommer, mais les budgets de cybersécurité des institutions financières sont en haut, très en haut de la moyenne. Le niveau de maturité de leurs experts et les moyens déployés sont très en haut de la moyenne des autres secteurs de l'industrie. Ça, je suis prêt à l'affirmer, certainement.

M. Chassin : Est-ce que, donc, vous avez essayé de faire de l'économétrie, là, sur combien de fois, quand on est touchés par une fuite de données, on est victimes de fraude? J'aurais tendance à vous poser la question inverse aussi. Combien de fois une entreprise, par exemple, victime d'un vol de données s'en rend compte? Est-ce qu'on a une idée de la proportion?

M. Fernandez (José) : Oui, c'est une bonne question. Comme je vous disais, de détecter qu'il y a eu une fraude ou une pénétration de l'externe est pas mal plus facile que de détecter que quelqu'un est parti avec les données sur une clé USB à l'interne. Il y a des méthodes de détection pour les deux, mais les méthodes de détection de quelqu'un qui avait droit à accéder à ces données-là part avec l'information, c'est beaucoup plus difficile et c'est une technologie et un savoir-faire qui est beaucoup moins mature.

M. Chassin : L'Association des banquiers canadiens nous a parlé, dans le fond, qu'ils militaient — là, je traduis un peu leurs propos — pour que les lois fédérales leur permettent d'échanger davantage d'information entre institutions financières sur les crimes financiers. Est-ce que vous pensez que ça peut être une piste intéressante?

Le Président (M. Simard) : Très rapidement, s'il vous plaît.

M. Fernandez (José) : Écoutez, pas seulement entre eux, mais avec nous, les chercheurs, parce que ça nous permettrait d'arriver à des conclusions peut-être plus intéressantes pour vous, des vrais faits, du «event-based decision-making».

Le Président (M. Simard) : Merci beaucoup. Je cède maintenant la parole à une professeure en service public et chercheure aussi, voilà, Mme la députée de Saint-Laurent.

Mme Rizqy : Merci beaucoup. Juste pour être très claire, le Pr Dupont, lui, il est titulaire de la Chaire de recherche du Canada en sécurité, identité et technologie de l'Université de Montréal. Et vous, Pr Fernandez, vous êtes à la Polytechnique et vous êtes le titulaire de la chaire de recherche industrielle en cybersécurité et intelligence artificielle à la Polytechnique de Montréal. C'est bien ça?

M. Fernandez (José) : Juste pour clarifier, il y a un programme de recherche avec Desjardins, et ce programme de recherche là...

Mme Rizqy : Non, mais je voulais distinguer les deux chaires de recherche. Il y a deux différentes... Il y en a une avec l'Université de Montréal. Donc, c'est juste...

M. Fernandez (José) : Oui, oui, effectivement, il y a une chaire de...

Mme Rizqy : Inquiétez-vous pas, je pose mes questions de façon très précise et chirurgicale habituellement.

M. Fernandez (José) : Oui, d'accord, O.K., d'accord. Oui, M. Dupont a sa chaire de recherche, et moi, j'ai la mienne. Ce sont deux chaires bien différentes.

Mme Rizqy : Parfait. Maintenant qu'on a dit ça, je regarde... Vous savez, quand on est chercheur, souvent, les noms sont importants. Donc, si, par exemple, vous êtes le premier chercheur, votre nom va apparaître, le deuxième et le troisième. Quand je m'en vais sur celui de M. Dupont, je ne vois pas votre nom dans sa chaire de recherche. Je vois d'autres noms

de chercheurs associés. Quand, par contre, je vais sur votre site Web, le premier nom que je vois après Polytechnique, donc, dans vos partenaires, c'est d'abord Desjardins en premier, suivi de Polytechnique. Je vais vous parler...

