# Système bancaire ouvert

02/11/2019

Mémoire soumis à
Finances Canada

ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

# Introduction

L'Association des banquiers canadiens est heureuse de soumettre le présent mémoire au ministère des Finances en réponse au document de consultation sur les mérites d'un système bancaire ouvert au Canada (document de consultation). Les banques favorisent un secteur des services financiers concurrentiel et novateur, qui utilise les solutions technologiques au développement rapide afin de mieux servir les consommateurs et répondre aux attentes grandissantes de ses clients. Les banques du Canada ont toujours été les premières à adopter les nouvelles technologies susceptibles de rendre les activités bancaires simples et pratiques pour les consommateurs, tout en cultivant leur confiance. Tournées résolument vers l'avenir, les banques ont aménagé des centres d'innovation internes et établi des partenariats avec des organisations externes, notamment des universités, des incubateurs et des entreprises de technologie, en vue d'imaginer, de concevoir et de livrer des innovations et des solutions numériques pour leurs clients.

À titre d'intervenant clé qui serait grandement affecté par l'évolution vers un système bancaire ouvert au Canada, le secteur bancaire est heureux de cette possibilité de poursuivre sa collaboration avec le gouvernement fédéral en vue de comprendre pleinement les avantages et les risques d'un système bancaire ouvert. Dans le présent mémoire, nous soumettons notre point de vue sur le système bancaire ouvert dans un contexte purement canadien, et axons nos commentaires sur des thèmes soulevés dans le document de consultation, dans l'ordre suivant :

- **Contexte canadien**
- **Risques potentiels d'un système bancaire ouvert**
    1. **Protection des consommateurs**
    2. **Vie privée et confidentialité**
    3. **Crimes financiers**
    4. **Stabilité financière**
- **Rôle du gouvernement fédéral**

Nous serons ravis d'explorer d'autres thèmes pertinents avec le gouvernement fédéral, à mesure que progresse l'examen des mérites d'un système bancaire ouvert.

# Contexte canadien

Nous sommes d'accord avec le commentaire dans le document de consultation affirmant qu'un système bancaire ouvert offre des avantages pour les consommateurs, dont les PME, les institutions financières comme les banques, et les autres fournisseurs tiers de services financiers. Pourvu que les risques inhérents à un système bancaire ouvert soient gérés efficacement, un tel système donnera aux consommateurs la possibilité de partager plus facilement les données propres à leurs opérations financières, et de tirer profit des produits et services nouveaux et novateurs qui seront personnalisés selon leurs besoins.

Comme mentionné dans le document de consultation, différents pays ont adopté différentes approches, selon le niveau et l'ampleur de l'activité du marché, ainsi que la portée des catalyseurs ayant déclenché les réactions politiques et celles du marché dans ces pays. Plusieurs pays ont commencé à explorer les possibilités d'un système bancaire ouvert à la suite de la crise financière mondiale de 2008-2009. Les défaillances systémiques bancaires et la perte de confiance qui s'en est suivie ont obligé le marché et les décideurs à trouver des solutions de rechange à leur système bancaire. Contrairement aux institutions financières dans ces pays, les banques du Canada ont survécu à la crise financière mondiale et maintenu un très haut niveau de confiance de la part des consommateurs. Dans son examen des modèles de système bancaire ouvert qui sont explorés, introduits ou mis en œuvre ailleurs dans le monde, le gouvernement est vivement encouragé à regarder ces modèles d'une optique purement canadienne.

Également, le document de consultation souligne la nécessité d'examiner soigneusement le contexte plus large des initiatives stratégiques qui affectent le secteur financier au Canada parallèlement à l'examen des mérites d'un système bancaire ouvert. Nous sommes d'accord avec la lumière jetée dans le document sur l'initiative de modernisation des paiements, sur les consultations en matière de numérique et de données et sur la stratégie nationale de cybersécurité. En ce qui concerne l'initiative de modernisation des paiements en particulier, nous sommes du même avis présenté dans le document de consultation que si le gouvernement décidait d'adopter un système bancaire ouvert comprenant l'initiation des paiements, « on procéderait aux différentes étapes appropriées de l'harmonisation à la modernisation du système des paiements ». Vous n'êtes pas sans savoir que la portée et la feuille de route de l'initiative de modernisation des paiements au Canada sont particulièrement ambitieuses et complexes et exigent des intervenants des coûts et des ressources considérables. Aussi, des efforts doivent être investis afin d'améliorer les options offertes aux clients en veillant à ce que les fournisseurs tiers et les autres sources de données clients soient tenus d'échanger ces renseignements selon les

