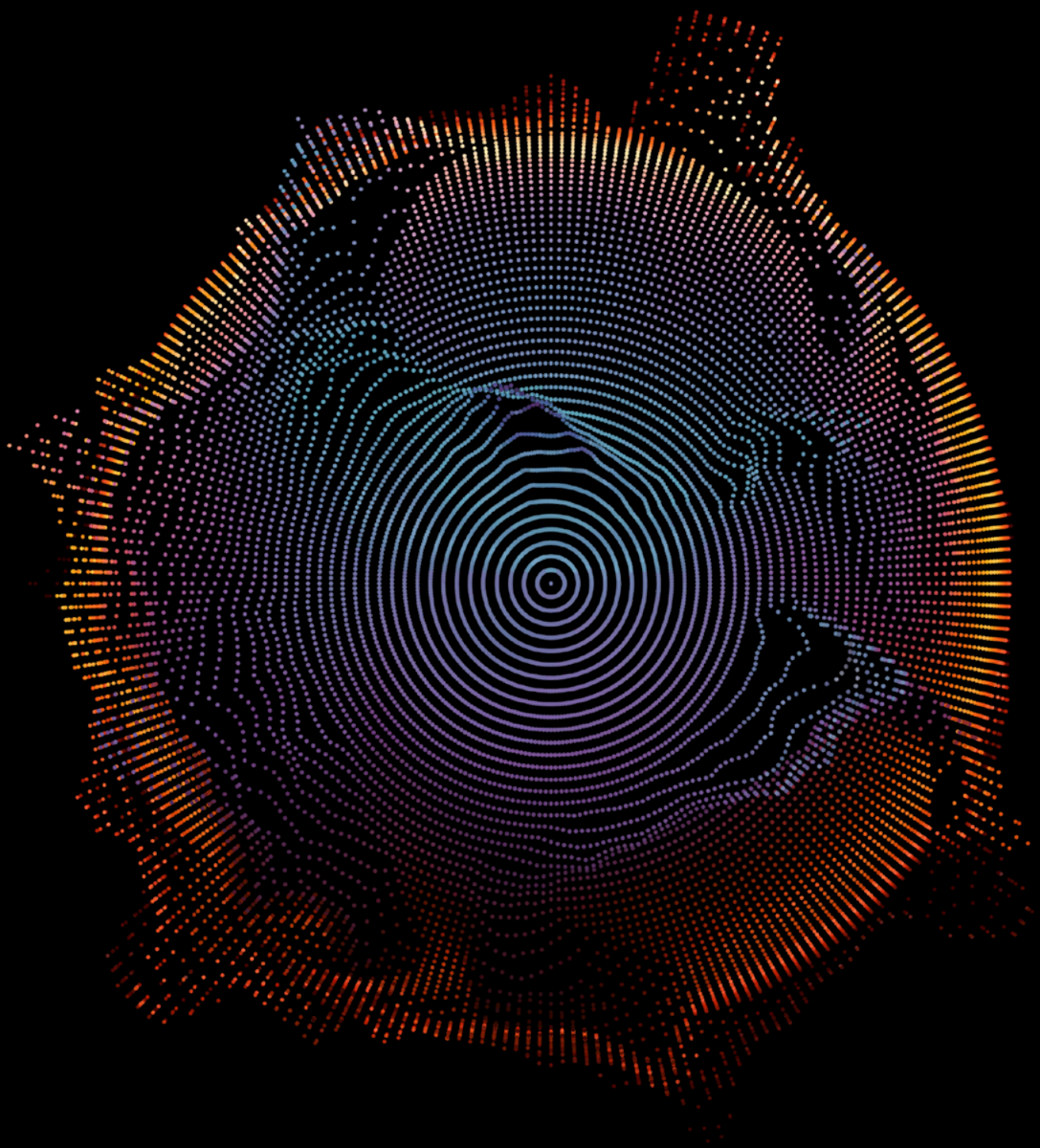
Deloitte.



Créer un cadre pour régir un système bancaire ouvert au Canada

Éléments à considérer et incidence des principaux choix liés à la conception

Table des matières

Sommaire **2**

Introduction **4**

Qu'est-ce que le système bancaire ouvert ? **5**

Forces motrices du mouvement du système bancaire ouvert **6**

Méthodes actuelles de partage des données dans les services financiers **8**

Les données ouvertes et l'avenir des services financiers **10**

Système bancaire ouvert et risques émergents **12**

Points à considérer pour un cadre de système bancaire ouvert au Canada **14**

Le contexte canadien **20**

Principes de conception d'un cadre de système bancaire ouvert **22**

Un cadre de système bancaire ouvert pour le Canada **24**

Aperçu du cadre **25**

1. Étendue du système bancaire ouvert **26**

2. Normes **38**

3. Modèle commercial et modèle de responsabilité **50**

Conclusion **54**

Sommaire

À mesure que croît l'importance stratégique des données dans l'économie numérique, divers modèles visant à permettre aux consommateurs de partager leurs données personnelles avec des organisations tierces prolifèrent dans le secteur des services financiers. Au cours des cinq dernières années, sur la base du principe de contrôle des clients et de portabilité de leurs données personnelles, de nombreux territoires à l'échelle mondiale se sont dotés de modèles réglementaires ou sectoriels pour donner accès aux données dans un système bancaire ouvert afin de combler les lacunes des modèles d'accès aux données actuels et d'accélérer les innovations fondées sur les données.

