SENATE SÉNAT

CANADA

First Session
Forty-second Parliament, 2015-16-17

Proceedings of the Standing Senate Committee on

BANKING, TRADE AND COMMERCE

Chair:
The Honourable DAVID TKACHUK

Thursday, October 26, 2017

Issue No. 27

Consideration of a draft agenda (future business)

and

Third meeting:

Study and report on issues and concerns pertaining to cyber security and cyber fraud

INCLUDING:
THE SEVENTEENTH REPORT OF THE COMMITTEE
(Credit unions and the use of the word "banking")

WITNESSES:
(*See back cover*)

Première session de la quarante-deuxième législature, 2015-2016-2017

Délibérations du Comité sénatorial permanent des

BANQUES ET DU COMMERCE

Président :
L'honorable DAVID TKACHUK

Le jeudi 26 octobre 2017

Fascicule nº 27

Étude d'un projet d'ordre du jour (travaux futurs)

et

Troisième réunion :

Étudier, pour en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude

Y COMPRIS :
LE DIX-SEPTIÈME RAPPORT DU COMITÉ
(Les coopératives de crédit et l'utilisation du terme « opérations bancaires »)

TÉMOINS :
(*Voir à l'endos*)

53584

STANDING SENATE COMMITTEE
ON BANKING, TRADE AND COMMERCE

The Honourable David Tkachuk, *Chair*

The Honourable Joseph A. Day, *Deputy Chair*

and

The Honourable Senators:

Black
Boisvenu
Campbell
Carignan, P.C.
Greene
* Harder, P.C.
(or Bellemare)
Maltais
Massicotte
Moncion
Ringuette
* Smith
(or Martin)
Tannas
Unger
Wetston

*Ex officio members

(Quorum 4)

Changes in membership of the committee:

Pursuant to rule 12-5 and to the order of the Senate of December 7, 2016, membership of the committee was amended as follows:

The Honourable Senator Greene replaced the Honourable Senator Galvez (*October 26, 2017*).

The Honourable Senator Boisvenu replaced the Honourable Senator Enverga (*October 25, 2017*).

The Honourable Senator Galvez replaced the Honourable Senator Wallin (*October 25, 2017*).

COMITÉ SÉNATORIAL PERMANENT
DES BANQUES ET DU COMMERCE

Président : L'honorable David Tkachuk

Vice-président : L'honorable Joseph A. Day

et

Les honorables sénateurs :

Black
Boisvenu
Campbell
Carignan, C.P.
Greene
* Harder, C.P.
(ou Bellemare)
Maltais
Massicotte
Moncion
Ringuette
* Smith
(ou Martin)
Tannas
Unger
Wetston

* Membres d'office

(Quorum 4)

Modifications de la composition du comité :

Conformément à l'article 12-5 du Règlement et à l'ordre adopté par le Sénat le 7 décembre 2016, la liste des membres du comité est modifiée, ainsi qu'il suit :

L'honorable sénateur Greene a remplacé l'honorable sénatrice Galvez (*le 26 octobre 2017*).

L'honorable sénateur Boisvenu a remplacé l'honorable sénateur Enverga (*le 25 octobre 2017*).

L'honorable sénatrice Galvez a remplacé l'honorable sénatrice Wallin (*le 25 octobre 2017*).

Published by the Senate of Canada
Available on the Internet: http://www.parl.gc.ca

Publié par le Sénat du Canada
Disponible sur internet : http://www.parl.gc.ca

MINUTES OF PROCEEDINGS

OTTAWA, Thursday, October 26, 2017
(74)

[*English*]

The Standing Senate Committee on Banking, Trade and Commerce met this day at 10:35 a.m., in room 9, Victoria Building, the chair, the Honourable David Tkachuk, presiding.

Members of the committee present: The Honourable Senators Black, Boisvenu, Campbell, Carignan, P.C., Greene, Maltais, Massicotte, Moncion, Ringuette, Tannas, Tkachuk, Unger and Wetston (13).

In attendance: Adriane Yong, Analyst, Parliamentary Information and Research Services, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, October 17, 2017, the committee continued its study on issues and concerns pertaining to cyber security and cyber fraud. *(For the complete text of the order of reference, see proceedings of the committee, Issue No. 26.)*

WITNESSES:

Canadian Bankers Association:

Darren Hannah, Vice President, Finance, Risk and Prudential Policy;

Andrew Ross, Director, Payments and Cyber Security;

Sandy Stephens, Assistant General Counsel.

The chair made a statement.

Mr. Ross made a statement and, together with Ms. Stephens and Mr. Hannah, answered questions.

At 11:45 a.m., the committee suspended.

At 11:47 a.m., pursuant to rule 12-16(1)(d), the committee resumed in camera to consider a draft agenda (future business) and report.

It was agreed that the draft interim report concerning credit unions and the use of the terms "bank," "banker" and "banking" be adopted with the changes discussed today, and that the Subcommittee on Agenda and Procedure be authorized to approve the final version of the report taking into consideration this meeting's discussions, and with any necessary editorial, grammatical and translation changes required.

It was agreed that the chair be authorized to table the amended report in the Senate, at the earliest opportunity.

PROCÈS-VERBAL

OTTAWA, le jeudi 26 octobre 2017
(74)

[*Traduction*]

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 10 h 35, dans la pièce 9 de l'édifice Victoria sous la présidence de l'honorable David Tkachuk (*président*).

Membres du comité présents : Les honorables sénateurs Black, Boisvenu, Campbell, Carignan, C.P., Greene, Maltais, Massicotte, Moncion, Ringuette, Tannas, Tkachuk, Unger et Wetston (13).

Également présente : Adriane Yong, analyste, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 17 octobre 2017, le comité entreprend son étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude. *(Le texte intégral de l'ordre de renvoi figure au fascicule n° 26 des délibérations du comité.)*

TÉMOINS :

Association des banquiers canadiens :

Darren Hannah, vice-président, Finances, risques et politique prudentielle;

Andrew Ross, directeur, Paiements et cybersécurité;

Sandy Stephens, avocate-conseil adjointe.

Le président a fait une déclaration.

M. Ross fait une déclaration et, avec Mme. Stephens et M. Hannah, répond aux questions.

À 11 h 45, la séance est suspendue.

À 11 h 47, conformément à l'article 12-16(1)d) du Règlement, la séance se poursuit à huis clos afin que le comité examine un projet d'ordre du jour (travaux futurs) et un rapport.

Il est convenu que l'ébauche de rapport provisoire concernant les coopératives de crédit et l'utilisation des termes « banque », « banquier » et « opérations bancaires » en fonction des discussions menées aujourd'hui soit adopté, que le Sous-comité du programme et de la procédure soit autorisé à approuver la version définitive du rapport en tenant compte des discussions d'aujourd'hui, et en y apportant tout changement jugé nécessaire, que ce soit au niveau de la forme, de la grammaire ou de la traduction.

Il est convenu que le président soit autorisé à déposer le rapport modifié au Sénat, dès que possible.

At 11:54 a.m., the committee adjourned to the call of the chair.

À 11 h 54, la séance est levée jusqu'à nouvelle convocation de la présidence.

ATTEST:

ATTESTÉ :

La greffière du comité,

Lynn Gordon

Clerk of the Committee

REPORT OF THE COMMITTEE

Tuesday, October 31, 2017

The Standing Senate Committee on Banking, Trade and Commerce has the honour to table its

SEVENTEENTH REPORT

Your committee, which was authorized by the Senate on Wednesday, January 27, 2016 to examine and report on the present state of the domestic and international financial system, now tables an interim report concerning credit unions and the use of the terms "bank," "banker" and "banking".

Over the course of two meetings, the committee heard testimony regarding the Office of the Superintendent of Financial Institutions' (OSFI) June 2017 advisory about the *Bank Act*'s prohibition on the use of certain terms by financial service providers that are not federally regulated banks.

Section 983 of the *Bank Act* restricts the types of entities that can use the terms "bank," "banker" and "banking" as part of a corporate name or to describe financial products and services. Restricting the use of the term "bank" for the corporate name of a federally regulated bank is reasonable, given the potential for consumer confusion in the evolving financial and fintech services sectors.

However, prohibiting the use of the terms "bank," "banker" and "banking" as verbs and to describe financial products and services is a concern. For decades, credit unions and caisses populaires have used "bank," "banker" and "banking" to describe the products and services they offer to their members, and according to the Department of Finance Canada and OSFI, there have been no complaints or other examples of misunderstanding among consumers about the use of these terms by financial service providers that are not federally regulated banks.

Rather than strictly enforcing section 983, we recommend that the Department of Finance Canada and OSFI continue to consult with the credit unions and caisses populaires to develop a reasonable and practical solution that takes into consideration the current use of these terms by financial service providers and the general public, and permit prudentially regulated deposit-taking entities that are supervised at the federal or provincial level to use these words as verbs to describe their financial products and services.

RAPPORT DU COMITÉ

Le mardi 31 octobre 2017

Le Comité sénatorial permanent des banques et du commerce a l'honneur de déposer son

DIX-SEPTIÈME RAPPORT

Votre comité, qui a été autorisé par le Sénat le mercredi 27 janvier 2016 à examiner, pour en faire rapport, la situation actuelle du régime financier canadien et international dépose maintenant un rapport provisoire concernant les coopératives de crédit et l'utilisation des termes « banque », « banquier » et « opérations bancaires ».

En juin 2017, le Bureau du surintendant des institutions financières (BSIF) a publié un préavis sur l'interdiction faite aux fournisseurs de services financiers, aux termes de la *Loi sur les banques*, d'utiliser certains termes s'ils ne sont pas des banques sous réglementation fédérale. Lors de deux réunions, le comité a entendu des témoignages au sujet de ce préavis.

L'article 983 de la *Loi sur les banques* limite à certaines entités le droit d'utiliser les termes « banque », « banquier » ou « opérations bancaires » dans leur dénomination sociale ou dans la description de leurs produits et services financiers. Il est raisonnable, vu l'évolution du secteur des services financiers et des technologies financières et du risque de confusion qui y existe pour les clients, que seules les banques sous réglementation fédérale soient autorisées à utiliser le terme « banque » dans leur dénomination sociale.

Cependant, l'interdiction des termes « banque », « banquier » et « opérations bancaires » comme verbes et dans les descriptions des produits et services financiers pose problème. Depuis des dizaines d'années, les coopératives de crédit et les caisses populaires utilisent les termes « banque », « banquier » et « opérations bancaires » pour décrire les produits et services qu'elles offrent à leurs membres. Selon le ministère des Finances Canada et le BSIF, l'utilisation de ces termes par des fournisseurs de services financiers qui ne sont pas des banques sous réglementation fédérale n'a suscité aucune plainte ni autre malentendu chez les clients.

Au lieu d'exiger la stricte observation de l'article 983, nous recommandons que le ministère des Finances Canada et le BSIF continuent de consulter les coopératives de crédit et les caisses populaires afin de mettre au point une solution pratique et raisonnable. Cette solution tiendrait compte de l'utilisation actuelle de ces termes par les fournisseurs de services financiers et le grand public et permettrait aux institutions de dépôt, si elles respectent la règle de prudence et sont supervisées aux paliers fédéral ou provincial, d'utiliser ces mots comme des verbes pour décrire leurs produits et services financiers.

The committee looks forward to examining this provision and any proposed amendments during the next statutory review of the *Bank Act* and the federal financial sector framework in 2019.

Respectfully submitted,

Le comité espère étudier cette disposition et son éventuelle modification lorsque la *Loi sur les banques* et le cadre du secteur financier fédéral feront l'objet de leur prochain examen législatif, en 2019.

Respectueusement soumis,

Le président,

DAVID TKACHUK

Chair

EVIDENCE

OTTAWA, Thursday, October 26, 2017

The Standing Senate Committee on Banking, Trade and Commerce met this day at 10:35 a.m. in public, to study and report on issues and concerns pertaining to cyber security and cyber fraud; and in camera, for the consideration of a draft agenda (future business).

Senator David Tkachuk (*Chair*) in the chair.

[*English*]

The Chair: Welcome to our invited guests and members of the general public who are following today's proceedings of the Standing Senate Committee on Banking, Trade and Commerce either here or listening via the web.

My name is David Tkachuk, and I'm the chair of this committee. Today is our fourth meeting studying issues and concerns pertaining to cybersecurity and cyberfraud, including cyber-threats to Canada's financial and commercial sector. In the second portion of our meeting, we will have a brief in camera discussion regarding future business.

I'm pleased to welcome, from the Canadian Bankers Association, Darren Hannah, Vice President, Finance, Risk and Prudential Policy; Andrew Ross, Director, Payments and Cyber Security; and Sandy Stephens, Assistant General Counsel. Thank you for joining us today. After your opening statement, we will have our usual question and answer session. Please proceed.

Andrew Ross, Director, Payments and Cyber Security, Canadian Bankers Association: Good morning. I would like to thank the committee for the opportunity to speak with you today about cybersecurity and cyberfraud. As coincidence may have it, October is Cyber Security Awareness Month, so the committee's hearings are timely.

The CBA is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals.

Banks in Canada are leaders in cybersecurity and have invested heavily to protect the financial system and the personal information of their customers from cyber-threats. Despite the growing number of attempts, banks have an excellent record of protecting their systems from these threats. Banks take seriously the trust that has been placed in them by Canadians to keep their money safe and to protect their personal and financial information.

TÉMOIGNAGES

OTTAWA, le jeudi 26 octobre 2017

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 10 h 35, en séance publique, afin d'étudier, pour en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude, puis à huis clos pour étudier un projet d'ordre du jour (travaux futurs).