mêmes modalités lorsque le client demande cet échange. Plus généralement, le gouvernement pourra envisager les données clients dans le contexte de secteurs autres que le secteur bancaire, et voir comment le fait que les clients contrôlent plus facilement leurs propres données dans ces secteurs stimulerait l'innovation. Dans le contexte de la révision de l'interaction entre un système bancaire ouvert et ces autres initiatives, il est essentiel pour Finances Canada de poursuivre la discussion et la collaboration avec les décideurs politiques et les organismes de réglementation qui sont directement impliqués dans ces initiatives, de même que les organismes de réglementation qui se penchent sur les divers enjeux liés au système bancaire ouvert, comme le Commissariat à la protection de la vie privée du Canada et le Bureau du surintendant des institutions financières.

Jusqu'à présent, les institutions financières canadiennes ont grandement investi dans le développement de l'infrastructure nécessaire à la protection et à la sécurité des renseignements personnels et financiers des clients. Donner à un plus grand nombre de fournisseurs tiers un accès aux données financières emmènera progressivement une plus forte demande opérationnelle et technique sur l'infrastructure et les nouveaux systèmes, nécessitant des efforts continus pour l'entretien, les améliorations et la formation. Par conséquent, l'examen des modèles de système bancaire ouvert devra tenir compte de la façon dont les autres participants du marché pourront contribuer aux capacités fondamentales que les institutions financières ont établies, et continuent d'améliorer, en vue de soutenir la pérennité d'une gouvernance et d'une protection adéquates des données.

# Risques potentiels d'un système bancaire ouvert

Afin d'obtenir tous les avantages potentiels d'un système bancaire ouvert, il faudra écarter et réduire les risques connexes par une division adéquate des responsabilités entre tous les participants, notamment les consommateurs, les institutions financières et les autres fournisseurs tiers.

Dans les pages suivantes, nous exposons notre opinion au sujet des risques potentiels et des stratégies de mitigation associés aux quatre domaines soulignés dans le document de consultation.

## 1. Protection des consommateurs

Nous appuyons les observations notées dans le document de consultation au sujet de l'importance de la protection des consommateurs. Les renseignements personnels et confidentiels des clients doivent être maintenus en toute sécurité, en tout temps, par tous les participants au système bancaire ouvert, y compris les fournisseurs tiers. Les renseignements des clients doivent être communiqués seulement

après avoir obtenu le consentement éclairé de la personne en cause, de façon transparente qui permet au client de comprendre comment les données relatives à ses opérations financières seront utilisées et conservées en toute sécurité. Également, les clients devront recevoir l'information nécessaire pour prendre des décisions éclairées au sujet des services offerts par un fournisseur tiers, notamment tout produit ou service offert comme valeur ajoutée. Par ailleurs, il est essentiel que les consommateurs comprennent la procédure de recours dont ils disposent dans le cas de violation des données ou d'utilisation abusive des données sur les opérations financières par un tiers fournisseur. Une fois qu'un fournisseur tiers a reçu les données relatives aux opérations financières, il en devient entièrement responsable, y compris dans les cas de mauvais usage. À cette fin, il faudra penser aux exigences auxquelles les fournisseurs tiers doivent se soumettre afin de respecter leurs obligations financières envers les clients : fonds, liquidité, assurance, etc. Ce point est particulièrement important lorsque le fournisseur tiers est une société de technologie qui n'est pas soumise au même cadre de supervision exhaustif que les banques canadiennes. Le développement d'un système bancaire ouvert au Canada doit tenir compte aussi de la façon de réglementer certains participants, là où il y a une lacune dans la réglementation, notamment les fournisseurs tiers qui ne sont pas sous réglementation fédérale, les fournisseurs tiers qui ne sont pas canadiens et les fournisseurs tiers qui auront accès au système par association. Il est essentiel que les clients soient protégés, peu importe la nature du fournisseur tiers. À mesure que de nouveaux modèles de gestion font surface, il est essentiel que les clients ne perdent pas les mécanismes de protection qui leur sont accordés par la réglementation applicable aux institutions financières.