Permettre aux clients de partager leurs données financières personnelles avec des tiers de confiance peut potentiellement donner lieu à des améliorations et à la création de valeur dans les services financiers – qu'il s'agisse de conseils numériques, d'automatisation financière ou de nouveaux produits. Toutefois, ouvrir l'accès aux données de nature sensible sans établir les protections appropriées peut également poser de nouveaux risques pour le système financier et ruiner la nouvelle plus-value créée.

Le Canada est reconnu pour sa capacité de maintenir la sécurité et la stabilité de son secteur financier. À mesure que progresseront les discussions sur le système bancaire ouvert dans les années à venir, le Canada a une occasion unique de concevoir un modèle d'accès aux données par des tiers qui présente une valeur suprême pour les clients en combinant l'innovation et l'aspect concurrentiel avec la préservation de la résilience du système.

Créer un cadre pour régir un système bancaire ouvert au Canada | Sommaire

Pour ce faire, le Canada doit amorcer une réflexion sur les objectifs ultimes du système bancaire ouvert et les caractéristiques uniques du secteur canadien des services financiers et en tenir compte pour concevoir le cadre d'accès aux données. Pendant ce processus de conception, les intervenants devront notamment répondre aux trois questions essentielles suivantes :

1. Étendue

Quels types de données et quelles institutions devraient être concernés par le cadre ?

2. Normalisation

Dans quelle mesure la gouvernance, le partage des données et l'authentification doivent-ils être centralisés et normalisés ?

3. Modèle commercial et modèle de responsabilité

Comment les interactions entre les générateurs de données et les utilisateurs de données devraient-elles être structurées ?

Ce document vise à aider les principaux intervenants à prendre en considération les incidences de ces décisions en analysant les choix qui ont été faits par d'autres territoires afin d'établir un cadre de système bancaire ouvert qui convient aux Canadiens. Nous sommes convaincus qu'en orientant efficacement la discussion et en apprenant des expériences d'autres territoires, le Canada a la capacité non seulement de tirer profit des avantages d'un système bancaire ouvert, mais aussi d'établir un plan pour une véritable économie numérique.

Introduction

Qu’est-ce que le système bancaire ouvert ?

Le système bancaire ouvert est un mouvement mondial faisant la promotion du droit des consommateurs à partager leurs renseignements financiers avec des tiers.

Bien que de nombreux territoires disposent de politiques établies en vertu des lois à l’égard du système bancaire ouvert, ce dernier est plus qu’une politique – c’est un mouvement constitué de changements techniques, concurrentiels et réglementaires pour aider les consommateurs à reprendre le contrôle de leurs propres données et en améliorer la portabilité entre les institutions.

Dans certains territoires, les politiques sur le système bancaire ouvert exigent une ouverture à la fois de l’accès aux données et des activités d’initiation de paiement. Dans ce document, nous traiterons surtout des considérations canadiennes concernant les politiques qui touchent le partage des données et les renseignements sur les comptes, et moins des activités d’initiation de paiement.

Forces motrices du mouvement du système bancaire ouvert

L'avènement de la quatrième révolution industrielle a été marqué par l'émergence d'entreprises utilisant des données pour créer de la valeur. L'importance croissante des données a renforcé la valeur que les clients, les entreprises et les gouvernements accordent aux données, ce qui a entraîné une réflexion approfondie afin de déterminer qui a ultimement le droit de les contrôler. Par conséquent, nombre d'intervenants croient maintenant que les consommateurs ont le droit de contrôler leurs données personnelles détenues par diverses organisations et ont ainsi le droit d'en avoir le contrôle – ce qui inclut la possibilité de les partager avec les tiers de leur choix. Cette philosophie est profondément ancrée dans l'effort de modernisation des lois sur la protection des renseignements personnels, comme le Règlement général sur la protection des données (RGPD) dans l'Union européenne, et dans les changements proposés à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) par la Chambre des communes du Canada.

Il ne tient pas du hasard qu'au cours des deux dernières décennies, divers modèles de partage des données ont émergé dans le secteur des services financiers, où l'on génère et l'on traite une vaste quantité de données personnelles, afin de répondre à la demande croissante des consommateurs pour le partage des données. Cependant, bon nombre de ces pratiques présentent des lacunes intrinsèques en raison de compromis faits à la sécurité, à l'interopérabilité et à l'accessibilité. Au cours des dernières années, certaines régions ont travaillé à la création d'une approche harmonisée afin de permettre le partage des données tout en tentant de surmonter ces difficultés, ce qui a entraîné la mise en place de mesures réglementaires et des collaborations sectorielles dans divers territoires à l'échelle mondiale – des travaux dont le Canada peut apprendre.

Ce document vise à discuter des principaux choix qui définissent un cadre de système bancaire ouvert et de leurs répercussions, indépendamment du fait que le cadre soit issu d'une politique ou établi par les acteurs du marché.