Le sénateur David Tkachuk (*président*) occupe le fauteuil.

[*Traduction*]

Le président : Bienvenue à nos invités et aux membres du public qui suivent les travaux du Comité sénatorial permanent des banques et du commerce, ici même, ou via le Web.

Je suis David Tkachuk, président du comité. Nous en sommes à notre quatrième réunion pour l'étude des questions et préoccupations relatives à la cybersécurité et à la cyberfraude, y compris les cybermenaces au secteur financier et commercial du Canada. Dans la deuxième partie de notre réunion, nous aurons un bref huis clos pour discuter des affaires à venir.

Je suis heureux d'accueillir les porte-parole de l'Association des banquiers canadiens, Darren Hannah, vice-président, Finances, risques et politique prudentielle; Andrew Ross, directeur, Paiements et cybersécurité; et Sandy Stephens, avocate-conseil adjointe. Merci d'être là. Votre déclaration initiale sera suivie, comme d'habitude, d'une période de questions et réponses. Veuillez commencer.

Andrew Ross, directeur, Paiements et cybersécurité, Association des banquiers canadiens : Bonjour. J'aimerais commencer par remercier les membres du comité pour cette occasion de vous parler aujourd'hui de cybersécurité et de fraude cybernétique. Les auditions du comité tombent à point, vu qu'octobre est le Mois de la sensibilisation à la cybersécurité.

L'ABC est la voix de plus de 60 banques canadiennes et étrangères qui contribuent à l'essor et à la prospérité économique du pays. L'ABC préconise l'adoption de politiques publiques favorisant le maintien d'un système bancaire solide et dynamique, capable d'aider les Canadiens à atteindre leurs objectifs financiers.

Les banques au Canada sont des chefs de file de la cybersécurité. Elles ont lourdement investi dans les mesures de protection du système financier et des renseignements personnels de leurs clients contre les menaces cybernétiques. Malgré le nombre croissant de tentatives, les banques affichent un excellent bilan en matière de protection de leurs systèmes contre les cybermenaces. En effet, elles prennent au sérieux la confiance que les Canadiens leur accordent pour garder en sécurité leurs dépôts ainsi que leurs renseignements personnels et financiers.

Canadians have come to expect greater convenience when using and accessing financial services, and banks have invested heavily to provide Canadians faster and more convenient ways to do their banking. Now, consumers can bank anytime from virtually anywhere in the world through online banking and mobile apps providing real-time access to their financial information. Today, 72 per cent of Canadians primarily do their banking online or via their mobile device. That's up from 52 per cent just four years ago.

Par ailleurs, les Canadiens s'attendent à plus de simplicité dans l'obtention de services financiers. Les banques ont fait de grands investissements en vue d'assurer à leurs clients des modes d'accès et d'utilisation plus rapides et plus pratiques lorsqu'il s'agit de services bancaires. Les consommateurs peuvent accéder aux services bancaires pratiquement n'importe quand et de n'importe où dans le monde, grâce aux services bancaires en ligne et aux applications bancaires mobiles qui leur donnent un accès en temps réel à leurs renseignements financiers. Aujourd'hui au Canada, 72 p. 100 des consommateurs utilisent principalement les services bancaires en ligne et sur leurs appareils mobiles. Une hausse par rapport aux 52 p. 100 il y a tout juste quatre ans.

As more banking and other transactions are done electronically, networks and systems are becoming increasingly interconnected. This requires banks, government and other sectors to work together to ensure Canada's cybersecurity framework is strong and able to adapt to the digital economy.

Avec l'augmentation d'opérations bancaires, et autres, effectuées électroniquement, les réseaux et les systèmes deviennent de plus en plus interconnectés. Ainsi, les banques, le gouvernement et d'autres secteurs doivent collaborer pour veiller à ce que le cadre de la cybersécurité au Canada soit solide et capable de s'adapter à l'économie numérique.

As the committee is well aware, the Department of Public Safety is currently leading a review of Canada's cybersecurity strategy. The CBA has been an active participant in those consultations, and we would like to outline for the committee many of the recommendations we have already submitted to the government.

Sécurité publique Canada, comme vous le savez bien, a déjà entamé un processus d'examen de la stratégie canadienne en matière de cybersécurité. L'ABC participe activement aux consultations dans le cadre de ce processus. Nous désirons présenter au comité plusieurs des recommandations que nous avons ainsi soumises au gouvernement.

The Canadian cybersecurity framework would benefit from having one lead agency within the federal government to deal with cyber-threats. Within the current cybersecurity landscape, there are many federal government departments and agencies that have oversight of different critical infrastructure sectors. An opportunity exists to integrate all of these government cyberactivities across critical infrastructure sectors into one single government agency. This would improve Canada's resilience by developing common standards, enhancing coordination for intelligent sharing across sectors and with law enforcement, and providing a single point of interaction for consumers and businesses to report cyber-related incidents and cybercrime.

Pour que le cadre de la cybersécurité au Canada soit efficace, un seul organisme fédéral devra assumer la responsabilité des cybermenaces. Dans le paysage actuel de la cybersécurité, divers ministères et organismes fédéraux supervisent différents secteurs des infrastructures essentielles. II est possible d'intégrer, dans un seul organisme fédéral, toutes les activités cybernétiques gouvernementales à travers ces secteurs. Ainsi, la résilience cybernétique du Canada sera raffermie grâce au développement de normes communes, à la coordination améliorée du partage des renseignements entre les divers secteurs et avec les forces de l'ordre, et à la présence d'un seul point d'interaction pour que les consommateurs et les entreprises puissent signaler les incidents et les crimes cybernétiques.

The delivery of financial services relies on other sectors, such as telecommunications and electricity. Canadians need to be assured that all critical infrastructure sectors are protecting them from cyber-threats. Therefore, we encourage the government to create a consistent set of standards and rules for all critical infrastructure sectors. Consistent standards will provide stronger oversight and greater comfort to those using and relying on these services.

La prestation des services financiers dépend d'autres secteurs, comme les télécommunications et l'électricité. Il faut que les Canadiens soient rassurés du fait que tous les secteurs des infrastructures essentielles les protègent contre les cybermenaces. À cette fin, nous encourageons le gouvernement à établir un ensemble uniforme de normes et de règles qui s'appliquent à tous les secteurs des infrastructures essentielles. Des normes uniformes permettront une supervision plus rigoureuse et rassureront ceux qui utilisent ces services et en dépendent.

The telecommunications sector is the conduit through which electronic data flows. Identifying and blocking malicious traffic and sharing that information across sectors would benefit

Le secteur des télécommunications est le canal de diffusion des données électroniques. L'identification et le blocage du trafic malveillant, et le partage de ces renseignements avec tous les

consumers and businesses, including banks. Once a cyber-threat is identified, allowing telecommunications providers to block known malicious traffic can help stop further transmission of bad data. Blocking bad data would significantly reduce the volume of malicious e-mails that target those most vulnerable, such as consumers and small businesses. This would also limit the spread of viruses, botnets and other forms of malicious software that target corporations and governments. It is our understanding that legislative changes are needed to allow telecommunications providers to proactively block bad traffic, and we encourage the government to study legislative options for making this possible.

secteurs d'activité seront à l'avantage des consommateurs et des entreprises, dont les banques. Une fois qu'une cybermenace est identifiée, autoriser les fournisseurs de services de télécommunications à bloquer le trafic malveillant ainsi repéré contribuera à arrêter la transmission ultérieure de mauvaises données. Le blocage des données malveillantes réduira considérablement le volume des courriels malicieux qui visent les destinataires vulnérables, comme les consommateurs et les petites entreprises. Ce blocage contribuera également à limiter la propagation de virus, de réseaux zombies et d'autres formes de maliciels lancés contre les organisations et les gouvernements. II nous semble que des changements législatifs sont de mise pour permettre aux fournisseurs de services de télécommunications de bloquer le trafic malveillant de façon proactive. Nous encourageons le gouvernement à examiner les options législatives pour y arriver.

Canadian banks and other businesses are also customers of telecommunications companies. Enabling those companies to share threat information with relevant customers would help improve cyber-resiliency. The converse is also true. The financial sector has invested heavily in robust cyber-resilience capabilities to identify malicious data on its systems. Sharing this information with telecommunications companies and allowing them to block malicious end points would stop traffic from spreading to other businesses and consumers. Accordingly, any legislative changes should enable this two-way sharing of information.

En outre, les banques et autres entreprises canadiennes comptent parmi les clients des sociétés de télécommunications. Donner aux sociétés de télécommunications les moyens de partager les renseignements au sujet des menaces avec les clients adéquats permettra à ces derniers d'améliorer leur résilience cybernétique. L'inverse est également vrai. Le secteur financier a massivement investi dans de grandes capacités de résilience cybernétique afin de pouvoir identifier les données malveillantes sur ses systèmes. Partager ces renseignements avec les sociétés de télécommunications — et les autoriser à bloquer les terminaux malveillants — contribuera à arrêter la propagation du flux à d'autres entreprises et aux consommateurs. Par conséquent, tout changement législatif devra permettre ce partage de renseignements bidirectionnel.

The benefits of sharing threat information extend beyond the financial and telecommunications sectors to other sectors, government and law enforcement. Rapid intelligent sharing of threats is a highly effective means of minimizing the impact of cyber-threats. In order to achieve timely sharing between the private sector and government agencies, improved sharing protocols and control integration is required. We support initiatives such as the Canadian Cyber Threat Exchange, which promotes the exchange of cybersecurity information and best practices between government and businesses.

Les bénéfices du partage des renseignements sur les cybermenaces s'étendent à d'autres secteurs que les finances et les télécommunications, au gouvernement et aux forces de l'ordre. Le partage rapide des renseignements au sujet des cybermenaces est un moyen hautement efficace pour minimiser l'impact des cyberattaques. II est nécessaire de mettre en œuvre de meilleurs protocoles de communication et une intégration des contrôles afin d'arriver à un partage opportun de renseignements entre le secteur privé et les organismes gouvernementaux. Nous appuyons les initiatives comme l'Échange canadien de menaces cybernétiques, qui encourage l'échange de renseignements sur la cybersécurité et les pratiques exemplaires entre le gouvernement et les entreprises.

While we support greater information sharing, we recognize that security and privacy go hand in hand. The Personal Information Protection and Electronic Documents Act, or PIPEDA, balances the privacy rights of individuals with the needs of organizations to collect, use and disclose personal information in the course of carrying out their business. However, recent amendments to PIPEDA impede the ability of organizations to share personal data to detect, prevent and suppress cybercrime. Banks fully support and adhere to PIPEDA; however, a mechanism to share information about

Nous encourageons certes un plus grand échange de renseignements, mais nous sommes conscients du fait que la sécurité et la confidentialité vont de pair. La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) assure l'équilibre entre les droits à la confidentialité des particuliers et le besoin des organisations de recueillir, d'utiliser et de communiquer les renseignements personnels dans le cadre de leurs activités. Toutefois, de récentes modifications à la LPRPDE entravent la capacité des organisations de communiquer des renseignements personnels en vue de détecter,

cyber-criminals will be necessary to improve Canada's cyber-resilience.

de prévenir et de neutraliser la cybercriminalité. Les banques appuient pleinement la LPRPDE et s'y conforment. Néanmoins, un mécanisme de partage de renseignements sur les cybercriminels est essentiel pour améliorer la résilience cybernétique du Canada.

Similar to initiatives to improve financial literacy, we also recommend the development of a national cyberliteracy program. Cyber-criminals often target ordinary citizens; thus, greater cyberawareness is needed to reduce the number of victims. A national cyberliteracy program that educates and helps protect consumers would help to deal with current and future threats.

Tout comme les initiatives axées sur le rehaussement du niveau de littératie financière, nous recommandons l'élaboration d'un programme national de littératie cybernétique. Puisque les cybercriminels s'attaquent souvent à des citoyens ordinaires, la sensibilisation à la cybersécurité devient essentielle pour réduire le nombre de victimes. Un programme national de littératie cybernétique, destiné à l'éducation et à la protection des consommateurs, contribuera à traiter les menaces actuelles et à venir.

Today, there is a global shortage of cybersecurity personnel. A talent pool to address the demand is required, both now and for the future. Building Canada's talent pool requires improved educational options for careers in cybersecurity, retraining options for the existing workforce, mature career development management practices and creative cross-pollination with high-demand disciplines that are closely linked to cybersecurity. We believe Canada has an enormous opportunity to leverage our strong education systems and to retrain our highly educated workforce to fill that gap.

De nos jours, il existe un manque général de personnel dans le domaine de la cybersécurité, d'où l'importance de produire un bassin de talents pour répondre à la demande présente et future. Constituer un bassin de talents au Canada passe, entre autres, par de meilleurs programmes éducatifs pour une carrière en cybersécurité, la formation du personnel actuel, des pratiques avérées de gestion du développement des carrières, ainsi qu'une pollinisation croisée créative avec des disciplines en forte demande et étroitement liées à la cybersécurité. Nous sommes d'avis que le Canada est en mesure de tirer profit de notre excellent système d'éducation et de recycler notre main-d'œuvre hautement qualifiée afin de combler cette lacune.

As the financial sector undergoes tremendous change driven by technology, new entrants are able to deliver financial services digitally, fuelling competition. Of course, increased competition has a positive impact in the marketplace, accelerating innovation and increasing choice for Canadians. Throughout this change, protecting consumers' security and privacy while ensuring the safety, soundness and stability of the overall financial system in Canada remains paramount.