Le point suivant traitant des effets sur la confidentialité d'un système bancaire ouvert contient des commentaires additionnels au sujet des éléments spécifiques à la protection des consommateurs qui sont nécessaires afin de veiller à ce que les consommateurs bénéficient réellement du système bancaire ouvert.

## 2. Renseignements personnels et confidentialité

L'investissement massif dans la technologie, les infrastructures et la formation en vue de protéger les renseignements personnels et confidentiels que les clients leur ont confiés est une priorité des institutions financières. Toutefois, la protection de ces renseignements doit être une responsabilité commune à tous les participants au système bancaire ouvert, y compris les clients et les autres fournisseurs tiers. Le traitement de renseignements délicats, extrêmement personnels et confidentiels est une tâche clé dans tout modèle de système bancaire ouvert. Le traitement de tels renseignements fait appel à l transparence et au consentement éclairé des clients, à des normes homogènes applicables à l'utilisation et à la gestion

responsables des données sur les opérations financières des clients, ainsi qu'à des mécanismes de sécurisation de ces données.

La réussite d'un système bancaire ouvert dépend de la présence d'un niveau élevé de confiance. Et la confiance dans un système bancaire ouvert, de même que son adoption à large échelle, est favorisée par le respect du principe de la confidentialité des données, qui en est en fait une composante clé. La confidentialité est l'un des éléments essentiels auquel s'attend le client, qui l'amène à avoir confiance dans les gardiens traditionnels de ses données sur les opérations financières. Un autre aspect favorisant la confiance est l'utilisation et la gestion responsables des données sur les opérations financières. Les institutions financières ont développé des normes, qu'elles respectent, garantissant l'absence d'un mauvais usage de données ainsi que la présence de mécanismes de protection de ces données. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), loi exhaustive, neutre sur le plan technologique et fondée sur des principes, s'applique à toutes les organisations canadiennes parallèlement à une législation provinciale similaire le cas échéant. La LPRPDE offre le cadre législatif et la souplesse nécessaires pour répondre aux préoccupations émergentes en matière de dispositions législatives sur la protection des renseignements personnels échangés aux fins du système bancaire ouvert.

Aux termes de la LPRPDE, la connaissance et le consentement sont généralement requis préalablement à la collecte, à l'utilisation ou à la communication de renseignements personnels. Le consentement est valide seulement lorsqu'il est raisonnable de s'attendre à ce que l'individu comprenne la nature, la fin et les conséquences de la collecte, de l'utilisation ou de la communication de ses renseignements personnels.  Par ailleurs, la collecte, l'utilisation ou la communication de renseignements personnels se limitent aux fins qu'une personne raisonnable jugerait adéquates dans les circonstances. Conformément à ces exigences, les fournisseurs tiers devront expliquer clairement aux clients quels renseignements personnels spécifiques seront recueillis, comment ces renseignements seront utilisés, à qui ils seront communiqués, comment les droits d'un client pourront être limités, ainsi que tout dommage potentiel qui pourrait découler du partage des renseignements personnels du client. Également, les fournisseurs tiers devront expliquer aux clients la procédure de recours si jamais leurs renseignements personnels ont été compromis d'une façon ou d'une autre, et leur fournir un processus simple leur permettant de retirer leur consentement. La déclaration aux clients est importante pour que le client puisse garder le contrôle des données sur ses opérations financières. Elle doit faire partie des exigences (sécurité et autres) que les fournisseurs tiers, ainsi que tous les participants à l'écosystème, doivent respecter. À cet égard, le Commissariat à la protection de la vie privée possède un pouvoir élargi de surveillance et d'application de la loi, notamment la capacité de mener des vérifications sur les politiques et les pratiques en matière de renseignements personnels des organisations, de conclure des ententes de conformité avec des

organisations et de renvoyer les organisations non conformes devant la cour fédérale.