Méthodes actuelles de partage des données dans les services financiers

Aujourd'hui, divers mécanismes sont utilisés pour faciliter le partage des données financières des clients, comme le téléchargement de fichiers CSV, le processus d'extraction, de transformation et de chargement (ou « grattage d'écran »), et les partenariats de partage des données bilatéral. Pour élaborer un cadre de système bancaire ouvert efficace, il est donc important de comprendre ce mouvement comme l'évolution de ces modèles de partage des données.

Créer un cadre pour régir un système bancaire ouvert au Canada | Introduction

CSV

Dès l'apparition des services bancaires en ligne, la plupart des institutions financières ont offert aux consommateurs la possibilité de télécharger les données sur leurs opérations par l'intermédiaire de portails en ligne dans un format de fichier CSV couramment analysable et pouvant être partagé avec d'autres fournisseurs. Cependant, cette méthode présente sa part de problèmes, notamment pour les raisons suivantes : elle est souvent compliquée pour les clients, elle n'est pas idéale pour le partage répété de données, elle n'est pas uniforme d'une institution à une autre et elle se limite souvent aux données sur les opérations. Mais surtout, cette méthode de partage des données comporte des mesures de sécurité insuffisantes pour protéger les données, entraînant des possibilités de manipulation de données.

Extraction, transformation et chargement (ETL)

Souvent appelées « grattage d'écran », les pratiques ETL ont d'abord été créées pour contourner les difficultés que présente le partage des fichiers CSV pour les consommateurs. Les fournisseurs de processus d'extraction, de transfert et de chargement permettent à un tiers approuvé par le client d'utiliser les identifiants de connexion aux services bancaires en ligne de ce dernier pour ouvrir une session dans le portail de l'institution financière et de « gratter », c'est-à-dire extraire, les données du portail. Ces fournisseurs effectuent ensuite le rapprochement, l'enrichissement et la transformation des données extraites, puis chargent cette information reformatée dans la base de données du tiers.

Dans de nombreux marchés financiers, particulièrement aux États-Unis, l'accroissement des pratiques ETL a suscité l'émergence de nombreux cas d'utilisation de partage des données novateurs – de l'évolution de gestionnaires financiers personnels aux tableaux de bord de comptabilité enrichis pour les petites entreprises. Bien que cette méthode simplifie la vie des consommateurs, elle génère de nouvelles préoccupations sur le plan de la sécurité, notamment en ce qui concerne le stockage des identifiants de connexion aux comptes bancaires en ligne des clients, les possibilités limitées de se conformer aux exigences de consentement éclairé, les responsabilités mal définies et le stockage des données recueillies par les fournisseurs de processus d'extraction, de transfert et de chargement. En raison de ces risques, de nombreuses institutions financières ont mis en place des mesures temporaires pour bloquer l'accès ETL, ce qui cause des problèmes de disponibilité des données et des coûts accrus pour maintenir la connectivité. En fait, ces risques sont si élevés que certains marchés présentant un système bancaire ouvert bannissent les pratiques ETL – mais seulement pour les institutions et les types de données assujettis au système bancaire ouvert.

Partage des données bilatéral

Pour améliorer les aspects sécuritaires et opérationnels du grattage d'écran, de nombreuses institutions financières à l'échelle mondiale ont formé des partenariats de partage des données privés, soit directement avec des tiers fournisseurs, soit avec des fournisseurs de processus d'extraction, de transfert et de chargement. Dans la plupart des cas, ces partenariats remplacent la saisie d'identifiants de connexion et l'accès aux plateformes en ligne non sécuritaires par une authentification fondée sur une interface de programmation d'applications (API) et un partage des données soutenu par des modalités de commerce et de responsabilité officielles. Cependant, parce qu'ils sont fondés principalement sur des relations individuelles, ces partenariats de partage des données fermés ne peuvent pas être utilisés à grande échelle et se limitent souvent aux organisations utilisant beaucoup de données, comme les plateformes de comptabilité numériques.

La prochaine phase de partage des données

L'élaboration et l'adoption d'un cadre de système bancaire ouvert harmonisé améliorent le processus de partage des données de nombreuses façons :

- **Interopérabilité augmentée :** en raison de l'adoption généralisée de protocoles de partage des données et de lignes directrices standardisés, le système bancaire ouvert facilite l'accès aux données des clients par les tiers et procure une valeur ajoutée aux consommateurs.
- **Fiabilité et sécurité supérieures :** le système bancaire ouvert constitue une option plus sûre et plus stable que les pratiques de partage des données actuelles.
- **Normes clairement définies sur des questions comme la responsabilité :** le système bancaire ouvert peut accroître la confiance et la participation dans l'écosystème du partage des données – tant auprès des consommateurs (préoccupés par une mauvaise utilisation possible de leurs données) que des institutions financières (soucieuses des risques émergents liés à la responsabilité et à la réputation que posent les tiers).
- **Meilleure accessibilité :** le système bancaire ouvert réduit sensiblement le coût du partage des données entre les sociétés de services financiers par l'établissement d'API ouvertes et le transfert du contrôle des données aux consommateurs.