D'emblée, parce qu'il faut crever l'abcès, il y a des gens qui nous regardent, et aujourd'hui c'est la question à 1 million de dollars, vous ne voulez pas parler de Desjardins, mais la consultation s'appelle Desjardins. Et, en ce moment, c'est que, sincèrement, j'ai un profond malaise parce que le conflit n'a pas été divulgué à nous, les parlementaires. Alors, je vous pose la question. Est-ce que vous, vous avez divulgué votre conflit d'intérêts ici à la secrétaire ou au président de la commission avant de venir ici?

M. Fernandez (José) : Non, parce que j'ai été invité en tant que représentant du groupe SERENE-RISC.

Mme Rizqy : D'accord. En tout respect, je vois votre bac d'ingénieur, et vous êtes au courant que, dans votre code de déontologie, articles 3.05 et 3.03, vous avez aussi un devoir de dénoncer un conflit d'intérêts. Et, parmi la politique, même de la Polytechnique, de laquelle vous êtes professeur, l'article 7.4, Politique relative à l'intégrité ou conflit d'intérêts en recherche... Pour nous, c'était important de le savoir. Puis j'espère que la prochaine fois, si jamais vous êtes invité, vous aurez le réflexe juste de dénoncer votre conflit d'intérêts.

Mais maintenant on va apprécier vos réponses. Et vous avez parlé beaucoup de l'identité numérique. Est-ce que vous avez relaté le nombre de pays qui ont désormais l'identité numérique? Et, si oui, ces pays-là, est-ce qu'ils ont eu des fuites?

M. Fernandez (José) : Je veux juste te faire un commentaire par... Si vous me permettez...

Mme Rizqy : Ah! pour moi, ce sera «vous», ce ne sera pas «tu».

M. Fernandez (José) : Mais l'invitation a eu lieu ce lundi, O.K.? Et la première chose que j'ai faite en arrivant ici, c'est de présenter mon conflit d'intérêts.

Mme Rizqy : L'invitation a eu lieu lundi, on est jeudi. Je pense que... Nous, on l'a appris ce matin dans le journal.

M. Fernandez (José) : Donc, par rapport à votre question, vous m'avez posé la question : Quels sont les pays qui ont déployé une identité numérique? C'est ça?

Mme Rizqy : Quels sont les pays qui ont eu des failles par la suite malgré qu'ils ont l'identité numérique?

M. Fernandez (José) : Écoutez, les trois pays que j'ai mentionnés, qui sont les plus connus, dont les projets d'identité numériques sont le plus avancé ou le plus... sont l'Estonie, l'Espagne et la Belgique. Que je sache, il n'y a pas eu de... Je ne connais pas d'incident par rapport à l'identité numérique déployée par l'État dans ces pays-là.

Mme Rizqy : ...que l'Estonie, malgré qu'elle ait utilisé l'identité numérique, en 2014, il semblerait qu'il y a eu quand même une faille de données assez importante.

M. Fernandez (José) : Je ne suis pas au courant de cette faille de données là.

Mme Rizqy : D'accord. Et est-ce que vous êtes au courant de comment fonctionne la journalisation dans le secteur bancaire?

M. Fernandez (José) : La journalisation, bien sûr, il s'agit de... Bon, que ce soit dans le secteur bancaire ou dans les systèmes informatiques, la journalisation, c'est tout simplement la pratique d'enregistrer les transactions de façon informatique, si on parle au niveau du système informatique, de les enregistrer sur des serveurs dans ce qu'on appelle un journal, oui.

Mme Rizqy : Moi, il n'y a pas... Quand j'étais un peu plus jeune — eh oui, j'ai déjà été un peu plus jeune — je travaillais dans une banque, et, dès lors qu'un membre de mon équipe rentrait dans un dossier qu'il n'avait pas le droit de rentrer, on avait quand même une alerte. On pouvait savoir qu'effectivement telle personne, malgré qu'il n'y a pas eu d'appel, qu'il n'y a pas eu de courriel, aucune demande du client... la personne était entrée dans le dossier et, rapidement, on pouvait le savoir et rencontrer l'employé en question, lui poser certaines questions, et probablement le mettre sous enquête, et même, des fois, conduire à un congédiement. Croyez-vous que la journalisation est quand même assez importante dans les institutions financières, notamment après avoir entendu l'ABC, qui disait que c'est quand même une pratique très courante dans le secteur des banques canadiennes qui sont régies par l'ABC?