Alors que le secteur financier est le terrain d'importants changements provoqués par la technologie, les nouveaux acteurs arrivent à livrer les services financiers de façon numérique, attisant la concurrence. Évidemment, une plus grande concurrence a des effets positifs sur le marché, car elle stimule l'innovation et élargit le choix offert aux consommateurs. Tout au long de ce processus de changement, veiller à la préservation de la sécurité et de la confidentialité des consommateurs, ainsi qu'à la sécurité, à la robustesse et à la stabilité du système financier canadien dans son ensemble, demeure primordial.

Most new technology-based financial services firms are less regulated than established financial institutions, and many are largely unregulated. This makes it difficult to assess the cyber-resilience of these firms. Some may have the same risk controls as banks; however, most will not possess the same depth of experience in defending and protecting data in the rapidly evolving digital threat environment. Further, the connected nature of financial services means that this growing list of market participants has the ability to spread cybercontagion throughout the sector. As a result, cyber-resilience needs to be a central consideration for policymakers when defining the future framework for financial services.

La plupart des nouvelles entreprises de technologie financière sont moins réglementées que les institutions financières établies, et nombreuses d'entre elles ne le sont pratiquement pas. II est donc difficile d'évaluer la résilience cybernétique de ces entreprises. Certaines pourraient certes avoir les mêmes contrôles des risques que les banques. Or, la plupart n'ont pas la même vaste expérience en matière de défense et de protection des données dans l'environnement de menaces numériques en rapide évolution. En outre, le fait que les services financiers soient connectés signifie que ce nombre croissant de participants sur le marché a le potentiel d'être un contaminant cybernétique pour le secteur. Pour cette raison, la résilience cybernétique doit être au centre des considérations des législateurs qui tracent l'avenir du cadre législatif en matière de services financiers.

In conclusion, I want to reiterate that cybersecurity is a priority for Canada's banks. They continue to collaborate and invest to protect Canadians' personal and financial information. Banks support the government's work to protect Canadians while promoting innovation and competition. However, the industry recognizes that threats and challenges are constantly evolving. We want to work more collaboratively with the government and other sectors. In order to achieve that objective, we encourage the federal government to finalize and implement its renewed cybersecurity strategy to protect Canadians and improve Canada's cyber-resilience.

En conclusion, je souligne de nouveau que la cybersécurité est une priorité pour les banques au Canada. Les banques continuent à collaborer et à investir dans l'objectif de protéger les renseignements personnels et financiers des consommateurs. Également, elles appuient le travail du gouvernement dans la protection des Canadiens tout en encourageant l'innovation et la concurrence. Ceci dit, le secteur bancaire est conscient de l'évolution perpétuelle des menaces et des défis, et désire collaborer davantage avec le gouvernement et avec les autres secteurs. À cette fin, nous encourageons le gouvernement fédéral à mettre au point et à implanter sa nouvelle stratégie en matière de cybersécurité, qui vise à protéger les Canadiens et à améliorer la résilience cybernétique du Canada.

Thank you very much for your time, and I look forward to your questions.

Je vous remercie du temps que vous nous avez accordé et je serai heureux de répondre à vos questions.

The Chair: Thank you. We will begin questions.

Le président : Merci. Nous allons passer aux questions.

[*Translation*]

Senator Boisvenu: Welcome to our witnesses. Thank you for your excellent presentation, Mr. Ross. I have a few questions for you. First, have you prepared an inventory or done research on the origins of cyberattacks against the financial sector in Canada? Are some of these attacks related to terrorist organizations?

[*English*]

Mr. Ross: It's safe to say that in many cases, origins are tracked, but it's also true to recognize that this is a global phenomenon; it's a borderless issue. As much as we may have some of that information, looking at nation states or particular sectors or countries actually does not necessarily address the full picture of ensuring resilience for the country.

[*Translation*]

Senator Boisvenu: There are two components in the financial sector: the portfolio administrators and those who invest their savings. Are these cyberattacks putting those savings at risk at this time? If there are no investors in the financial sector, there will be no sector as such. Is the security barrier between the administrators and the investors relatively secure, or are there risks for the investors?

[*English*]

Mr. Ross: First, let me assure you that banks treat cybersecurity as vitally important. Trust is paramount to everything banks do. The banks have invested heavily to ensure the cyber-resilience of their systems.

[*Français*]

Le sénateur Boisvenu : Bienvenue à nos invités. Merci de votre excellent exposé, monsieur Ross. J'ai quelques questions à vous poser. D'abord, avez-vous fait un inventaire ou une recherche sur la provenance des cyberattaques qui touchent le milieu financier au Canada? Est-ce que certaines de ces attaques sont liées à des organismes terroristes?

[*Traduction*]

M. Ross : On peut dire sans trop risquer de se tromper qu'il est bien souvent possible de remonter aux origines, mais il faut aussi reconnaître que c'est un phénomène mondial, qui ne connaît pas de frontières. Nous avons beau avoir une partie de cette information, l'examen des États-nations ou des secteurs ou pays particuliers ne permet pas nécessairement de dégager l'ensemble du tableau de la résilience du pays.

[*Français*]

Le sénateur Boisvenu : Il y a deux composantes dans le domaine financier : les administrateurs de portefeuille et les épargnants. Est-ce que, actuellement, ces cyberattaques mettent à risque les épargnants comme tels? S'il n'y a pas d'épargnants dans le domaine financier, il n'y a pas de système qui se tient. Est-ce que la barrière de sécurité entre les administrateurs et les épargnants est relativement sécuritaire ou y a-t-il des risques pour les épargnants?

[*Traduction*]

M. Ross : Tout d'abord, je peux vous assurer que les banques attachent une importance cruciale à la cybersécurité. La confiance est primordiale dans tout ce qu'elles font. Les banques ont investi gros dans la résilience cybernétique de leurs systèmes.

So the direct answer to your question is that Canadians' money is safe in Canadian banks.

[*Translation*]

Senator Boisvenu: When I read your brief, Mr. Ross, I got the impression that the Canadian system was relatively behind with regard to the management of cybersecurity. Is this a global phenomenon, or is Canada currently lagging behind other countries?

[*English*]

Mr. Ross: You recognize this is a worldwide phenomenon. It's also safe to say that the threat continues to evolve. Canada and other countries must evolve with it.

It is fair to say that other countries have developed and started to implement revised strategies, which is why we are encouraging the Canadian government to act quickly to implement the strategy being contemplated today.

Senator Moncion: I have a few questions, but they are all related. First, explain how you work with other financial institutions to avoid the spreading of attacks. How many attacks do you get a day? What are the losses incurred year over year? What has happened over the years? Because I think it started very high and I think it is going down. And how does the Equifax breach affect your members?

Mr. Ross: First, as it relates to collaboration, the banks in Canada work very closely among themselves and across other sectors, including law enforcement and government. The banks are involved in things like the cyber-threat exchange and CCIRC. We have great relationships with law enforcement and other agencies. From that perspective, I believe, and I think you have heard in some of the hearings you have had up to now, that the financial sector takes a leadership position as it relates to cybersecurity.

In terms of numbers and data, I would say that Canada continues to protect the assets of Canadians, although we always hear the bad things in the news. It's safe to say that obviously the digital economy has also created enormous opportunity, so we are seeing more volume going through digital channels than we would have before. We need to keep in mind not just the raw numbers but how those numbers equate to the opportunities that have presented themselves.

Pour répondre directement à votre question, disons que l'argent des Canadiens est en sécurité dans les banques canadiennes.

[*Français*]

Le sénateur Boisvenu : En lisant votre mémoire, monsieur Ross, j'ai eu l'impression que le système canadien est relativement en retard quant à la gestion de la sécurité cybernétique. Est-ce un phénomène mondial ou est-ce que le Canada, en ce qui a trait à la situation actuelle, est en retard sur d'autres pays?

[*Traduction*]

M. Ross : Vous reconnaissez que le phénomène est mondial. On peut aussi dire sans risquer de se tromper que la menace n'a pas fini d'évoluer. Le Canada et les autres pays doivent évoluer avec elle.

Il est juste de dire que d'autres pays ont révisé leurs stratégies et commencé à mettre en œuvre leurs nouvelles stratégies. C'est pourquoi nous pressons le gouvernement canadien à agir rapidement pour mettre en œuvre la stratégie envisagée aujourd'hui.

La sénatrice Moncion : J'ai quelques questions, mais elles sont toutes reliées. En premier lieu, expliquez comment vous collaborez avec les autres institutions financières pour freiner la propagation des attaques. Combien d'attaques avez-vous par jour? Quelles sont les pertes subies d'une année à l'autre? Qu'est-il arrivé au fil des ans? Parce que je pense que c'est parti de très haut et que cela diminue. Et quelle incidence l'attaque sur Equifax a-t-elle sur vos membres?

M. Ross : Tout d'abord, pour ce qui est de la collaboration, les banques au Canada collaborent très étroitement entre elles et avec d'autres secteurs, dont les forces de l'ordre et le gouvernement. Les banques participent à des activités comme l'échange des cybermenaces et le CCRIC. Nous avons d'excellents rapports avec les forces de l'ordre et d'autres organismes. Dans cette optique, je pense — et vous avez dû l'entendre dans vos audiences — que le secteur financier assume une position de tête dans la cybersécurité.

Au niveau des chiffres et des données, je dirais que le Canada continue de protéger les avoirs des Canadiens, même si l'actualité ne s'intéresse toujours qu'aux mauvaises nouvelles. On ne se trompe pas en disant que l'économie numérique a ouvert d'immenses perspectives, de sorte que nous n'avons jamais vu autant de volume transiter par les canaux numériques. Nous devons garder à l'esprit non seulement les chiffres bruts, mais aussi la façon dont ils reflètent les occasions qui se sont présentées.

Sandy Stephens, Assistant General Counsel, Canadian Bankers Association: Banks obviously want to mitigate any harm that could come to their customers, so they would work with third parties to ensure that if they are able to help mitigate the harm to their customers, that they are able to do so. In this instance, credit card numbers have been provided to the banks by the networks, and they will monitor those credit cards for any unusual transaction. If they see any unusual activity, they will take appropriate steps, which could include notifying their customers.

Senator Moncion: How did Equifax affect your business?

Ms. Stephens: With regard to their breach, I know that Equifax did notify the impacted customers directly. I can't speak to the banks' interactions with Equifax as far as their business relationship.

Senator Moncion: What would be your concern, or are you concerned about that breach? Equifax is used by all financial institutions.

Ms. Stephens: Absolutely. Our banks will be looking into this matter and ensuring that services that they use and their customers' information is protected.

Mr. Ross: If I can add to that, our recommendations point a lot to resilience. Obviously any breach, regardless of size, is an issue. It impacts customers and businesses. It's not good for anyone. What we are advocating for is continuing to get in front of it and ensuring that Canadians are protected so that we do not have those types of breaches.

The Chair: When the information from Equifax was breached, did that information include not only the names of individuals but perhaps other matters that a credit agency would ask? Would it have included the customer, as in my case, the Royal Bank or Bank of Montreal? Would it have included all that information?

Darren Hannah, Vice President, Finance, Risk and Prudential Policy, Canadian Bankers Association: Just to be clear, senator, at this stage, only Equifax knows the extent of what the breach was. To get a precise answer to that question, you ultimately have to ask Equifax.

Are banks diligent about this? Absolutely. At the end of the day, a number of these people may well be bank clients. We want to be sure that our clients are properly protected.

The Chair: Would it not be the responsibility of Equifax to get ahold of the banks as soon as this happened to let them know that perhaps their customers have been jeopardized?

Sandy Stephens, avocate-conseil adjointe, Association des banquiers canadiens : Certes, les banques veulent atténuer le préjudice qui pourrait menacer leurs clients, ce pour quoi elles collaborent avec des tierces parties. Dans ce cas-ci, les réseaux ont fourni des numéros de carte de crédit aux banques, qui les surveilleront dans toute transaction inusitée. Si elles constatent une activité qui sort de l'ordinaire, elles prendront les mesures qui s'imposent, notamment en avisant leurs clients.

La sénatrice Moncion : Quelle a été l'influence d'Equifax sur vos affaires?

Mme Stephens : Equifax a informé directement sa clientèle de la violation de ses données. Je ne peux pas parler des relations d'affaires des banques avec Equifax.

La sénatrice Moncion : Qu'est-ce qui vous inquiéterait? Ou est-ce que cette violation vous inquiète? Toutes les institutions financières utilisent les services d'Equifax.

Mme Stephens : Absolument. Nos banques se pencheront sur l'affaire et vérifieront que les services qu'elles utilisent et les renseignements de leur clientèle sont protégés.

M. Ross : Permettez-moi d'ajouter un commentaire. Nos recommandations mettent nettement l'accent sur la résilience. Bien sûr, toute violation, quelle qu'en soit l'ampleur, est un problème. Elle touche la clientèle et les entreprises. Ce n'est bon pour personne. Nous préconisons de continuer de bloquer le problème et de voir à protéger les Canadiens contre ces genres de violations.

Le président : Lors de la violation chez Equifax, l'information comprenait-elle non seulement les noms des particuliers, mais peut-être aussi d'autres détails susceptibles d'intéresser une agence de crédit. L'information aurait-elle précisé le client, comme dans mon cas, la Banque Royale ou la Banque de Montréal? Toute cette information aurait-elle été là?