En vue de la conception d'un cadre régissant un système bancaire ouvert au Canada, il est important de noter que les pratiques de partage des données plus ouvertes et harmonisées s'inscrivent dans un spectre évolutif où elles côtoient d'autres méthodes. Même avec la mise en place du système bancaire ouvert, des méthodes de partage des données alternatives continueront d'exister pour combler diverses lacunes.

Les données ouvertes et l'avenir des services financiers

En offrant un accès plus vaste aux données des clients, le système bancaire ouvert a le potentiel non seulement d'accroître la concurrence et l'innovation dans le secteur des services financiers, mais aussi, combiné à d'autres changements dans le secteur – comme une infrastructure de paiement simplifiée, l'intelligence artificielle (IA) et l'arrivée d'acteurs non traditionnels –, de permettre des changements plus vastes dans l'économie en général.

Voici quelques façons dont le système bancaire ouvert pourrait changer le visage du secteur canadien des services financiers :

Émergence d'interfaces centrales

Aujourd'hui, les fournisseurs de produits financiers ont le contrôle des données financières des clients, en grande partie parce que ces sociétés possèdent les interfaces numériques. Pour les personnes qui font affaire avec plus d'une institution financière, cela est peu pratique, car elles n'ont qu'une vue fragmentée de leur portefeuille financier.

En permettant à des tiers de confiance d'avoir accès aux données financières des clients, le système bancaire ouvert permet à certains acteurs d'agir en tant qu'interface centrale reliant l'information de nombreux concepteurs de produits financiers et connexes. Cette désagrégation de la chaîne de valeur des services financiers pourrait changer la façon dont les Canadiens accèdent à leurs renseignements financiers et les gèrent. Par exemple, sans les frontières séparant aujourd'hui les concepteurs de produits financiers des distributeurs, les outils de gestion des finances personnelles et les plateformes de comptabilité numériques pourraient améliorer la qualité et l'étendue de leurs interfaces.

Prolifération des conseils numériques

À mesure qu'elle évolue, l'interface financière centrale doit offrir aux consommateurs une valeur accrue si elle veut les attirer. L'évolution de l'intelligence machine, la rapidité accrue des véhicules de paiement et un accès plus vaste aux données des clients permettront aux plateformes financières en ligne d'offrir plus qu'un simple affichage d'information regroupée en fournissant des conseils financiers numériques de manière plus active.

Des signes montrent que ce changement s'amorce. De nombreux outils de gestion des finances personnelles numériques sont passés à la gestion de souscriptions et à la comparaison de produits, comme Bean, au Royaume-Uni, et Clarity Money, aux États-Unis. Au fil de l'évolution du système bancaire ouvert, ces services pourraient éventuellement permettre des recommandations de solutions de rechange et une gestion des finances presque entièrement automatisée.

Moins d'obstacles à l'entrée

L'émergence d'interfaces centrales créera des occasions uniques pour les acteurs non traditionnels, incluant les détaillants, les institutions financières internationales, les grandes sociétés technologiques et les entreprises de technologie financière. Sans l'obligation réglementaire d'offrir des comptes de dépôt, ces acteurs pourront participer plus facilement à la chaîne de valeur des services bancaires et possiblement tirer profit de leur nouvelle position dans le marché en devenant des interfaces centrales pour la gamme de produits de tiers. Par conséquent, les organisations qui détiendront des données exclusives protégées – comme les détaillants ayant accès aux données d'opérations ou les grandes sociétés technologiques ayant accès aux données sur les préférences des utilisateurs – pourraient jouir d'un avantage par rapport aux institutions financières traditionnelles. D'autres pourront agir en tant que fournisseurs de produits de placement et de prêt en travaillant avec les interfaces centrales.