• (17 h 50) •

M. Fernandez (José) : Oui. Je ne vais pas faire de commentaire... Enfin, comment dire? De façon générale, quel que soit le secteur industriel, que ce soit le secteur bancaire ou un autre, la journalisation est une bonne idée. Ça fait partie des bonnes pratiques de la sécurité informatique. Et je vous dirais plus, que, justement... La loi Sarbanes-Oxley, aux États-Unis, qui était sur la protection de l'intégrité des états financiers de compagnies cotées en bourse, faisait était que, justement, il fallait déployer des mesures, y compris la journalisation, pour s'assurer qu'il n'y ait pas manipulation de ces données-là. Donc, oui, la journalisation est une bonne pratique, est une pratique standard en sécurité informatique.

Mme Rizqy : O.K. Alors, une institution financière qui collecte quand même beaucoup d'informations et de données... Lorsqu'un employé est mis sur un programme, par exemple, de fidélisation de clients et qu'il a accès à presque tous les clients, mais qu'il n'a pas été mis sous un effet de journalisation, est-ce que ça, ça peut conduire à une plus grande brèche informatique?

M. Fernandez (José) : Répétez la question. Je veux juste... que je comprends bien.

Mme Rizqy : Si vous mettez un employé en charge d'un programme assez important puis qu'il a accès à tous les clients, tout le monde, peu importent les comptes, cette personne-là, tout à coup, se retrouve, là, avec les clés de la maison, est-ce que cette personne-là, le premier réflexe, ça ne serait pas de la mettre dans un programme de journalisation?

M. Fernandez (José) : Ouf! Les programmes de journalisation sont faits au niveau des applications informatiques. On ne fait pas de programme de journalisation pour une personne, O.K., différentes applications. Et, en fait, je ne le sais pas, si vous avez une application Web, par exemple, pour faire une demande de crédit ou autre chose, on va programmer, au niveau de cette application-là, les transactions pour cette application-là.

Mme Rizqy : ...souvent travailler avec un ordinateur de l'employeur, non?

M. Fernandez (José) : Mais ce que je suis en train de vous dire, c'est qu'il est extrêmement difficile de faire un journal de toutes les activités de tous les ordinateurs, de toutes les applications, surtout dans une très, très grande organisation. Alors, c'est très difficile de faire un journal pour toutes les activités. En général, les journaux sont un par application, un pour telle base de données, un pour telle page Web. Et, justement, un des problèmes technologiques importants, qui est, en fait, un problème de recherche aussi, d'innovation, c'est comment centraliser tous ces journaux-là.

Mme Rizqy : Si vous me permettez, puisque le temps file et que je dois aller dans un débat de fin de séance, je vais y aller rapidement. Je ne vous parle pas de tout le monde. Je vous parle de quelqu'un qui confie la clé de la maison puis qu'on lui dit : Vous avez accès à tout le monde, à tous nos clients. Cette personne-là, habituellement, on va s'assurer de faire un suivi très étroit, non?

M. Fernandez (José) : Écoutez, il y a ici deux aspects. Là, si vous me posez une question sur quelles devraient être les pratiques en termes de sécurité du personnel et de vigilance des personnes, ça, ce n'est pas mon domaine, demandez à un ex-policier. Mais, si vous me demandez quelles sont les mesures qui sont mises en place pour surveiller des systèmes informatiques, je vais vous donner la même réponse. En général, cette surveillance-là, elle est faite par application. Alors, si le monsieur théorique que vous disez avait accès à une application critique, et cette application critique là, parce qu'elle est critique, n'est pas journalisée, ça, ce n'est pas très bon. Si cette application-là est critique et journalisée, oui, mais est-ce que ça veut dire que toutes les applications sont enregistrées ou journalisées? Ça, ce n'est pas nécessairement le cas.