Le principe de responsabilité, à l'annexe 1 de la LPRPDE, est particulièrement important dans le contexte d'un système bancaire ouvert. Ce principe stipule qu'une organisation est responsable des renseignements personnels dont elle a la gestion. Lorsqu'un client demande à une institution financière de communiquer ses renseignements personnels à un fournisseur tiers, ce dernier aura la responsabilité exclusive de ces renseignements personnels dont il a la gestion[1]. Étant donné que dans un système bancaire ouvert les fournisseurs tiers sont responsables des renseignements personnels dont ils ont la gestion, il est essentiel qu'ils se conforment aux exigences de la LPRPDE – y compris l'exigence d'adopter des mesures de protection correspondant au degré de sensibilité des renseignements personnels en question. Il faudra prêter une attention particulière aux divers niveaux de sophistication des participants au système bancaire ouvert, ainsi qu'au besoin de veiller à ce que tous les participants comprennent leurs droits et leurs responsabilités au titre de la LPRPDE. Ce volet peut être réalisé de diverses façons, notamment au moyen d'ententes contractuelles entre participants, de normes sectorielles ou encore d'un processus d'accréditation des fournisseurs tiers auprès d'un organisme sectoriel ou de réglementation comme c'est le cas du modèle suggéré dans le cadre de surveillance des paiements de détail[2]. En outre, les campagnes d'éducation et de sensibilisation du Commissariat à la protection de la vie privée sont des exigences essentielles. Le client doit comprendre la différence entre le consentement qu'il donne à son institution financière, lequel régit le partage des données sur ses opérations financières avec un fournisseur tiers, et le consentement qu'il donne au fournisseur tiers, lequel régit l'utilisation de ces données par le fournisseur tiers et le recours dont dispose le client envers ce fournisseur.

Bien que la LPRPDE s'applique aux renseignements personnels, il importe de noter que les obligations de confidentialité que suivent les institutions financières dépassent les renseignements personnels. Les fournisseurs tiers doivent donc répondre à des exigences similaires à celles que nous avons détaillées en matière de protection plus générale de la confidentialité des données sur les opérations financières des clients. De même, il est essentiel de différencier clairement entre les données sur les opérations financières des clients et les renseignements exclusifs (p. ex., données enrichies) des institutions

[1] Conformément à la LPRPDE, cette communication à la demande du client est différente de la communication dans le cas où l'organisation confie le traitement des renseignements personnels à une tierce partie. Dans ce cas, l'organisation qui fait le transfert demeure responsable des renseignements personnels ainsi communiqués – consulter le bulletin d'interprétation du Commissariat à ce sujet : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/bulletins-sur-l-interpretation-de-la-lprpde/interpretations_02_acc/

[2] Le Cadre de surveillance des paiements de détail exige de tous les fournisseurs de services de paiement de s'inscrire auprès « de l'organisme de réglementation fédéral des paiements de détail désigné » et de fournir à cet organisme une liste complète de renseignements spécifiques.

financières. Il sera essentiel de reconnaître et de préserver les capacités des institutions financières à protéger leurs renseignements exclusifs dans un contexte de système bancaire ouvert.

La déclaration aux clients est importante pour que ces derniers puissent garder le contrôle des données sur leurs opérations financières. Toutefois, n'étant pas suffisante pour un système robuste, la déclaration doit s'accompagner d'exigences de sécurité et autres, que doivent respecter les fournisseurs tiers ainsi que tous les participants à l'écosystème. Afin de profiter de tous les avantages décrits dans le document de consultation, un système bancaire ouvert doit comprendre des mesures de sécurité adéquates et d'autres mécanismes de protection pour les données sur les opérations financières à l'échelle de l'écosystème, de même qu'un processus de règlement des plaintes efficace.

## 3. Crime financier

Un système bancaire ouvert comprend des caractéristiques spécifiques – prolifération des données, connectivité accrue, usage de coordonnées de connexion par les fournisseurs tiers pour accéder aux données des clients, etc. – qui le rendent vulnérable au crime financier. Il est essentiel de comprendre ces risques et les qu'ont les participants au système bancaire ouvert pour les gérer.