Créer un cadre pour régir un système bancaire ouvert au Canada | Introduction

Concurrence accrue sur le plan des produits

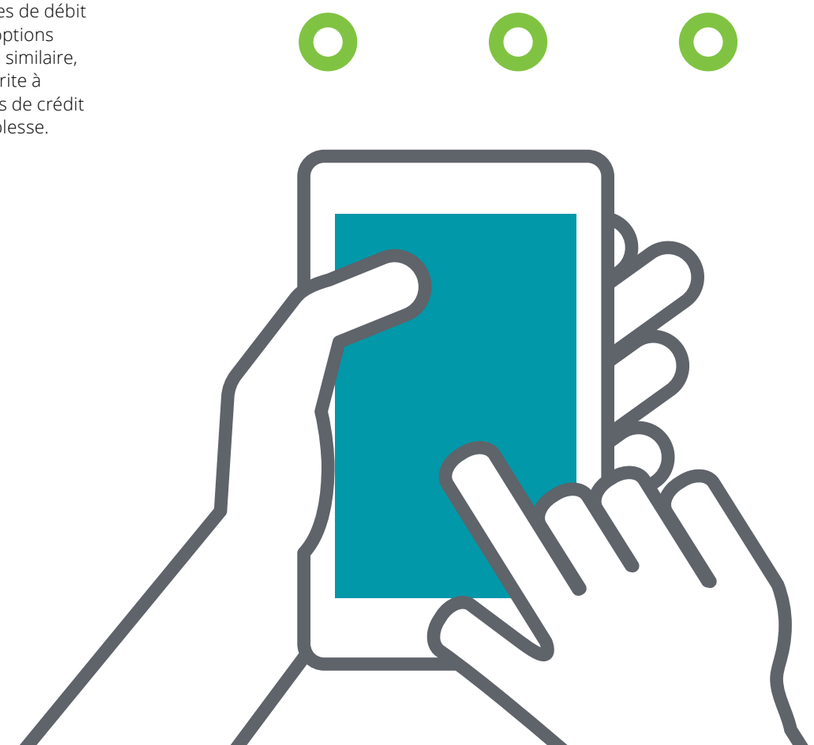
La prolifération des interfaces centrales permettra aux consommateurs d'avoir une meilleure connaissance des autres produits financiers, de les comparer et de passer à d'autres fournisseurs sans mettre fin à la relation principale avec l'interface centrale. Cela permettra également une substitution de produits traditionnels en fonction des besoins, comme le remplacement des dépôts à long terme par des fonds du marché monétaire, par exemple.

Produits complétant d'autres produits

Une visibilité presque en temps réel des opérations financières des consommateurs permettra également l'élaboration de produits novateurs pouvant être acquis en complément de produits actuels. Par exemple, des produits de prêts à tempérament numériques pourraient être souscrits pour compléter des cartes de débit et de crédit existantes en tant qu'options d'emprunt plus durables. De façon similaire, une assurance pourrait être souscrite à l'égard d'achats portés à des cartes de crédit de tiers afin d'obtenir plus de souplesse.

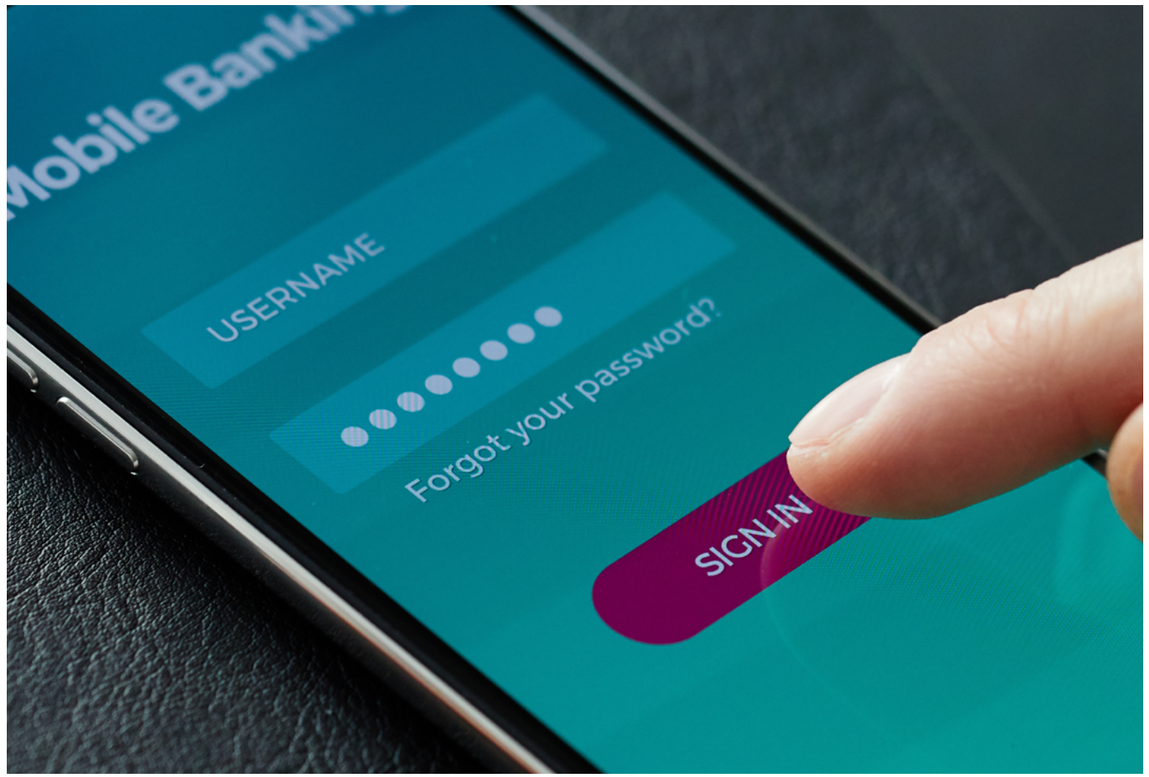
Approbation plus raffinée des prêts

Un accès plus large aux données d'opérations des particuliers permettra aux prêteurs d'acquérir une compréhension plus fine du profil de risque des clients. Les prêteurs pourront ajouter aux dossiers de crédit des données empiriques sur les flux de trésorerie afin de mieux comprendre les particuliers qui ne font pas actuellement affaire avec eux. De plus, les prêteurs pourront évaluer les risques pour chaque transaction en tenant compte du contexte, comme le type d'achat ou le montant total emprunté.