Le Président (M. Simard) : M. le député de Robert-Baldwin.

M. Leitão : Très bien. Merci beaucoup.

Le Président (M. Simard) : Il vous reste deux minutes, cher collègue.

M. Leitão : Eh bien, merci, M. le Président. Votre générosité s'est arrêtée là.

Écoutez, on va y aller rapidement. Vous avez mentionné qu'en ce qui concerne les fuites de données il y a essentiellement deux sources, la source extérieure, externe, et la source intérieure. Moi, j'ai une théorie, mais je n'ai pas les moyens de la prouver ou pas, mais j'ai l'impression... Pas une théorie. J'ai l'impression que les institutions financières en général ont mis et mettent beaucoup de ressources sur la détection des menaces extérieures. Donc, tout ce qui est cybersécurité, ils mettent de plus en plus de systèmes et de mécanismes de détection, et on met beaucoup de ressources financières pour contrer ces menaces externes, et que peut-être les menaces internes, les moyens de détection de ces menaces internes n'ont pas nécessairement... ne se sont pas améliorées au même rythme que les mesures de détection des menaces externes. Pensez-vous que c'est une impression qui peut se tenir?

M. Fernandez (José) : Oui, et une des raisons pour ça, c'est que, pour pouvoir détecter l'intention de quelqu'un de faire quelque chose, il faut regarder des données autres que juste les transactions de journal dont parlait votre collègue Mme la députée. Il faut regarder potentiellement d'autres informations pour que ce soit efficace. Il faut regarder les e-mails, il faut regarder sur quels sites Web ils sont allés, O.K.? Et c'est là qu'effectivement il y a des techniques d'intelligence artificielle qui peuvent dire : Ah! cette personne-là, peut-être qu'elle n'est pas contente avec son travail et peut-être qu'elle va faire quelque chose de mauvais. Et la problématique avec ça, c'est une problématique éthique très importante.

Donc, théoriquement, c'est possible. Est-ce qu'on veut vraiment le faire? Et, si on veut le faire, il faudrait que ce soit encadré, parce qu'il y a un revers très important en termes de protection de la vie privée.

M. Leitão : Très rapidement... M. le Président, vous êtes distrait.

Le Président (M. Simard) : Cher collègue...

M. Leitão : Vous êtes distrait. Donc, vous êtes... Je me permets d'y aller rapidement.

Le Président (M. Simard) : ...

M. Leitão : Hein, pardon?

Le Président (M. Simard) : Je suis distrait pour 10 secondes.

M. Leitão : Juste pour mentionner peut-être quelque chose qui pourrait être intéressant, c'est que les...

Le Président (M. Simard) : Très bien. Merci beaucoup, M. le député. M. le député de Gouin, à vous la parole.

M. Nadeau-Dubois : Moi, je suis plus habitué que mon collègue à faire avec peu de temps. Ce n'est pas une qualité, hein, c'est de la nécessité.

D'abord, un bref retour sur cette fameuse question, là, d'apparence de conflit d'intérêts. Je veux prendre le temps de dire ici, au micro, à quel point c'est regrettable, cette situation-là. Et je veux dire que c'est surtout regrettable que vous en soyez l'objet personnellement puis qu'il y ait une controverse médiatique autour de ça, alors que, dans les faits, vous êtes surtout une victime collatérale de la manière que le gouvernement a décidé de travailler, c'est-à-dire extrêmement rapidement et de manière cavalière, avec les oppositions. Si on avait eu le temps de travailler ce mandat d'initiative de manière transpartisane, en prenant le temps de faire les choses, on aurait pu se constituer un bassin d'experts beaucoup plus large, et la situation fâcheuse dans laquelle vous vous trouvez aujourd'hui ne se serait pas produite. Je pense que c'est important de le mentionner d'emblée.