Darren Hannah, vice-président, Finances, risques et politique prudentielle, Association des banquiers canadiens : Soyons clairs, sénateur : à ce stade-ci, seule Equifax connaît l'ampleur de la violation. Pour avoir une réponse précise à votre question, il faudra en fin de compte la poser à Equifax.

Les banques font-elles preuve de diligence sur ce point? Absolument. Au bout du compte, plusieurs de ces personnes sont peut-être les clients des banques. Nous voulons être certains que nos clients sont bien protégés.

Le président : Ne serait-il pas de la responsabilité d'Equifax de prévenir tout de suite les banques que leurs clients ont peut-être été victimes?

Mr. Hannah: We certainly have encouraged Equifax to be as forthcoming as they can. Certainly there has been dialogue. At the end of the day, I think your question was what specific information was potentially compromised. It's a question that has to be addressed by Equifax. They are the only ones who can answer that question with certainty.

The Chair: I'm surprised they would not have provided that to their customers, their banks. If a bank is their customer, should they not have provided that information and said, "Look, we have a problem; 10,000 of your customers' data have been jeopardized"? Would that not have been provided almost immediately?

Ms. Stephens: Equifax has been in dialogue with their customers and with the banks.

Senator Moncion: The bank is the customer of Equifax, not your customers. You are using the service so that you can get information on your customers, so the responsibility lies with the financial institution. If the breach comes, you're responsible at the end of the day for the information that is provided by you to Equifax. I find the answer a little bit awkward. You're saying that Equifax will get in touch with your customers, when you are the customer of Equifax, not me as a bank customer.

Ms. Stephens: I think that Equifax will have products that are direct to a consumer as well, but definitely banks work with third parties to mitigate the risk to their customers, so if there is a way that banks can manage to help mitigate a risk, but the actual breach was with Equifax and they have notified those customers. They have the data that would allow them to assess that risk and notify the impacted consumers.

Senator Unger: Thank you for your presentation. Speaking of a breach, a week ago researchers at a university in Belgium announced that they had discovered a way to completely defeat the encryption on Wi-Fi networks. It's alarming, but the response from government agencies and the media has been quite muted about this issue. I'm assuming that you're aware of it.

Mr. Ross: We are certainly aware of it. We hear stories of these types of things all the time. One of the benefits of researchers is obviously to identify where there may be gaps or issues prior to malicious actors identifying them. That's something that banks obviously are informed of. It is expected that providers would also be informed of that and that remediation plans would be put in place and that those who use those types of systems would in fact patch those systems to ensure that no one is affected.

Mr. Hannah: Senator, if I can build on what my colleague has said, in some respects, what you're saying points to why we made the recommendations we have made. Ultimately,

M. Hannah : Bien sûr, nous avons incité Equifax à faire preuve de la plus grande transparence. Bien sûr, il y a eu un dialogue. En définitive, je pense que vous vouliez savoir quels renseignements précis auraient pu être compromis. C'est à Equifax d'examiner la question. Personne d'autre ne peut répondre à cette question avec certitude.

Le président : Je suis surpris qu'Equifax n'ait pas fourni cela à ses clients, à ses banques. N'aurait-elle pas dû fournir cette information aux banques clientes en disant : « Écoutez, nous avons un problème; 10 000 données de vos clients ont été compromises »? Cela n'aurait-il pas dû être fait presque immédiatement?

Mme Stephens : Equifax a discuté avec ses clients et avec les banques.

La sénatrice Moncion : C'est la banque qui transige avec Equifax, pas vos clients à vous. Vous utilisez les services d'Equifax pour obtenir de l'information sur vos clients, si bien que la responsabilité revient à l'institution financière. En cas de violation, c'est vous qui êtes responsable en définitive de l'information que vous fournissez à Equifax. Je trouve la réponse un peu faible. Vous dites qu'Equifax va prendre contact avec vos clients. Mais le client d'Equifax, c'est vous; pas moi comme cliente de la banque.

Mme Stephens : Je pense qu'Equifax aura des produits destinés directement aux consommateurs également, mais il est certain que les banques travaillent avec des tiers pour atténuer les risques pour leurs clients… S'il y a un moyen pour les banques d'aider à atténuer le risque… Mais la violation est survenue chez Equifax, qui a avisé ces clients. Elle a les données qui lui permettraient d'évaluer le risque et d'informer les consommateurs concernés.

La sénatrice Unger : Merci de votre exposé. Parlant de violation, la semaine dernière, des chercheurs d'une université belge ont annoncé la découverte d'un moyen de déjouer complètement le chiffrement des réseaux Wi-Fi. Voilà de quoi inquiéter, mais la réaction des organismes gouvernementaux et des médias a été plutôt timide. Je suppose que vous êtes au courant.

M. Ross : Oui, bien sûr. Nous entendons toujours parler de ce genre de choses. Un des avantages des chercheurs est évidemment de découvrir les lacunes ou les problèmes avant les personnes malveillantes. Les banques en sont évidemment prévenues. On s'attend que les fournisseurs en soient aussi informés et mettent en place des plans de correction et que les utilisateurs de ce type de systèmes installent des rustines pour protéger tout le monde.

M. Hannah : Madame la sénatrice, j'aimerais renchérir sur les propos de mon collègue. À certains égards, vous demandez pourquoi nous avons fait les recommandations que nous avons

cybersecurity has to be a layered approach. There has to be information sharing to try to build resilience; there has to be traffic monitoring to reduce the amount of malicious traffic that filters through; there has to then be education awareness so that I know, as a consumer or as an individual, what to look for. Ultimately, it has to be a multilayered approach because at the end of the day the threat evolves all the time. The intent is to have multiple layers so there is awareness, there is prevention and there is greater capacity to respond.

Senator Unger: This breach is specifically known as Krack. It has discovered a way to completely defeat the encryption that WPA2 provides on Wi-Fi networks. It affects all modern Wi-Fi equipment for mobile phones, tablets and work stations, routers, printers and the usual things.

My question is specific to Krack. Have you found a way to notify your clients? This issue is not really being talked about. It's only coming from sort of top levels, although there is a large article that was released by the *National Post* in a specific article. They talk about "it could be about to hit the Wi-Fi fan." Specifically, with regard to Krack, have you done anything to alert clients of banks?

Mr. Hannah: The challenge with something of that nature, senator, is that it goes beyond banking. Then you are getting into the question of how secure is my personal situation at home and all the things I do over top of it. On an institutional issue, that becomes more of a national issue at that point in time. Awareness raising has to go beyond anything that would be related to banking if you are talking about something that is more generic in its threat from a customer and citizen point of view.

Senator Unger: One last question on your concern about PIPEDA: You said that recent amendments to PIPEDA impede the ability of organizations to share personal information. That kind of speaks to what I have been asking about. What are your concerns?

Mr. Ross: A while back, PIPEDA made changes to eliminate what was called an investigative body and replaced it with rules that still allows for fraudulent data to be shared. However, it doesn't allow the sharing of intelligence. If you see anomalies or things that look odd but may not be confirmed fraud, those are the activities that aren't allowed to be shared as a result of the changes. We are suggesting that we need the ability to share some of that intelligence so that, as a collective, we may start to see patterns and threats evolve and grow. Then we can actually put a remediation plan in place to avoid the impacts of that.

faites. En définitive, la cybersécurité doit être une approche à plusieurs niveaux. Il faut partager l'information pour accroître la résilience; il faut surveiller le trafic pour réduire l'introduction de codes malveillants; puis il faut faire de la sensibilisation pour que le client ou le particulier sache quoi surveiller. En fin de compte, l'approche doit être à plusieurs niveaux parce que, en définitive, la menace ne cesse pas d'évoluer. Il s'agit d'avoir plusieurs niveaux pour faire de la sensibilisation et de la prévention et accroître la capacité d'intervention.

La sénatrice Unger : Cette violation s'appelle Krack. Krack a trouvé moyen de déjouer tout le chiffrement du WPA2 sur les réseaux Wi-Fi. Il attaque tout le matériel Wi-Fi moderne pour les téléphones mobiles, les tablettes et les postes de travail, les routeurs, les imprimantes et tout le reste.

Ma question concerne spécifiquement Krack. Avez-vous trouvé une façon d'aviser vos clients? On ne parle pas vraiment de cette question. Elle vient seulement des plus hauts niveaux, mais le *National Post* a publié un grand article là-dessus. On serait peut-être sur le point de frapper l'éventail Wi-Fi. Plus particulièrement, en ce qui concerne Krack, avez-vous quoi que ce soit pour alerter les clients des banques?

M. Hannah : Le problème, madame la sénatrice, c'est que cela dépasse les services bancaires. Puis, on aborde la question de la sécurité de ma situation personnelle à la maison et de tout ce que je fais en plus. Au niveau institutionnel, cela devient alors un problème national. La sensibilisation doit aller au-delà de tout ce qui se rapporte aux banques si vous parlez d'une menace plus générique du point de vue du client et du citoyen.

La sénatrice Unger : Une dernière question sur ce qui vous préoccupe dans la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE. Vous avez dit que les récentes modifications à la LPRPDE empêchent vos membres de communiquer des renseignements personnels. Voilà justement ce dont je parle. Quelles sont vos préoccupations?

M. Ross : Il y a un certain temps, des changements à la LPRPDE ont éliminé les organismes d'enquête pour les remplacer par des règles qui permettent toujours l'échange de données frauduleuses. Par contre, la LPRPDE ne permet pas le partage de renseignements. Les anomalies ou les choses qui semblent bizarres, mais qui ne sont pas nécessairement des cas de fraude confirmés sont justement les activités que les changements interdisent de communiquer. Nous sommes d'avis que nous devons pouvoir partager certains de ces renseignements pour que, collectivement, nous puissions commencer à voir les tendances et les menaces évoluer et grossir. Alors, nous pourrons nous donner un plan de correction pour éviter les répercussions.

Ms. Stephens: In the changes where the investigative body was removed, they added two new exceptions for consent to allow for sharing. One of them is in order to prevent fraud, but it's only related to fraud, and I think there are many other areas where there would be a benefit of sharing to prevent criminal offences other than fraud and along those lines with cyber as well.

Senator Massicotte: Give me a sense of the big picture. All of us are using Canadian banks. We rely on Canadian banks. All we have is a statement or reading off your iPad of maybe the sums we have either lent or in deposit with you. It's all electronic; it's all in the air. Sometimes when we wake up in the night, there's the feeling that it could disappear and how could you prove what you had before? What is the risk of someone hacking into your accounts and some of that money disappearing, on a risk of 100 per cent? You seem very sure. Is it 99.99 per cent certain that we shouldn't worry about that risk?

Mr. Ross: It's difficult to put a number on it, to be fair, because the risk continues to evolve. What I can share with you is that trust is paramount to what banking is. Without trust, banks would struggle to exist. Canadians losing that trust would —

Senator Massicotte: I understand that. You may lose our trust, but if you lose my money it's even more serious.

Mr. Ross: Absolutely. Canadians are protected. If they lose money or are defrauded of their money through a cyberattack, they are protected. The banks have I believe what we refer to as zero liability. If there are any losses that a consumer or business undertakes as a result of fraudulent events, the banks make them whole.

Senator Massicotte: You will automatically put the cash back? There is no argument and no need to hire a lawyer; it is 100 per cent guaranteed?

Mr. Ross: The banks will keep them whole.

Senator Massicotte: Let me tell you about my frustration. Look at the credit bureaus. In this case, there has been a hack, and they left with a lot of information, including names and social insurance numbers. If one of the banks had your balance sheet, they would have that. All of that could be public. It really bugs me to think that these companies get this information with the presumption that they will take the same measures you do relative to your clients and we find ourselves having trust in people who disappoint us and the information is out there. I think 10,000 Canadians have been violated to that degree. While I'm a little bit pissed off at them, I must admit, where did they get that information? They got it from you.

Mme Stephens : Dans les changements qui ont fait disparaître l'organisme d'enquête, on a ajouté deux nouvelles exceptions au consentement pour permettre la communication. La première vise à prévenir la fraude, mais elle n'est reliée qu'à la fraude. Je pense qu'il y a beaucoup d'autres domaines que la fraude et, dans le même ordre d'idées, la cybernétique où il serait avantageux de communiquer des renseignements pour prévenir des infractions criminelles.

Le sénateur Massicotte : Donnez-moi une idée du grand tableau. Nous utilisons tous les banques canadiennes. Nous comptons sur elles. Nous n'avons rien d'autre qu'un relevé papier ou électronique des sommes que nous vous avons prêtées ou confiées en dépôt. Tout est électronisé; tout est dans les airs. Il m'arrive de me réveiller la nuit avec le sentiment que mon argent pourrait disparaître et que je ne pourrais pas prouver ce que j'avais. Quel est le risque qu'on pirate mon compte et qu'une partie de mon argent se volatilise avec une certitude de 100 p. 100? Vous semblez très sûr de vous-même. Y a-t-il 99,99 p. 100 de certitude que je n'ai pas à m'en faire avec cela?

M. Ross : C'est difficile à chiffrer, pour être honnête, parce que le risque ne cesse d'évoluer. Mais je peux vous dire que la confiance est primordiale dans le secteur bancaire. Sans la confiance, les banques auraient bien du mal à exister. Les Canadiens perdant cette confiance…

Le sénateur Massicotte : Je comprends cela. Vous pouvez perdre notre confiance, mais si vous perdez mon argent, c'est encore plus grave.

M. Ross : Absolument. Les Canadiens sont protégés. S'ils perdent de l'argent ou sont victimes d'une cyberattaque, ils sont protégés. Les banques ont ce que nous appelons une responsabilité zéro, sauf erreur. Elles rembourseraient les pertes qu'un consommateur ou une entreprise subirait à cause d'activités frauduleuses.