Système bancaire ouvert et risques émergents

Bien que le système bancaire ouvert présente d'innombrables possibilités pour le secteur des services financiers, il est clair que la multiplication des pratiques de partage des données avec les tiers qui s'ensuivra posera également un nouvel éventail de risques pour notre système financier. Pour préserver la sécurité et la solidité de notre écosystème financier, le cadre de système bancaire ouvert devra non seulement déceler activement ces risques émergents, mais aussi prendre les mesures appropriées pour les atténuer.



Créer un cadre pour régir un système bancaire ouvert au Canada | Introduction

Pour ce faire, des questions épineuses devront être posées :

Nouveaux venus sur le marché
Comment leurs activités seront-elles régies afin de s'assurer que des mesures de protection et de contrôle des consommateurs et de l'écosystème sont en place ?

Le système bancaire ouvert permet à des acteurs non traditionnels offrant une gamme restreinte de produits d'entrer dans la chaîne de valeur des services financiers sans devenir des banques ou des institutions financières pleinement autorisées.

Protection des données
Comment assurerons-nous la sécurité des données qui sont partagées entre les acteurs de l'écosystème ?

Comme les données des consommateurs seront réparties parmi un plus grand nombre d'acteurs du secteur (possiblement soumis à différentes normes de sécurité des données), les organisations deviendront plus à risque d'être ciblées par des tiers malveillants et de commettre des erreurs, ce qui augmente la probabilité que des cyberattaques et des fuites de données accidentelles se produisent.

Fraude
Comment nous assurerons-nous que l'écosystème n'est pas exposé à des tiers frauduleux ?

À mesure que le nombre d'interactions augmentera entre les acteurs de l'écosystème dans un cadre ouvert, les possibilités que des tiers frauduleux participent à des activités d'hameçonnage et accèdent à des renseignements permettant d'identifier des personnes risquent d'augmenter.

Protection des renseignements personnels
Quelles améliorations devront être apportées aux mesures de protection des renseignements personnels pour protéger adéquatement les données des consommateurs ?

Afin que le système bancaire ouvert fonctionne efficacement, les clients devront non seulement être éduqués et informés, mais aussi consentir à la façon dont leurs données seront utilisées. Sans mécanisme approprié en place, les renseignements personnels des clients peuvent être utilisés à des fins contraires à leurs intérêts.

Recours
Comment l'écosystème de services bancaires ouvert sera-t-il mis en œuvre pour gérer efficacement les responsabilités tout en réduisant les risques pour les clients ?

Dans un environnement de données réparties, il deviendra plus difficile d'intenter des recours en cas d'infraction, d'événement frauduleux ou d'incident de cybersécurité de toute sorte, ce qui peut représenter une lacune dans le soutien à la clientèle.

Répartition des coûts
Comment le système bancaire ouvert gérera-t-il collectivement les efforts associés au système pour inciter toutes les parties à participer activement ?

L'établissement et l'exploitation d'un mécanisme de partage des données plus sécuritaire coûteront des sommes importantes tant aux institutions financières individuelles qu'au système financier global (jusqu'à 200 millions de dollars pour une banque australienne de premier rang[1]). Si le système bancaire ouvert augmente comme prévu le nombre de pratiques de partage des données utilisées par les consommateurs, le coût du maintien du système augmentera également. Sans une répartition équitable de ces coûts, les avantages du système bancaire ouvert pourraient être annulés par les coûts accrus transférés aux clients.

Un cadre de système bancaire ouvert prudent devra non seulement reconnaître ces risques émergents, mais aussi établir un solide cadre réglementaire à l'appui pour les atténuer – qui inclura, entre autres choses, des cadres robustes de gouvernance financière et des réglementations rigoureuses en matière de confidentialité des renseignements. Cette étape de base est essentielle, parce que sans une gestion attentive des risques potentiels associés au système bancaire ouvert, les avantages nets d'un environnement de données ouvert seront moindres, ce qui diminuera également la participation.

Points à considérer pour un cadre de système bancaire ouvert au Canada

Précédents à l'échelle mondiale

Comme de nombreux territoires dans le monde ont déjà adopté le système bancaire ouvert, le Canada dispose de nombreux exemples dont il peut s'inspirer pour l'établissement de son propre cadre. Cela dit, en raison de la diversité des systèmes bancaires et des situations parmi les pays, il n'existe pas de conception standard; en fait, les cadres établis présentent d'énormes variations sur le plan des politiques et de la conception.

Créer un cadre pour régir un système bancaire ouvert au Canada | Points à considérer pour un cadre de système bancaire ouvert au Canada

Un certain nombre de territoires dans le monde ont commencé à mettre en œuvre des politiques de système bancaire ouvert, qui se trouvent à différents stades de maturité.

Canada
Les organismes de réglementation ont commencé à discuter du système bancaire ouvert dans le cadre du budget fédéral 2018. Un comité consultatif sur le système bancaire ouvert a été établi en septembre 2018, et le processus de consultation a commencé en janvier 2019 avec la publication d'un document de consultation.