Maintenant, sur le fond, qu'est-ce que les institutions financières au Québec, au Canada devraient faire de mieux pour éviter les situations comme on a vécu chez Desjardins?

M. Fernandez (José) : En ce qui concerne la prévention de cet incident, et je vais faire l'hypothèse non vérifiée que c'est vraiment un «insider threat», écoutez, effectivement, il y a l'analyse à faire, O.K.? Il y a des options technologiques qui sont potentiellement intrusives. Il y a peut-être des... Je pense que tous sont conscients, toutes les banques sont conscientes que ça aurait pu leur arriver. Donc, elles sont toutes préoccupées puis elles sont en train de regarder leurs procédures internes pour voir si on peut faire mieux.

Ce que je trouve... Et ça, c'est important, mais je pense qu'ultimement la façon plus efficace et peut-être plus intéressante pour la société de minimiser les risques... Oui, on peut regarder les banques et les tenir responsables si elles ont fait des erreurs graves. Mais je pense que c'est à nous aussi de nous organiser et dire : Bien, comment est-ce qu'on peut faire pour que, si ça arrive, les conséquences soient minimales, là? Et je reviens encore sur mon discours d'une société où est-ce qu'on a une identification numérique, où le vol de données de la banque ne serait pas si grave que ça.

M. Nadeau-Dubois : Vous avez parlé des bénéfices économiques d'une telle mesure, j'imagine, pour les entreprises elles-mêmes. Pourquoi c'est bon pour les consommateurs, cette mesure-là?

M. Fernandez (José) : Bien, je reviens à ma mère, à mon père. Mon père, qui est mourant, qui a le cancer, il a besoin de faire des transactions pour pouvoir renouveler sa carte de la RAMQ. Bien, il pourrait le faire de chez lui, sur son lit de mort, pour pouvoir avoir ses médicaments, O.K.? Il n'aurait pas besoin de se déplacer.

Le Président (M. Simard) : Très bien. Merci beaucoup, M. le député de Gouin. Je cède maintenant la parole au député de Jonquière.

M. Gaudreault : Oui. Je pense que votre témoignage est un éloquent exemple des conséquences de l'identité numérique. Je veux vous entendre là-dessus, spécifiquement sur la question de l'identité numérique. Est-ce que le Québec est capable d'agir seul pour construire une identité numérique?

M. Fernandez (José) : Oui, oui, parce qu'essentiellement, au Canada, la question de l'identité étant seulement une question provinciale, comment est-ce qu'on prouve notre identité aujourd'hui? On n'a pas de carte d'identité canadienne. On a soit un permis de conduire soit une carte de la RAMQ.

M. Gaudreault : C'est un passeport.

M. Fernandez (José) : Au niveau international, mais le passeport est surtout utilisé pour les transactions internationales. Donc, je pense que, dans un contexte canadien... En Europe, c'est surtout à un niveau national, ce sont... parce qu'il y a un ministère de l'Intérieur, un corps policier national qui émet des cartes d'identité. Dans un contexte canadien, ce que je crois qui est plus raisonnable, c'est que ce soit vraiment à un niveau provincial que ce soit pris étant donné qu'on a déjà l'infrastructure, on a déjà les procédés pour émettre un permis de conduire ou une carte de la SAAQ.

M. Gaudreault : Donc, vous pensez qu'on a tout ce qu'il faut en termes de droit civil, de compétence... parce que cette identité numérique pourrait-elle être applicable sur les banques, considérant que les banques sont de compétence fédérale?

M. Fernandez (José) : C'est une très bonne question. Je ne suis pas un expert en droit, mais je pense qu'en termes d'infrastructures, en termes de procédés, 90 % du travail est déjà fait parce qu'on a des fonctionnaires, on a déjà des procédés pour... Si j'ai besoin d'une nouvelle carte de la RAMQ, un nouveau... cette partie-là, administrative, qui est une grande partie du coût, elle est déjà mise en place.