Lorsqu'un plus grand nombre de parties transmet et conserve des données sur les opérations financières (prolifération de données), les risques de prise de contrôle de comptes et de vol d'identité augmentent – surtout si les niveaux de contrôle sur les mesures de protection, dont les normes d'authentification, diffèrent d'un participant du marché à un autre. Une plus forte connectivité au sein du système bancaire ouvert augmente le niveau de vulnérabilité des réseaux. Si les institutions financières n'ont pas un accès direct à toutes les données sur les opérations financières des clients et sur les renseignements au sujet des appareils que ces derniers utilisent, leur capacité de se servir des données sur les opérations financières aux fins de l'authentification multifactorielle pourrait être affectée, de même que leur capacité de gérer les risques de fraude et d'empêcher le mauvais usage des données au moyen de la surveillance des opérations.

Également, la pratique courante suivie par les fournisseurs tiers de se servir des coordonnées de connexion bancaires pour accéder aux données sur les opérations financières conduit à un stockage des coordonnées de connexion bancaires par les fournisseurs tiers, ce qui les rend vulnérables au crime financier. Si un fournisseur tiers n'a pas des mécanismes de contrôle solides, les risques qu'une cyberattaque réussisse sont grands, se soldant par une fraude et des pertes potentielles pour les clients. De plus, comme les institutions financières n'ont pas une idée du nombre de clients ayant partagé leurs

coordonnées de connexion bancaires avec des fournisseurs tiers, une cyberattaque sur le fournisseur tiers sera difficile à déceler, à maîtriser et à gérer.

La mise en place de mesures de sécurité adéquates par les fournisseurs tiers, et plus particulièrement l'utilisation de procédures solides d'authentification des clients, est une exigence clé pour la gestion des risques de prolifération des données et de connectivité accrue, qui sont associés au système bancaire ouvert. En outre, les nouvelles interfaces de programmation d'applications (interfaces) doivent continuer à ne permettre l'accès qu'au moyen de protocoles de communication sécurisés qui facilitent la communication entre les systèmes des institutions financières et les fournisseurs tiers, sans que le client ait à partager ses coordonnées de connexion bancaires. Ainsi, grâce aux interfaces, les fournisseurs tiers peuvent accéder aux données sans conserver les coordonnées de connexion bancaires des clients, en tirant plutôt profit des processus solides d'authentification et d'autorisation des institutions financières, ce qui réduit le risque d'exposer les coordonnées de connexion des clients. De plus, pour donner un accès à travers les interfaces spécifiques aux institutions financières, le service permettra de désactiver cet accès à la demande du client ou en cas de problème de sécurité. La plupart des marchés favorisent une norme d'interface spécifique, ce que le secteur financier au Canada peut faire.

Évidemment, la tâche de réglementer un plus grand nombre de participants dans un système bancaire ouvert est plus complexe. Avec les multiples nouveaux arrivants, il se peut qu'il y ait une inégalité entre les divers niveaux de sécurité et de protection, créant ainsi des vulnérabilités dans le système financier. Bien que plusieurs exigences soient traitées dans les dispositions actuelles de la LPRPDE et puissent faire l'objet d'ententes avec les fournisseurs tiers, il y a également une opportunité pour le secteur d'adopter des normes de sécurité spécifiques qui seraient un moyen plus efficace et plus souple d'assurer la conformité aux exigences portant sur la conservation, le traitement et la communication sécuritaires des données des clients.

Les clients aussi jouent un important rôle à cet effet. La sécurité des données sur les opérations financières des clients est d'une grande importance pour les institutions financières, qui consacrent des sommes énormes à la protection de ces données. Les institutions financières sont conscientes des menaces continues pour les renseignements des clients et effectuent une surveillance soutenue des activités afin d'assurer la protection des données. Les institutions financières ont certes prévu des systèmes complexes afin de protéger leurs clients contre les menaces, il n'en demeure pas moins que le gouvernement a la responsabilité d'éduquer les consommateurs sur les répercussions du partage de leurs renseignements avec les fournisseurs tiers. Les efforts soutenus d'éducation en matière de

sensibilisation à la cybersécurité sont essentiels pour que les consommateurs comprennent les étapes requises pour se protéger dans un environnement de système bancaire ouvert.