Le sénateur Massicotte : Vous rembourserez automatiquement l'argent? Pas d'argument ni besoin de retenir les services d'un avocat; c'est garanti à 100 p. 100?

M. Ross : Les banques indemniseront leurs clients.

Le sénateur Massicotte : Laissez-moi vous parler de ma frustration. Voyez les bureaux de crédit. Dans ce cas-ci, il y a eu du piratage, et beaucoup d'information a été volée, y compris des noms et des numéros d'assurance sociale. Si une banque avait votre bilan, le pirate aurait mis la main dessus. Tout cela pourrait être public. Je n'aime pas du tout penser que vous fournissez cette information à ces entreprises en supposant qu'elles prendront les mêmes mesures que vous pour protéger vos clients. Et nous faisons confiance à des gens qui nous déçoivent et qui ont l'information. Je pense que 10 000 Canadiens ont ainsi été victimes de violations. Je dois admettre que cela me met en colère. D'où cette information vient-elle? De chez vous.

The Chair: Strike that last sentence there. He's upset.

Senator Massicotte: It does get me upset. What gets me more upset is the information came largely from you, or from Wal-Mart or whatever, because most of you have relationships with these firms and use them significantly. While I'm upset at them, I could be upset at you and I probably should be upset at you because you did not take the measures or assurance to make sure they had adequate safeguards to make sure you never lost that information. You gave that personal information to them and now it's in the public domain. How do you deal with that? How do you regain my trust?

Mr. Ross: First, senators, let me say I've heard worse language than the language that was struck.

Having said that, it goes back to our recommendations. We believe there needs to be consistent standards and we need to be building off of resilience, not reaction. We need to avoid these threats and avoid these issues before they become issues. We need to have consistent standards and oversight to ensure and give Canadians a comfort that their data is being protected throughout the ecosystem. The ecosystem continues to evolve and grow through competition and innovation. Foundational to all of this, we need to make sure those standards are consistent.

Senator Massicotte: I appreciate that, but before you shared my information with these industries, did you take any measures to make sure they had adequate safeguards in place? If that is the case, why did it take six or nine months for it to become public after it occurred?

Mr. Ross: Banks, as part of their risk management and any relationships with third parties, do ensure that there are security standards and safeguards in place. I can't speak about Equifax specifically; nor can I speak, quite frankly, to what is happening today in that we are seeing a lot of non-banks and suppliers that don't have a relationship with the banks and are still getting that information. As a customer, I can sign up to a third party and allow banking information to flow to that third party without the banks being aware of that. As much as we can protect — and we have plans in place and we do review the security of the parties that we partner with — there is a big gap, and the gap is growing of those third parties that we don't have relationships with and don't have any oversight of.

Senator Massicotte: I appreciate that, but most of the information they had is confidential, personal information — balance sheets and so on. I suspect most of us don't give that information to anybody other than our bank. To accept that they had that information means it came from one of your bank members. You do an internal audit and measure your risks, but obviously you made a mistake. Maybe I should have the right to

Le président : Supprimez cette dernière phrase. Il est en colère.

Le sénateur Massicotte : Oui, je suis en colère. Je le suis d'autant plus que l'information est venue surtout de chez vous, ou de chez Wal-Mart, ou de quelqu'un d'autre, parce que la plupart d'entre vous avez des relations avec ces entreprises et les exploitez sans vous gêner. Je suis en colère contre elles, et je pourrais l'être contre vous. Je devrais probablement l'être parce que vous n'avez pas pris les mesures ou l'assurance qu'il aurait fallu pour vous garantir qu'elles avaient des protections suffisantes pour que vous ne perdiez jamais ces renseignements. Vous leur avez donné ces renseignements personnels, et voilà qu'ils sont du domaine public. Comment corriger cela? Comment regagner ma confiance?

M. Ross : En premier lieu, mesdames et messieurs les sénateurs, je vous jure que j'ai entendu pire comme langage.

Cela dit, revenons à nos recommandations. Nous croyons qu'il faut des normes uniformes, qui doivent reposer sur la résilience, et non pas sur la réaction. Nous devons éviter ces menaces et ces dangers avant qu'ils ne deviennent des problèmes. Il nous faut des normes et une surveillance uniformes pour donner aux Canadiens la certitude que leurs données sont protégées dans tout l'écosystème. L'écosystème continue d'évoluer et de croître par le fait de la concurrence et de l'innovation. À la base, nous devons veiller à la convergence de ces normes.

Le sénateur Massicotte : Je comprends tout cela, mais avant de partager mes renseignements avec ces industries, avez-vous vérifié que leurs mesures de protection étaient suffisantes? Si oui, pourquoi aura-t-il fallu six ou neuf mois pour rendre le rapport public?

M. Ross : Dans le cadre de leur gestion des risques et de leurs relations avec des tiers, les banques veillent à se donner des normes de sécurité et des garanties. Je ne saurais parler spécifiquement d'Equifax ni, bien honnêtement, expliquer pourquoi tant de non-banques et de fournisseurs qui n'ont pas de relations avec les banques obtiennent quand même cette information. En tant que client, je peux m'inscrire auprès d'une tierce partie et permettre de lui communiquer mes renseignements bancaires sans que les banques le sachent. Dans la mesure où nous pouvons protéger les renseignements — et nous avons des plans en place et vérifions la sécurité des parties avec qui nous travaillons — il y a un écart très net, qui se creuse de jour en jour, avec des tierces parties avec lesquelles nous n'avons pas de relations et que nous ne surveillons pas.

Le sénateur Massicotte : Je comprends, mais le plus clair de l'information qu'elles avaient est confidentielle; je parle d'information personnelle, de bilans et ainsi de suite. Je soupçonne que la plupart d'entre nous ne donnons cette information à personne d'autre que la banque. Accepter qu'elles avaient cette information, c'est prouver qu'elle provenait d'un de vos membres. Vous faites un audit interne et mesurez vos

sue you because of the damage you caused because you did not do your homework.

Ms. Stephens: You're right, but the system is important. In order for people to be able to obtain credit and have a system where you can underwrite credit is important. To Mr. Ross' point, there are contractual obligations for having sufficient security safeguards for this type of data.

Again, this is an Equifax issue. It's probably best to address some of these questions to Equifax.

Senator Wetston: I'm interested in the papers you have written on cybersecurity. One that I took a quick look at was your 2014 report entitled*Cyber Security: Protecting the Resilience of Canada's Financial System*, and I have your CBA response to Public Safety Canada as well. Just looking at your presentation today, it's very consistent with the approach obviously. I wouldn't suggest otherwise.

I'm trying to understand, because the banks are integrated institutions. I asked this question of the previous witness somewhat differently, but the transfer of risk, particularly on a systemic level, can occur without a cybersecurity attack. It's not all potentially as a result of cybersecurity. The financial crisis we had 10 years ago was not as a result of cybersecurity issues. I think you would probably agree with me there. It was probably as a result of greed and other such factors, poor behaviour on the part of industry. You might agree with me there, or not.

The point I'm trying to get at here, you talk a little bit about the future framework for financial services, and there is the good and the bad of security of technology, the benefits that we get and the harms that it can create. We understand that cybersecurity threats are probably one of the harms that flow from innovation and technology advancement.

When I look at your sector, the banking sector, it wouldn't surprise you that most of the banks are also in the capital markets as well on the banking side. Much of your focus has been on the banking side. Can you tell me what you are doing on the capital market side to deal with cybersecurity threats? Are they the same? Are they different?

I know all the banks have spent I think billions of dollars on cybersecurity collectively in Canada to deal with these threats and the processes you need to put in place to address these attacks. I'm sure you've done a lot of that. Can you help me with the scenario that banks are more than just banks in the traditional sense and are regulated by OSFI?

risques, mais vous avez manifestement commis une erreur. Je devrais peut-être avoir le droit de vous poursuivre pour les torts que vous m'avez causés en ne faisant pas vos devoirs.

Mme Stephens : Vous avez raison, mais le système est important. Il est important de pouvoir obtenir du crédit et d'avoir un système permettant de l'évaluer. Pour revenir à la réponse de M. Ross, il existe des obligations contractuelles d'avoir des garanties de sécurité suffisantes pour ce type de données.

Encore une fois, c'est le problème d'Equifax. Il vaudrait probablement mieux poser ces questions à Equifax.

Le sénateur Wetston : Je m'intéresse aux textes que vous avez signés sur la cybersécurité. J'ai jeté un coup d'œil sur votre rapport de 2014 intitulé *Résilience du système financier canadien : l'apport de la cybersécurité*, et j'ai la réponse de l'ABC à Sécurité publique Canada également. Votre exposé d'aujourd'hui est en tout point conforme à l'approche, bien sûr. Je ne saurais dire le contraire.

J'essaie de comprendre, car les banques sont des institutions intégrées. J'ai posé ma question en termes légèrement différents au témoin précédent, mais le transfert du risque, surtout au niveau systémique, peut se faire sans atteinte à la cybersécurité. Ce n'est peut-être pas tout à cause de la cybersécurité. Les problèmes de cybersécurité n'étaient pour rien dans la crise financière d'il y a 10 ans. Vous serez probablement d'accord là-dessus. La crise était probablement imputable à la cupidité et à d'autres facteurs du genre, comme le mauvais comportement de l'industrie. Vous pouvez être d'accord ou pas avec moi sur ce point.

Parlant du futur cadre des services financiers, la sécurité de la technologie a du bon et du mauvais, au niveau des avantages que nous en tirons et des préjudices qu'elle peut nous causer. Nous comprenons que les menaces à la cybersécurité font probablement partie des préjudices qui naissent de l'innovation et des progrès technologiques.

Dans votre secteur, le secteur bancaire, vous ne serez pas surpris que la plupart des banques aient aussi une présence sur les marchés financiers. C'est le secteur bancaire qui vous intéresse surtout. Pouvez-vous me dire ce que vous faites, sur les marchés financiers, pour contrer les menaces à la cybersécurité. Sont-elles les mêmes? Sont-elles différentes?

Je sais que les banques ont dépensé collectivement des milliards de dollars en cybersécurité au Canada pour contrer ces menaces et concevoir les processus à mettre en place pour repousser ces attaques. Je suis sûr que vous en avez fait beaucoup. Pouvez-vous m'aider à comprendre le scénario selon lequel les banques ne sont plus que des banques au sens traditionnel et sont réglementées par le BSIF?

Mr. Hannah: Absolutely. At the end of the day, from a bank financial group perspective, you are dealing with these issues at a group level and trying to leverage the infrastructure and the expertise you have across the group, whether that be a touch point on the wealth management side, the banking side, the insurance side or mutual funds.

My interaction with the client is often multifaceted, so I have an interest in making sure that client is protected across vectors. I want to try to make sure that I don't have any vulnerable points in there that can create the issue that you're talking about. When you are looking at an issue like that from a financial services perspective, from a bank perspective, if I multiple lines of business, I have to protect multiple lines of business.

Senator Wetston: The reason I was getting at that is there is a very large amount of business outside of the regulatory sphere of OSFI. I know that OSFI has — what do you call the guide here? There is a guide they put out. Help me with this, although I'll be searching for it. Do they have a guide that they produced on cybersecurity?

Mr. Ross: Self-assessment questionnaire, yes.

Senator Wetston: Yes. Is it a guide or questionnaire?

Mr. Ross: It's a questionnaire that OSFI uses to measure the financial institutions for which they regulate for their cyber-resilience.

Senator Wetston: In that regard, do the banks provide the data on breaches to OSFI so they have a better understanding of the threats to the system, including any systemic risks that might be included? I asked this question last week and I couldn't get an answer. I'm going to keep trying, perhaps when OSFI appears, chair.

Mr. Ross: Certainly as part of the questionnaire, banks do provide information to OSFI based on the guidelines that are in that. I don't recall, I'll be honest, if there are facts and figures, but certainly there are a number of components of cyber-resilience included in that questionnaire.

Senator Wetston: I will ask you to see if you have any data on that and provide it to the clerk of the committee, if possible. I'm interested to try and understand the magnitude of threats. Maybe each individual institution has to answer that question, or OSFI, but it would be helpful if you could provide that.

I see where financial services is going, and you may agree or disagree with me here. My sense is that some of the financial services that are being provided could be less threatened by cyberthreats than the traditional banking and financial market system. If we start with cybersecurity, generally speaking, and we think about fintech, crypto currencies and blockchain

M. Hannah : Bien sûr. Au fond, dans la perspective du groupe financier bancaire, vous gérez ces enjeux au niveau du groupe et essayez de tirer parti des infrastructures et de l'expertise que vous avez à l'échelle du groupe, que ce soit un point de contact pour la gestion du patrimoine, les banques, les assurances ou les fonds communs de placement.

Mon interaction avec le client est souvent multidimensionnelle et j'ai donc intérêt à protéger le client dans les divers vecteurs. Je veux éviter de voir des points de vulnérabilité susceptibles de créer le problème dont vous parlez. Lorsque vous avez un problème comme celui-là dans la perspective des services financiers — dans la perspective bancaire, s'il y a plusieurs secteurs d'activité — je dois les protéger tous.

Le sénateur Wetston : Si j'allais dans ce sens, c'est que beaucoup d'activités échappent à la sphère de réglementation du BSIF. Je sais que le BSIF a… Comment appelez-vous ce guide? Il a publié un guide. Aidez-moi un peu, pendant que je cherche. N'a-t-il pas produit un guide sur la cybersécurité?