• *(18 heures)* •

M. Gaudreault : O.K. Moi, je veux aussi quand même faire une référence, là, à votre présence et à votre chaire, qui est supportée par Desjardins, et je voudrais juste préciser quand même... parce que le député de Richelieu, tout à l'heure, faisait référence au fait qu'on avait consenti à votre présence. C'est vrai. Mais, en ce qui nous concerne, on en avait demandé quatre, autres experts, pas parce qu'on n'a pas confiance en vous et pas parce qu'on n'aime pas ce que vous dites, mais, comme dans plein de situations, plein de mandats d'initiative ou de commissions parlementaires de ce type, on peut avoir plusieurs experts comme vous. Mais d'autres institutions, par exemple, le Centre d'études en droit économique, l'UQAM, Michel Carlos, spécialiste dans la lutte contre la fraude, M. Waterhouse, expert en sécurité informatique, ça aurait permis d'aller encore plus loin à partir de vos interventions. Mais le gouvernement a refusé. Donc, on est...

M. Fernandez (José) : Mais, si je me permets...

Le Président (M. Simard) : En conclusion.

M. Fernandez (José) : Si vous permettez, je pense qu'aucun de ces collègues-là, et j'en connais plusieurs, même n'étant pas associé à un programme de recherche de Desjardins, ne se serait prononcé aujourd'hui pour la simple raison qu'on ne connaît pas les faits. Donc, je suis désolé de la situation qui a été causée. Mais, honnêtement, vous auriez fait venir Steve Waterhouse, Éric Parent, Claude Vigeant, ils n'ont pas les faits.

Le Président (M. Simard) : Merci beaucoup. Merci. Alors, Pr Fernandez, merci, pour votre contribution à nos travaux.

Sur ce, j'ajourne...

M. Leitão : ...

Le Président (M. Simard) : Oui? Oui, monsieur... Un instant, s'il vous plaît, cher collègue.

M. Leitão : Avant l'ajournement, j'aimerais...

Le Président (M. Simard) : Bon, s'il vous plaît, collègue, attendez-moi une seconde.

Des voix : ...

Le Président (M. Simard) : À l'ordre, s'il vous plaît! À l'ordre, s'il vous plaît! Je vous demanderais de reprendre vos places. Le député de Robert-Baldwin a demandé la parole.

M. Leitão : M. le député de Jonquière...

Le Président (M. Simard) : Nous avons des questions d'intendance à finaliser ensemble. Ce ne sera pas tellement long.

M. Leitão : Attendez, M. Fernandez, attendez un peu.

Le Président (M. Simard) : D'accord. Alors, voilà, merci pour votre collaboration. M. le député de Robert-Baldwin.

M. Leitão : Merci. Alors, M. le Président, conformément à l'article 176 de notre règlement, je vous demande de nous réunir en séance de travail mardi prochain sur les heures réglementaires de nos travaux afin que notre commission puisse déterminer les conclusions et les recommandations que nous entendons formuler.

Le Président (M. Simard) : Très bien. Alors, j'entends votre demande de respecter l'article 176. Nous allons faire les démarches diligentes et requises pour que nous puissions trouver une date qui nous soit commune à tous. Ça pourrait être celle-là ou une autre. Mais il nous faudra, bien entendu, répondre aux exigences formulées par l'article 176. Et, soit dit en passant, j'en profiterai... pour ceux qui le peuvent, après l'ajournement de nos travaux, si vous pouviez rester pour qu'on puisse voir les plages de disponibles à votre agenda.

Alors, sur ce, merci pour votre excellente collaboration durant cette journée de travail. Et on se retrouve le mardi 26 novembre, à 10 heures, où nous poursuivrons un nouveau mandat. Bonne fin de soirée.

(Fin de la séance à 18 h 03)