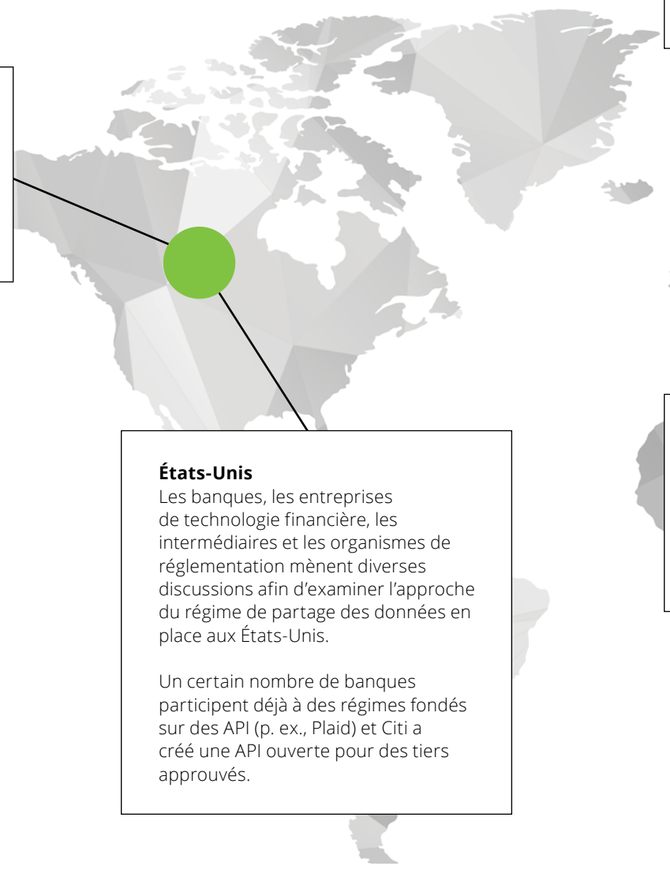
Quatre approches à l'échelle mondiale

Amérique
Attitude de laisser-faire en matière de réglementation; la méthode du grattage d'écran prédomine

Asie
Les États comptent sur les institutions pour favoriser l'innovation liée au système bancaire ouvert; la réglementation est relâchée et les soutient.

Europe
Système bancaire ouvert issu de la législation sur les services de paiement; volonté de légiférer en vue de l'uniformisation.

Australie
Approche fondée sur les règles; le système bancaire n'est qu'un élément d'un important mouvement pour établir une économie fondée sur les données.



États-Unis
Les banques, les entreprises de technologie financière, les intermédiaires et les organismes de réglementation mènent diverses discussions afin d'examiner l'approche du régime de partage des données en place aux États-Unis.

Un certain nombre de banques participent déjà à des régimes fondés sur des API (p. ex., Plaid) et Citi a créé une API ouverte pour des tiers approuvés.

Royaume-Uni : CMA
L'Autorité de la concurrence et des marchés (CMA) du R.-U. exige de neuf banques choisies qu'elles partagent les données bancaires et d'initiation de paiement selon les normes concernant les API ouvertes.
En vigueur en janvier 2018

Union européene : DSP2
Cette directive exige des banques qu'elles partagent les données bancaires et d'initiation de paiement, mais n'impose rien sur le plan technologique.
En vigueur en janvier 2019

Japon : API ouvertes
Les banques du Japon étaient tenues d'indiquer leur appui au régime des API ouvertes avant mars 2018 pour un déploiement d'ici 2020. Les tiers fournisseurs de services sont tenus de s'enregistrer et d'établir des ententes avec les banques.

Hong Kong : API ouvertes
L'autorité monétaire de Hong Kong a publié en janvier 2018 un document de consultation présentant l'approche envisagée à l'égard des API ouvertes dans le cadre de la nouvelle ère des services bancaires intelligents.

Singapour : API ouvertes
Dans un effort de création d'une « nation intelligente », la Monetary Authority of Singapore (MAS) et l'Association des banques de Singapour (ABS) ont publié un guide sur les API ouvertes pour inciter les institutions financières à élaborer et à partager ouvertement leurs API ouvertes.

Australie : Droit aux données des consommateurs
Une nouvelle législation annoncée en novembre 2017 accordera aux consommateurs un accès ouvert à leurs données des services bancaires, énergétiques, téléphoniques et internet. Le secteur bancaire sera le premier à être soumis à cette nouvelle législation.
En vigueur en 2019

Royaume-Uni

Au Royaume-Uni (R.-U.), la réglementation concernant le système bancaire ouvert a été motivée par l'objectif politique de réduire le pouvoir de marché des grandes banques en augmentant l'éventail de fournisseurs de services dans le marché. Dans une enquête portant sur le marché des services bancaires de détail réalisée en 2016, l'Autorité de la concurrence et des marchés (Competition and Markets Authority – CMA) du R.-U. a conclu que les banques plus anciennes et de plus grande envergure n'avaient pas besoin d'offrir des services très concurrentiels pour acquérir des clients, alors que les banques récentes et de taille plus modeste avaient du mal à croître. Cela signifie qu'un grand nombre de personnes paient plus qu'elles ne le devraient, et qu'elles ne bénéficient pas de nouveaux services[2]. Par conséquent, le cadre bancaire ouvert du R.-U. porte uniquement sur les neuf banques les plus importantes, sans exiger de réciprocité.