M. Ross : Un questionnaire d'autoévaluation, oui.

Le sénateur Wetston : Oui. C'est un guide ou un questionnaire?

M. Ross : C'est un questionnaire qui sert au BSIF à mesurer la résilience cybernétique des institutions financières qu'il réglemente.

Le sénateur Wetston : À cet égard, les banques envoient-elles leurs données sur les violations au BSIF, pour l'aider à comprendre les menaces qui pèsent sur le système, comme les risques systémiques qui pourraient être inclus? J'ai posé cette question la semaine dernière, et je n'ai pas eu de réponse. Je réessayerai, peut-être à l'occasion de la comparution du BSIF, monsieur le président.

M. Ross : Chose certaine, dans le questionnaire, les banques fournissent de l'information au BSIF conformément aux lignes directrices. Je ne me rappelle pas, bien honnêtement, s'il y a des faits et des chiffres, mais le questionnaire couvre certainement plusieurs composantes de la résilience cybernétique.

Le sénateur Wetston : Je vous demanderais d'envoyer à la greffière du comité les données que vous pourriez avoir à ce sujet, si possible. Je veux comprendre l'étendue des menaces. Peut-être que chaque institution, ou le BSIF, doit répondre à ma question; en tout cas, cette information serait utile.

Je vois où vont les services financiers, et vous pouvez être d'accord ou pas avec moi ici. J'ai le sentiment que certains services financiers offerts pourraient être moins exposés aux cybermenaces que le système bancaire et financier traditionnel. Commençons par la cybersécurité, en général, en pensant aux technologies financières, aux cryptomonnaies et à la technologie

technology — and I know you're talking about large value transfer systems that could also be threatened through the clearing and settlement process, which is also potentially threatened by a cybersecurity attack.

As the technology continues to evolve, the challenges are there. Do you see greater threats in these areas to investors, consumers and the public generally or less so as a result of these technologies developing?

Mr. Ross: I don't know whether the answer is increased threats. I think when you have more suppliers that are not regulated, you just don't have that information. You don't have that level of trust that these entities have the resilience that a financial institution has built.

Now, I'm not suggesting that a fintech would require the same magnitude of resilience and regulation, but it's risk-based and today there's fundamentally none for players not regulated. What we are suggesting through a number of consultations is, as it relates to cybersecurity, there at least needs to be a minimum standard based on the risk that any participant has or brings to the ecosystem.

Senator Ringuette: I'm hearing you talk about a multi-layered approach, being proactive and that Canadians are being protected against fraud. There are bank guarantees.

However, as with previous colleagues, I question with regard to Equifax. You are not acknowledging your responsibility toward your clients in regard to a multi-layered approach and to being proactive in protecting their information and this bank guarantee that you keep talking about. As yet, that we have not been able to get the banks to acknowledge their responsibility and being proactive in a specific event with regard to Equifax. That's a comment. It's not a question because I know you're not going to provide us with the detailed process that you are going through with regard to Equifax and your clients.

That being said, last week I read an article that TD Bank was moving its data processing to India. You are here today saying:

> Banks support the government's work to protect Canadians while promoting innovation and competition. We encourage the federal government to finalize and implement its renewed cybersecurity strategy to protect Canadians and improve.

What are the specific steps that you take when you decide to take a banking customer's data and move it outside of the Canadian jurisdiction? That in itself is a major concern to me as

des chaînes de bloc… Je sais que vos systèmes de transfert de paiements de grande valeur pourraient aussi être menacés dans le processus de compensation et de règlement, qui pourrait lui aussi être exposé à une attaque contre la cybersécurité.

L'évolution de la technologie s'accompagne toujours de nouveaux défis. Pensez-vous que ces technologies représentent de plus grandes menaces ou des menaces moindres dans ces domaines pour les investisseurs, les consommateurs et le grand public?

M. Ross : Je ne sais pas si c'est de plus grandes menaces. Si un plus grand nombre de fournisseurs ne sont pas réglementés, cette information n'est tout simplement pas disponible. On n'est pas aussi sûrs que ces entités ont la même résilience que l'institution financière.

Je ne dis pas qu'une entreprise de technologie financière aurait besoin du même degré de résilience et de réglementation, mais elle est fondée sur le risque et, aujourd'hui, il n'y a essentiellement rien pour les joueurs qui ne sont pas réglementés. Dans diverses consultations, nous sommes d'avis que, en matière de cybersécurité, il faut au moins une norme minimale fondée sur le risque que présente le participant pour l'écosystème.

La sénatrice Ringuette : Vous parlez d'une approche à plusieurs niveaux, vous parlez d'être proactifs et vous dites que les Canadiens sont protégés contre la fraude. Il y a des garanties bancaires.

Par contre, comme les collègues qui m'ont précédée, j'ai une question à propos d'Equifax. Vous ne reconnaissez pas votre responsabilité envers vos clients pour l'approche à plusieurs niveaux et pour ce qui est de la protection proactive de leur information et de la garantie bancaire dont vous ne cessez de parler. Nous n'avons pas encore pu persuader les banques de reconnaître leur responsabilité et d'être proactives dans le cas précis d'Equifax. C'est un simple commentaire. Ce n'est pas une question, car je sais que vous n'allez pas nous donner le processus détaillé que vous appliquez à l'égard d'Equifax et de vos clients.

Cela dit, la semaine dernière j'ai lu que la Banque TD fait traiter ses données en Inde. Voici que vous nous dites aujourd'hui :

> Les banques appuient le travail du gouvernement dans la protection des Canadiens tout en encourageant l'innovation et la concurrence. Nous encourageons le gouvernement fédéral à mettre au point et à implanter sa nouvelle stratégie en matière de cybersécurité, qui vise à protéger les Canadiens et à améliorer la résilience cybernétique du Canada.

Quelles mesures précises prenez-vous lorsque vous décidez de transférer à l'étranger les données d'un client bancaire? Voilà en soi une grande préoccupation pour moi, en tant que

a Canadian consumer who takes their financial services to a bank.

You're here in front of us saying, "Well, it's not our fault. Equifax has to deal with their own issue." You don't seem to acknowledge any kind of responsibility or proactive process, on the one hand, and then you have one of your major associate members that is taking its banking data, which is all of its customers, outside of the country. What is the process? Even though we have Canadian legislation, the data is not within our geographic territory. What are the steps that you are taking to make sure that Canadian banking data that is outside of our jurisdiction is protected? Where is your guarantee?

Mr. Ross: First, Canadian banks are regulated based on Canadian regulations and Canadian law.

Second, it's safe to say that regardless of where data is housed, whether it's down the street or around the world, it's still travelling through systems and telecommunication lines. At the end of the day, regardless of whether it's down the street or around the world, there are the same protections that Canadian banks put on that communication regardless.

When I talked about a measured approach, all of Canada's data is going somewhere else. Data is segregated based on the activities of employees, again, regardless of where they reside and work. As a result, only the data that is required for them to do their duties would be available to them. It's all monitored and audited. There is a multilevel approach. Banks take cybersecurity extremely seriously. The reality is the threat is the same threat whether it's piping information to a different country or down the street.

Ms. Stephens: I just don't want to leave the misrepresentation that our banks aren't keenly aware of the Equifax breach. It's a top priority for them to mitigate any risks to their customers.

Also, further to Mr. Ross' comments, under PIPEDA, it's clear that there is an accountability principle. The accountability is with, in this case, the bank. There is no way for that to be changed. Whether it's with vendors, onshore or offshore, that accountability stays with the bank, and there is a layered process, due diligence, on-site reviews and contractual protections. There is a layered, risk-management approach to selecting and monitoring a vendor to ensure compliance with the rules we have and to protect against cyber risks, et cetera.

consommatrice canadienne qui confie ses affaires financières à une banque.

Et vous êtes là à nous dire : « Ce n'est pas notre faute. C'est à Equifax de régler son problème. » Vous ne semblez pas accepter la moindre responsabilité ni obligation de proactivité, pendant que l'un de vos principaux membres associés envoie ses données bancaires, c'est-à-dire celles de tous ses clients, à l'étranger. Quel est le processus? Même si nous avons une loi canadienne, les données ne se trouvent pas dans notre territoire géographique. Que faites-vous pour protéger les données bancaires qui ne sont pas chez nous? Où est votre garantie?

M. Ross : Tout d'abord, les banques canadiennes sont soumises à la réglementation et à la loi canadiennes.

Ensuite, on peut dire sans risquer de se tromper que, peu importe où elles sont hébergées, que ce soit dans la même ville ou à l'autre bout du monde, les données passent toujours par des systèmes et des lignes de télécommunication. En définitive, qu'elles restent dans la même ville ou qu'elles aillent ailleurs dans le monde, elles font l'objet des mêmes protections que les banques canadiennes appliquent de toute façon à leur communication.

Quant à l'approche mesurée dont j'ai parlé, toutes les données du Canada sont envoyées ailleurs dans le monde. Elles sont séparées en fonction des activités des employés, encore une fois, sans égard à leur lieu de résidence ou de travail. Ainsi, ils n'ont accès qu'aux seules données dont ils ont besoin pour s'acquitter de leurs fonctions. Tout est surveillé et audité. Il y a une approche à plusieurs niveaux. La cybersécurité est une question extrêmement sérieuse pour les banques. La réalité est que la menace est la même, peu importe qu'on envoie l'information à l'étranger ou dans la même ville.

Mme Stephens : Je ne voudrais pas laisser passer l'impression erronée que nos banques ne sont pas parfaitement au courant de la violation d'Equifax. Leur priorité absolue est d'atténuer les risques pour leurs clients.

En outre, pour donner suite aux commentaires de M. Ross, il est certain qu'un principe de responsabilisation est enchâssé dans la LPRPDE. Dans le cas qui nous intéresse, la responsabilisation incombe à la banque. Il n'y a aucune façon de le changer. Que ce soit envers les fournisseurs au Canada ou à l'étranger, c'est la banque qui demeure responsable et il existe un processus à paliers multiples, assorti de principes de diligence raisonnable avec des examens sur place et des protections contractuelles qui interviennent. Pour sélectionner un fournisseur et le surveiller, une approche de gestion des risques à paliers est appliquée afin de veiller au respect des règles que nous avons instaurées et d'assurer une protection notamment contre les cyberrisques.

Senator Ringuette: Ms. Stephens, you are repeating the same thing right now; you take every measure, you're being proactive and so forth. You have not proven that to me in regard to Equifax. Why should I believe and trust banking data from TD Bank residing in India? Why should I trust banking information in regards to Visa or Mastercard that resides in the U.S.? Even though we would legislate, at the end of the day, for anything that's outside of Canada, we have no jurisdiction. We can't implement laws that would be applicable in the U.S. or in India.

I appreciate the spin that you're providing this morning, but I also have to indicate to you that it is not very reassuring. There is the Equifax breach. A good portion of that information was most likely provided to that entity by a banking institution. At the end of the day, it's not the banks that are the victims, and it's not Equifax that is the victim. It's the 10,000 Canadians who are the victims.

Mr. Hannah: You have put your finger on something, and I want to pick up on it because I think in some respects it answers the question. Banking is a trust-based business. I will put my funds only with an institution that I trust. I trust they will take care of it. If I lose that trust as an institution, then my business will migrate to somewhere else. If you are a bank, you have every incentive to take as much care as possible because it is a trust-based business, and we recognize that. That's ultimately the driving force beyond anything else. It's that trust basis that you know is at the heart of your franchise.

[*Translation*]

Senator Maltais: Thank you for your testimony. I have two short questions. Senator Ringuette asked you a question, but I'm not sure I understood your answer.

Senator Ringuette: There wasn't any.

Senator Maltais: Is the cybersecurity of banks equally secure in all of the bank branches and their subsidiaries throughout the world? If, for instance, Scotiabank has a branch in Cuba, do you ensure its cybersecurity there?

[*English*]

Mr. Ross: The answer is yes. As Mr. Hannah mentioned earlier, banks look at this holistically. They look at their entire operation. Regardless of where these institutions reside, they do typically take an organizational approach. The same regulations, law or care that they take protecting their data for Canadians is the same protections that they would use regardless of where their data is stored.

La sénatrice Ringuette : Madame Stephens, vous vous répétez; vous dites que vous prenez toutes les mesures, que vous agissez proactivement et ainsi de suite. Vous ne m'avez pas convaincue de l'avoir fait dans le cas d'Equifax. Pour quelle raison devrais-je croire des données bancaires provenant d'une entité de la TD en Inde et faire confiance à ces données? Pour quelle raison des renseignements bancaires concernant Visa ou Mastercard provenant des États-Unis devraient-ils m'inspirer confiance? Même si nous légiférerons, en fin de compte, nous n'avons pas compétence sur quoi que soit qui se déroule à l'extérieur du Canada. Nous ne pouvons instaurer des lois qui seraient applicables aux États-Unis ou en Inde.

J'apprécie votre apport ce matin, mais je dois aussi vous dire que ce n'est pas très rassurant. Des données d'Equifax ont été compromises. Une bonne partie de ces renseignements a fort probablement été donnée à cette entité par une institution bancaire. En fin de compte, les banques ne sont pas les victimes, pas plus qu'Equifax. Les victimes, ce sont plutôt les 10 000 Canadiens.