## 4. Stabilité financière

Comme soulevé dans le document de consultation, il faudra examiner aussi les risques pour la sécurité, la robustesse et la stabilité du système financier canadien dans son ensemble si les fournisseurs tiers ont accès aux données financières dans un système bancaire ouvert. Les consommateurs au Canada ont confiance dans notre système financier en raison de sa stabilité, qui s'est matérialisée dans le rendement des banques canadiennes durant la crise financière de 2008-2009. Pendant que le gouvernement fédéral explore les mérites d'un système bancaire ouvert, il est important de veiller à ce que la confiance des Canadiens dans leur système financier ne soit pas mise à l'épreuve. Le Conseil de stabilité financière a bien reconnu le besoin d'être prudent face aux innovations financières technologiques au stade précoce de leur développement, lorsqu'il a précisé que, même si les innovations ne semblent pas présenter actuellement un risque pour la stabilité financière, la vitesse à laquelle s'opèrent les changements en ce qui a trait aux FinTech pourra conduire à des prises de décision qui établiraient de graves précédents[3]. Dans le principe, ce point de vue s'applique également au système bancaire ouvert qui est à un stade précoce de son développement et de sa mise en œuvre dans de nombreux autres pays. Dans un tel contexte, le risque qui guette la stabilité financière doit être surveillé de près.

# Rôle du gouvernement fédéral

Le Canada est depuis toujours un chef de file mondial en matière de développement de solutions bancaires destinées à répondre aux grands objectifs de politique publique, grâce à une relation entre les institutions financières et les organismes de réglementation qui est fondée sur de solides consultations et une étroite collaboration. Une évaluation des moyens utilisés par d'autres pays afin d'introduire et de mettre en œuvre leur système bancaire ouvert montre une dépendance à la fois au secteur financier et aux organismes de réglementation, dépendamment des facteurs motivant la politique sous-jacente au système bancaire ouvert dans chacun de ces pays, ainsi que de son environnement juridique et réglementaire.

[3] Conseil de stabilité financière, *Financial Stability Implications from FinTech, Supervisory and Regulatory Issues that Merit Authorities' Attention*, le 27 juin 2017. Le Conseil de stabilité financière définit les FinTech comme des innovations financières facilitées par la technologie, pouvant aboutir à de nouveaux modèles, applications, processus ou produits et ayant de grandes retombées sur les marchés financiers et les institutions financières ainsi que sur la prestation de services financiers.

Dans certains pays, les autorités financières imposent aux banques l'obligation de donner à tous les fournisseurs tiers accrédités un accès aux renseignements de tout client qui aurait présenté tous les consentements requis. Dans de tels cas, l'organisme de réglementation financière supervise la gestion des risques de même que celle des stratégies de mitigation connexes exposées dans le présent mémoire, telles que les critères et procédures d'accréditation, les cadres de responsabilité adéquats, ainsi que les mécanismes susceptibles d'aider les fournisseurs tiers à honorer leurs responsabilités financières envers les clients (p. ex., assurance de responsabilité civile professionnelle ou garanties comparables). Ailleurs, les banques collaborent avec d'autres participants du marché, comme les organismes de réglementation, les entreprises de technologie financière et les agrégateurs de données, en vue de permettre un accès aux données des clients avec le consentement de ces derniers. Ces participants s'efforcent de garantir un accès sécurisé aux données en élaborant des normes techniques et des pratiques exemplaires pour les cadres d'authentification, de consentement, d'accès et de responsabilité. Des entités sectorielles sont formées dans l'objectif de contribuer à augmenter le potentiel d'efficacité dans l'écosystème en prévoyant, entre autres, des normes techniques et de sécurité communes et des critères d'accréditation minimales.

Dans ce mémoire, nous avons décrit le contexte canadien unique, ainsi que les risques envisageables et les solutions possibles dans le cadre de notre environnement juridique et réglementaire, dont il faut tenir compte dans l'évaluation de la façon de procéder au Canada.

# Conclusion

L'ABC soutient fermement l'innovation et la concurrence dans le secteur des services financiers, stimulées par les progrès technologiques. Vu que la sécurité des clients et l'expérience client sont au cœur des activités bancaires, nous avons décrit dans le présent document les risques potentiels qui doivent être écartés afin que les consommateurs au Canada et le secteur financier canadien puissent pleinement profiter d'un système bancaire ouvert et de mécanismes d'atténuation des risques.  À mesure que le ministère des Finances avance dans l'examen des mérites d'un système bancaire ouvert, nous resterons prêts à poursuivre notre collaboration sur ses enjeux et à acquérir une compréhension plus poussée des objectifs de politique qui sous-tendent cet examen.