M. Hannah : Vous avez mis le doigt sur quelque chose et je veux y revenir, car je pense qu'à certains égards, poser la question, c'est y répondre. Pour le secteur bancaire, tout est question de confiance. Je vais seulement confier mon argent à une institution en laquelle j'ai confiance. Je suis convaincu qu'elle agira au mieux. Si je perds cette confiance dans l'institution, je transférerai mes avoirs ailleurs. Les banques ont donc tout intérêt à être le plus attentionnées que possible, car ce secteur s'appuie sur la confiance et nous le savons. En fin de compte, c'est le moteur de tout le reste. C'est cette base de confiance qui, vous le savez, est au cœur de votre franchise.

[*Français*]

Le sénateur Maltais : Merci pour vos témoignages. J'ai deux courtes questions. La sénatrice Ringuette vous a posé une question, mais je ne suis pas sûr d'avoir bien compris votre réponse.

La sénatrice Ringuette : Il n'y en avait pas.

Le sénateur Maltais : Est-ce que la cybersécurité des banques est également assurée dans toutes les succursales bancaires et leurs filiales à travers le monde? Par exemple, si la Banque Scotia a une succursale à Cuba, y assurez-vous la cybersécurité?

[*Traduction*]

M. Ross : La réponse est oui. Comme M. Hannah l'a mentionné, les banques étudient le tableau d'ensemble. Elles examinent toute leur entreprise. Peu importe où leurs établissements se situent, elles appliquent d'habitude une approche organisationnelle. Les règlements, les lois et la diligence qu'elles appliquent pour protéger les données dont

[*Translation*]

Senator Maltais: Thank you.On page 2 of your brief, you refer to a lead federal organization, consistent standards for critical infrastructure sectors, and the blocking and sharing of malicious data communications. Do you share your information with the security systems of financial institutions that are not covered by the government Bank Act, such as for instance credit unions, caisse populaires, et cetera? Do you share information with them?

[*English*]

Mr. Ross: No personal information is shared. We do share intelligence. We do share through a number of avenues. One is obviously through CBA where in fact, as it relates to cybersecurity, we have invited and we include actually some non-members, including credit unions TMX and others to share intelligence. We also share that intelligence through the Canadian Cyber Threat Exchange, which was set up last year, and also we deal quite closely with CCIRC, an arm of public safety.

Within the financial services industry, we do a good job of sharing intelligence. Where there would be benefit is expanding that knowledge to other infrastructures and other critical sectors so that our knowledge can be shared with them and vice versa.

[*Translation*]

Senator Maltais: Do you work in cooperation with Canadian insurance companies?

[*English*]

Mr. Ross: We have some insurers at the table, and certainly a lot of financial institutions are also insurers. Again, taking that organizational view, by default, yes, they are part of that.

Certainly we continue to encourage Canadian organizations to get involved in CCIRC and CCTX and some of the structures that have been put in place. We would like to obviously see more. CCTX is relatively new. The banking industry was one of the driving forces in creating that entity.

elles disposent sur les Canadiens seraient les mêmes, peu importe l'endroit où les données sont entreposées.

[*Français*]

Le sénateur Maltais : Merci. À la page 2 de votre mémoire, il est question d'un organisme fédéral responsable, de normes uniformes pour les secteurs des infrastructures essentielles, et du blocage et du partage de la communication de données malveillantes.Est-ce que vous partagez vos renseignements avec les systèmes de sécurité des institutions financières qui ne sont pas couvertes par la Loi sur les banques du gouvernement, par exemple les *credit unions*, les caisses populaires, et cetera? Est-ce que vous partagez des renseignements avec eux?

[*Traduction*]

M. Ross : Nous n'échangeons aucun renseignement personnel. Nous échangeons des renseignements par diverses voies de communication, notamment dans le cadre de l'ABC, bien entendu; en matière de cybersécurité, nous avons invité certains groupes non membres, y compris les coopératives de crédit du groupe TMX à échanger des renseignements dont nous avons tenu compte. Nous avons aussi transmis ces renseignements par l'entremise de l'Échange canadien de menaces cybernétiques, qui a vu le jour l'an dernier, puis nous collaborons d'assez près avec le CCRIC, un organisme de Sécurité publique Canada.

Dans le secteur des services financiers, nous faisons du bon travail pour ce qui est de l'échange de renseignements. Il y aurait lieu par contre d'étendre ce savoir à d'autres infrastructures et secteurs essentiels, et d'apprendre d'eux, afin que nous puissions tous en profiter.

[*Français*]

Le sénateur Maltais : Est-ce que vous travaillez en collaboration avec les compagnies d'assurance canadiennes?

[*Traduction*]

M. Ross : Il y a des représentants des sociétés d'assurances parmi nous et assurément, bien des institutions financières offrent aussi des produits d'assurance. Je le répète, dans l'optique organisationnelle, par défaut, oui, elles font partie de l'équation.

Nous continuons à encourager les organismes canadiens à participer aux travaux du CCRIC et de l'Échange canadien de menaces cybernétiques et de certaines autres structures qui ont été établies. Nous aimerions bien sûr qu'il y en ait davantage. L'Échange canadien de menaces cybernétiques est assez récent et l'industrie bancaire a été l'un des moteurs de la création de cette entité.

Mr. Hannah: To build on what Mr. Ross has said and tie it back to the recommendations we have made, this is exactly why we think there would be value in having a lead coordinating agency creating common standards across critical infrastructures and improving information sharing. It's to get at exactly the point you're talking about, and that is that the industry is interrelated and critical infrastructure sectors rely on each other. To the extent that the government can play a role in building those bridges, help enhance the communication that's already there and create a common language across which to talk, that would make things all the better.

M. Hannah : Pour faire fond sur les propos de M. Ross et les relier aux recommandations que nous avons formulées, c'est exactement la raison pour laquelle nous pensons qu'il serait utile de mettre sur pied un organisme principal de coordination chargé d'élaborer des normes uniformes pour l'ensemble des infrastructures essentielles et d'améliorer le partage de l'information. Cela revient exactement à ce que vous dites; l'industrie est interdépendante et les secteurs des infrastructures essentielles dépendent l'un de l'autre. Dans la mesure où le gouvernement peut intervenir pour ériger ces ponts, aider à renforcer la communication déjà établie et créer un langage commun pour en parler, les choses ne pourront qu'aller mieux.

The Chair: It is in your self-interest, obviously.

Le président : C'est manifestement dans votre propre intérêt.

Mr. Hannah: Absolutely.

M. Hannah : Tout à fait.

The Chair: A breach in one institution would not only affect that one, but all of them; right?

Le président : Une violation dans une institution aurait des effets non seulement pour cette institution, mais aussi pour l'ensemble des établissements. Est-ce exact?

Mr. Hannah: Absolutely.

M. Hannah : Absolument.

The Chair: People would panic' right?

Le président : Il y aurait un mouvement de panique, non?

Mr. Hannah: It is certainly beneficial if you can share intelligence and knowledge across sectors because cybersecurity risks are, we'll call it, fungible. The same attack vectors and malware can be used in multiple circumstances.

M. Hannah : Il y a certainement des avantages à pouvoir s'échanger des renseignements et le savoir entre secteurs, puisque les risques en cybersécurité sont, nous dirons, fongibles. Les mêmes vecteurs d'attaque et les maliciels peuvent être utilisés dans de multiples circonstances.

The Chair: We demand certain safety measures, such as monitoring reserves, that banks have to use, and all the rest of it. Are you suggesting that we have some overall policy or legislation that would ensure new entrants to the marketplace have the same protection that the banks already have? Is there a minimum standard that could be legislated, or is the legislative process so slow it can't keep up with the technology of what is taking place?

Le président : Nous réclamons l'application de mesures de sécurité, comme la surveillance des réserves, que les banques sont tenues d'appliquer. Est-ce que vous suggérez d'instaurer une politique ou une loi générale en vertu de laquelle on veillerait à ce que les nouveaux participants du marché bénéficient de la même protection dont jouissent déjà les banques? Pourrait-on prévoir dans la loi une norme minimale ou le processus législatif est-il lent au point de ne pouvoir suivre la cadence de la technologie?

Mr. Ross: I think legislation would be helpful. You mention that legislation and the pace of change may not necessarily coincide. What we recommend, obviously, is to build the legislation that does allow for minimum standards and let regulators and the regulatory environment determine what those standards are, because they will change over time as the threats, systems and whatnot evolve.

M. Ross : Je suppose qu'une loi serait utile. Vous dites que la législation et le rythme du changement pourraient ne pas nécessairement coïncider. Nous recommandons, bien sûr, d'établir une loi qui autoriserait la mise en place de normes minimales et de laisser les organismes de réglementation et l'environnement réglementaire définir ces normes, car elles changeront au fur et à mesure que les menaces, les systèmes et ainsi de suite évolueront.

The Chair: I just don't want the legislation to have minimum standards. In other words, I don't want everybody to drive to the bottom. What you want is a lot of incentive for banks to continue increasing their standards of safety.

Le président : Je ne veux tout simplement pas que des normes minimales soient enchâssées dans une loi. Autrement dit, je ne veux pas que tout le monde s'en tienne au minimum. Inciter fortement les banques à continuer à resserrer leurs normes de sécurité, voilà ce que vous voulez.

Mr. Ross: There is no doubt about it. Again, banks understand regulation and they understand risk. I think that some of the things that banks do and understand would be helpful for other sectors to also follow.

The Chair: I was just going to get to that.

Mr. Ross: That is why our recommendation is that there need to be some common standards. I'm not suggesting that the same standard would apply to a bank as a small player. What I'm saying is there could some tiering and risk-based standards as relate to cybersecurity.

There are some absolute minimums. Regardless of the size of an organization, they do in some cases have the ability to inject cybercontagion into the essentially interconnected financial services and, in fact, beyond that. Again, we're talking about resilience and protection of Canadians across sectors that extend beyond banking.

The Chair: Senator Maltais, do you have another question? I didn't mean to interrupt you. You said it was the last one.

Senator Maltais: It is a quick question.

[*Translation*]

Would you be in favour of the federal government creating a regulatory organization grouping all cybersecurity services in the banking, financial and insurance sectors under federal regulation? Would you agree that one organization, of which you would all be members, be in charge of exchanging confidential information?

[*English*]

Mr. Ross: We certainly encourage and support federal jurisdiction. I think that's safe to say. I think there is an opportunity, again, to talk about having a lead agency, and we believe it should be at the federal level. Obviously, there may be some dynamics that need to be addressed as they relate to how financial institutions are regulated today. I mean, we have some that are under provincial bodies, but I absolutely think the value of creating a standard and a framework for all is that you can bring everyone up to a level of resilience.

At the end of the day, we are trying to create the resilience so we don't have to deal with and/or avoid impacts of an actual cyberbreach. I think that's fundamentally important and why our recommendations include things like the standardization of regulation and a centralized body.

M. Ross : Aucun doute à ce sujet; je le répète, les banques comprennent la réglementation et elles comprennent le risque. À mon avis, les banques font et comprennent certaines choses et d'autres secteurs auraient tout intérêt à s'en inspirer.

Le président : J'y arrivais justement.

M. Ross : Voilà pourquoi nous recommandons de mettre en place des normes communes. Je ne suggère pas d'appliquer la même norme à une banque modeste. Je dis qu'il pourrait y avoir certaines normes à paliers et axées sur les risques en matière de cybersécurité.

Il y a des seuils absolus. Peu importe la taille de l'organisation, elle peut parfois avoir la capacité de provoquer une cybercontagion dans les services financiers interdépendants et, en fait, au-delà de cela. Nous parlons encore de résilience et de protection des Canadiens dans l'ensemble des secteurs, sans nous limiter au secteur bancaire.

Le président : Sénateur Maltais, avez-vous une autre question? Je ne voulais pas vous interrompre. Vous aviez dit que c'était la dernière.

Le sénateur Maltais : J'ai une petite question.

[*Français*]

Seriez-vous d'accord pour que le gouvernement fédéral crée un organisme de réglementation où tous les services de cybersécurité, dans les secteurs bancaires, financiers et des assurances, seraient regroupés sous la réglementation fédérale? Seriez-vous d'accord à ce qu'un organisme, dont vous seriez tous membres, soit chargé de l'échange de renseignements confidentiels?

[*Traduction*]

M. Ross : Certes, nous encourageons et appuyons la compétence fédérale. Je pense qu'il est juste de le dire. À mon avis, nous avons l'occasion, je le répète, de discuter de la création d'un organisme principal et nous croyons que cela devrait se faire au niveau fédéral. Manifestement, il faudra peut-être se pencher sur certaines dynamiques portant sur la façon dont les institutions financières sont réglementées de nos jours. Je veux dire que certaines relèvent d'un organisme provincial, mais je suis absolument persuadé que l'établissement d'une norme et d'un régime s'appliquant à tous peut faire en sorte que tout le monde atteigne un niveau de résilience.

En fin de compte, nous nous efforçons d'instaurer la résilience afin de ne pas avoir à composer avec les conséquences d'une véritable violation de la cybersécurité ou à les éviter. Je pense que c'est fondamentalement important et c'est la raison pour laquelle nous recommandons notamment de normaliser la réglementation et de mettre en place un organisme central.

The Chair: I'm going to a second round. Even though we have until 12:30, we probably have, I would say, 15 or maybe 20 minutes of business that has to be done in camera. If you want an earlier lunch, govern yourself accordingly. Otherwise, you're going to run until 12:30.

[*Translation*]

Senator Boisvenu: What attracted my attention in your brief on page 2 is your statement that for the cybersecurity framework to be effective in Canada, we would need a single organization to take the lead. Obviously in the bureaucracy, the more people do the same tasks, the greater the risk of error. It's a very well-known theorem.

I have two questions for you. First of all, do you feel that there is a will to act on the part of the government? Next, what is the state of your relationship with the current government regarding its awareness of a situation which in your opinion presents some risks?

[*English*]

Mr. Ross: First, let me address the single body and it being housed within the federal government. We fully support a federally led single entity to manage cybersecurity and cyberawareness. I think there is value in doing so.

In the interaction today, we work very closely with the Department of Public Safety. As I said, we're partners in CCIRC under Public Safety. We also work with Finance and we work with law enforcement. So we do have a lot of interaction with federal agencies. Obviously, we have them with provincial counterparts as well.

We believe we have a lot of value to add to the ecosystem. We have a lot of knowledge. We invest heavily to ensure the safety and security of Canadians' financial data. Quite frankly, we have the ability to share some of that knowledge, and we want to share some of that knowledge with other industries and other sectors.

[*Translation*]

Senator Boisvenu: You are giving me a political answer. You say you have a lot of contacts and communications with these organizations, but that is not the question I asked. Where do you see real progress in the implementation of a strategy to ensure the safety of the banking system against cyberattacks? What progress have you seen in terms of putting in place a safety system?

Le président : Je commence un deuxième tour. Même si nous avons jusqu'à 12 h 30, nous devons probablement, selon moi, prévoir entre 15 et 20 minutes pour des travaux à huis clos. Si vous voulez manger plus tôt, agissez en conséquence. Autrement, vous devrez attendre à 12 h 30.

[*Français*]

Le sénateur Boisvenu : Ce qui a attiré mon attention dans votre mémoire, à la page 2, c'est lorsque vous affirmez que, pour que le cadre de cybersécurité soit efficace au Canada, il faudrait qu'un seul organisme en assure le contrôle. Évidemment, dans la bureaucratie, plus il y a de gens qui font les mêmes tâches, plus le risque d'erreur est grand. C'est un théorème tout à fait connu.

J'ai deux questions à vous poser. Tout d'abord, sentez-vous une volonté d'agir de la part du gouvernement? Ensuite, quel est l'état de vos relations avec le gouvernement actuel en ce qui concerne la sensibilisation face à la situation qui, selon vous, est à risque?

[*Traduction*]

M. Ross : Je vais d'abord répondre à la question au sujet du concept d'organisme unique relevant du gouvernement fédéral. Nous appuyons sans conteste l'idée d'une seule entité fédérale pour gérer la cybersécurité et la sensibilisation à cet égard. Je pense qu'il est utile de procéder ainsi.

S'agissant de l'interaction aujourd'hui, nous collaborons de près avec le ministère de la Sécurité publique. Comme je l'ai dit, nous sommes partenaires avec le CCRIC qui relève de Sécurité publique Canada. Nous collaborons également avec Finances Canada ainsi qu'avec les forces de l'ordre. Nous interagissons donc beaucoup avec les organismes fédéraux. De toute évidence, nous interagissons aussi avec les pendants provinciaux.

Nous pensons avoir beaucoup à apporter à l'écosystème. Nous en savons beaucoup. Nous investissons beaucoup pour garantir la sûreté et la sécurité des données financières des Canadiens. Franchement, nous sommes en mesure de partager une partie de ce savoir et nous voulons le faire avec d'autres industries et d'autres secteurs.

[*Français*]

Le sénateur Boisvenu : Vous me donnez une réponse politique. Vous me dites que vous entretenez beaucoup de relations et de communications avec ces organismes. Ce n'est pas la question que j'ai posée. De quelle façon sentez-vous qu'il y a eu une réelle progression dans la mise en place d'une stratégie pour assurer la sécurité du système bancaire contre les cyberattaques? Que remarquez-vous comme progression en termes de mise en place d'un système sécuritaire?

[*English*]

Mr. Ross: Within the financial sector, there is a large framework that has been set up in that sector to ensure cyber-resilience and protection of financial data. As I say, the threats continue to evolve, and we need to evolve with them. I do not believe we'll ever be at the end of the job in building out our co-operation with agencies both within government and law enforcement on this topic.

Senator Unger: I would like to go back to my previous questions. One of your recommendations is a single lead federal agency.

One comment: The federal government is being tight-lipped about how our recent security flaw found in virtually all Wi-Fi devices is affecting its departments, and public servants bringing their work home with them could be most at risk. My point is, the government is being tight-lipped about this issue.

So, if the banking institution is aware of this Krack vulnerability, which basically leaves the door open on all Wi-Fi networks, why would you not be informing your clients and at least recommending to them that they should connect to the Internet using a cable instead of Wi-Fi?

Mr. Ross: I believe what you referred to was the notion of Krack and federal government infrastructure. That is what I heard the question being. I think, quite frankly, that's something you would need to address with the federal government.

Senator Unger: I did. They were tight-lipped.

Mr. Ross: From our perspective, obviously there are instances where security issues reach beyond banking. Again, there is an opportunity and I think there is a need for federal leadership in this space to coordinate and build awareness out to those end points because, at the end of the day, we're talking about individuals, consumers and small businesses who need to be the ones who take actions to deal with any sort of a threat, such as the one you described.

Senator Wetston: You're well aware of the fact, as we all are, that federations invariably have extremely fragmented regulatory, legislative and constitutional systems to deal with significant issues like cybersecurity or other areas. If you can park this in the systemic risk area, you might have a chance to do it federally without any provincial or other concerns, given the Supreme Court reference on systemic risk a number of years ago that you would be familiar with.

My point is, if you look upstream, you talk about the telecommunications sector as a conduit through which electrical data flows. That's a big challenge from regulating the Internet,

[*Traduction*]

M. Ross : Un cadre imposant a été établi au sein du secteur financier pour garantir la cyberrésilience et la protection des données financières. Comme je l'ai dit, les menaces évoluent sans cesse et nous devons évoluer aussi. Je pense que nous ne finirons jamais de bâtir notre collaboration avec les organismes du gouvernement et avec les forces de l'ordre dans ce dossier.

La sénatrice Unger : Revenons sur quelques-unes de mes questions. L'une de vos recommandations porte sur la création d'un seul organisme fédéral.

Je dois dire que le gouvernement fédéral est peu loquace sur l'effet qu'ont sur ses ministères les failles du système de sécurité constatées récemment dans presque tous les dispositifs sans fil et sur le fait que les fonctionnaires qui apportent du travail à la maison sont les plus à risque. Je veux dire que le gouvernement est extrêmement discret à ce sujet.

Donc, si l'institution bancaire est au courant de cette vulnérabilité au krach, qui somme toute, ouvre la porte à tous les réseaux sans fil, pour quelle raison ne pas en informer vos clients et, à tout le moins, leur recommander de se brancher à Internet avec un câble au lieu du Wi-Fi?

M. Ross : Je pense que vous faites allusion à la notion de krach et à l'infrastructure du gouvernement fédéral. C'est ainsi que j'ai compris la question. À mon avis, il faudrait en saisir le gouvernement fédéral.

La sénatrice Unger : Je l'ai fait et ils sont restés muets.

M. Ross : Dans notre optique, les problèmes de sécurité vont parfois, de toute évidence, au-delà du secteur bancaire. Ici aussi le gouvernement fédéral pourrait et devrait faire preuve de leadership dans ce dossier pour coordonner et sensibiliser les intervenants à ces extrémités, car, en fin de compte, nous parlons des particuliers, des consommateurs et des petites entreprises qui doivent prendre des mesures pour affronter une menace quelconque, comme celle que vous avez décrite.

Le sénateur Wetston : Vous savez tous très bien, comme nous tous d'ailleurs, que les fédérations ont invariablement des systèmes réglementaire, législatif et constitutionnel extrêmement fragmentés pour faire face à des enjeux importants comme celui de la cybersécurité, entre autres. Si cet enjeu pouvait être intégré au domaine du risque systémique, il pourrait avec de la chance être réglé à l'échelle fédérale sans que des préoccupations de nature provinciale ou autre n'interviennent étant donné le renvoi au risque systémique fait par la Cour suprême il y a quelques années dont vous êtes au courant.

Ce que je veux dire, si on regarde en amont, c'est que vous avez dit que le secteur des télécommunications est le canal de diffusion des données électroniques. La réglementation

from freedom of expression and Charter issues, privacy issues. You're suggesting that the federal government should look at legislative options to deal with that — I call it more of an upstream issue, which, of course, is critical.

Do you have more to say about that? Have you done more thinking about that? What would those legislative options be? I realize you're focused on banking through your membership, but it has a broad effect on the economy. Concerns in your area can certainly create systemic risk in the economy should you have those kinds of serious challenges. Do you have any thoughts about that that you can share with the committee?

Mr. Ross: I believe that telecommunications falls under federal jurisdiction.

Senator Wetston: It does.

Mr. Ross: I would suggest that is one of the easier sectors to provide greater oversight. We mentioned in our remarks some of the challenges we have related to PIPEDA that limit the ability to share intelligence. It goes back to trying to build resilience, not dealing with a fraud after the fact.

Senator Wetston: Let me stop you there. I'm asking whether you have done more detailed thinking about this issue that you might be able to share with the committee, other than these general observations, which I'm not taking issue with; they are very real. If you haven't, you haven't. I'm digging more deeply here as to whether you can share that information.

Mr. Hannah: If I can jump in here, the approach we have taken is to try and lay out the architecture that we think would be appropriate, trying to make sure there are common standards across sectors. Recognizing there are jurisdictional issues, we would hope they can be resolved because, at the end of the day, the threat doesn't care about the jurisdiction in this particular case.

We believe that improved information sharing would be a key component of that. We think there needs to be a lead agency on that. We are strongly of the view that coming out of this, there has to be a mechanism to reduce the amount of malicious traffic because it flows out; there has to be a way to stop that.

We think irrespective of jurisdiction, there has to be an education effort, both for small businesses and for individuals to try to make sure that people understand and can take action themselves. From our point of view, we have taken the architectural approach. Once we have moved past that, then we

d'Internet et la prise en compte des questions de liberté d'expression, de Charte et de protection de la vie privée représentent un défi de taille. Vous laissez entendre que le gouvernement fédéral devrait envisager des solutions législatives face à cet enjeu — je parle plus d'un enjeu en amont qui, bien entendu, est important.

Avez-vous quelque chose à ajouter à ce sujet? Y avez-vous réfléchi davantage? En quoi consisteraient ces solutions législatives? Je comprends que vous ciblez le secteur bancaire par l'entremise de vos membres, mais cela a un vaste effet sur l'économie. Des craintes dans votre domaine peuvent certainement générer un risque systémique dans l'économie si vous êtes confrontés à des enjeux importants du genre. Avez-vous des idées à ce sujet, dont vous pourriez faire part aux membres du comité?

M. Ross : Je pense que les télécommunications sont de compétence fédérale.

Le sénateur Wetston : En effet.

M. Ross : Je dirais que c'est l'un des secteurs qu'il serait plus facile de surveiller davantage. Nous avons dit, dans nos remarques, avoir certains défis à cause de la LPRPDE qui limite la capacité d'échanger des renseignements. Cela revient à essayer de bâtir la résilience et non de composer avec une fraude après coup.

Le sénateur Wetston : Permettez-moi de vous interrompre. Je me demande si vous avez des réflexions plus précises à ce sujet dont vous pourriez faire part au comité, autres que ces observations générales avec lesquelles je ne suis pas en désaccord : elles sont très concrètes. Si vous ne l'avez pas fait, vous ne l'avez pas fait, c'est tout. J'insiste ici sur la question à savoir si vous pouvez communiquer cette information.

M. Hannah : Nous avons adopté comme approche, si je peux intervenir, d'essayer de définir l'architecture qui, selon nous, serait appropriée et de garantir des normes communes dans tout le secteur. Nous savons qu'il y a des questions de compétence et nous espérons qu'elles puissent se régler, car, en fin de compte, la menace n'est pas limitée par la compétence dans ce cas en particulier.

Nous estimons qu'il serait important, dans ce contexte, d'améliorer l'échange d'informations. À notre avis, il faudrait un organisme principal. Nous croyons fermement que ces réunions doivent permettre d'élaborer un mécanisme pour réduire le trafic malveillant parce que les données malveillantes circulent; il doit y avoir un moyen d'y mettre un terme.

Peu importe la compétence, nous pensons qu'il faut éduquer tant les petites entreprises que les particuliers pour essayer de veiller à ce que ces gens comprennent la situation et qu'ils puissent eux-mêmes prendre des mesures. Nous, nous avons adopté l'approche de l'architecture. Une fois cette étape franchie,

can get to the substance of how one gives effect to that. But that has been our focus.

The Chair: Thank you. Are we all done? If we are, thank you witnesses. We will say goodbye to the witnesses, then reconvene and do our in camera business.

(The committee continued in camera.)

nous pourrons alors nous attarder à la mise en pratique. Or, c'était notre souci principal.

Le président : Merci. Avons-nous terminé? Si oui, je remercie ceux qui ont comparu. Nous allons dire au revoir aux témoins, puis nous reprendrons la séance et poursuivrons nos travaux à huis clos.

(La séance se poursuit à huis clos.)

WITNESSES

Canadian Bankers Association:

Darren Hannah, Vice President, Finance, Risk and Prudential Policy;

Andrew Ross, Director, Payments and Cyber Security;

Sandy Stephens, Assistant General Counsel.

TÉMOINS

Association des banquiers canadiens :

Darren Hannah, vice-président, Finances, risques et politique prudentielle;

Andrew Ross, directeur, Paiements et cybersécurité;

Sandy Stephens, avocate-conseil adjointe.