Australie

En Australie, la réglementation sur le système bancaire ouvert a été adoptée pour répondre à la critique grandissante du public à l'égard des grandes banques, et vise à donner aux consommateurs le droit de contrôle de leurs données et les avantages qui en découlent. L'examen effectué par le gouvernement a révélé que le système bancaire ouvert était un outil utile pour donner aux consommateurs un meilleur accès à leurs données financières et réduire le temps, le coût et les inconvénients associés à la recherche et au choix de produits et de services financiers. Lorsque les consommateurs font de meilleurs choix quant aux moments où ils consomment et aux produits qu'ils achètent, ils incitent le secteur concerné à devenir plus efficace et plus concurrentiel[3]. Ce mouvement dépasse les services financiers et s'inscrit dans une volonté plus large du pays, fondée sur les droits relatifs aux données personnelles, de créer une économie de données ouverte. Avec le temps, on s'attend à ce que ce régime de données ouvert, comme le système bancaire ouvert, inclue ultérieurement les autres secteurs, à commencer par ceux des télécommunications et des services publics. En raison de cette vision, la politique sur le système bancaire ouvert de l'Australie est large et englobante, exige la participation de toutes les institutions acceptant des dépôts – non seulement des banques – et couvre les canaux tant numériques que physiques.

Japon

Au Japon, le mouvement du système bancaire ouvert est fondé sur l'objectif de promouvoir l'innovation et la modernisation du secteur bancaire dans le cadre de la stratégie de croissance de 2017 du gouvernement japonais[4]. Au Japon, les principaux intervenants des autorités réglementaires et gouvernementales ont la perception que leur secteur des services financiers accuse un retard par rapport à celui d'autres territoires, ce qui le rend plus susceptible de subir les effets de potentiels chocs exogènes et nuit à sa compétitivité à l'échelle mondiale. De plus, le recours massif aux paiements en espèces et des pratiques réglementaires historiquement strictes (restreignant la capacité des banques à détenir des participations importantes dans les entreprises de technologie financière, par exemple) ont étouffé la capacité d'innovation du secteur. Le système bancaire ouvert et la modernisation de la réglementation qui y sera associée (incluant un relâchement des restrictions concernant les investissements dans les entreprises de technologie financière) sont perçus comme des moyens clés pour augmenter la croissance, favoriser la compétitivité et promouvoir l'innovation.

Union européenne

En Union européenne (UE), la politique sur le système bancaire ouvert a pour objectifs de mieux harmoniser le secteur des paiements, qui est fragmenté, de moderniser le secteur financier et d'offrir aux consommateurs des alternatives aux grandes banques, qui ont été touchées par une défaillance systémique. L'UE a décidé d'adopter une approche de réglementation fondée sur les activités (en réglementant l'ensemble des services de paiement plutôt que des types particuliers d'institutions financières) et a accordé une attention particulière à l'application de normes techniques uniformes, notamment celles qui portent sur l'amélioration de la sécurité (p. ex., l'authentification et la communication). Cette attention portée à la réglementation des activités et à la promotion d'une normalisation technique est probablement due à la structure de marché unique de l'UE, où des milliers de fournisseurs de paiement de tailles et de niveaux de sophistication divers sont répartis entre 28 États membres, chacun ayant son propre contexte réglementaire et de marché. La principale mesure législative sur laquelle est fondée l'initiative de système bancaire ouvert – la Directive sur les services de paiement 2, ou DSP 2 – étend la portée de la législation précédente pour couvrir un plus large éventail d'opérations, assurer une application uniforme entre les États membres, et fournir un accès aux données de paiement des clients à des tiers. Cette directive étend également la gamme des fournisseurs de services de paiement admissibles (encourageant ainsi l'innovation) en facilitant l'entrée dans le marché pour les nouveaux fournisseurs, tout en assurant la protection des consommateurs par la voie de normes améliorées.

États-Unis

Aux États-Unis (É.-U.), l'établissement d'une réglementation régissant le système bancaire ouvert ne semble pas imminent; toutefois, divers acteurs du marché – incluant des organismes de réglementation, des associations commerciales, des institutions financières et des services de regroupement des données – publient des normes et des perspectives sur un modèle de partage des données potentiel dans le secteur. Par exemple, le Consumer Financial Protection Bureau (CFPB), un organisme de protection des consommateurs dans le secteur financier, a publié un ensemble de principes non contraignants axés sur le partage et le regroupement des données financières, alors que la National Automated Clearing House Association (NACHA), une association du secteur financier, a réuni un groupe sectoriel de normalisation des API dans le but d'élaborer des normes uniformes pour les API dans le secteur des services financiers. Un certain nombre d'entreprises de technologie financière importantes (incluant Betterment et Kabbage) ont également uni leurs forces pour créer un groupe de lobbyisme, le groupe Consumer Financial Data Rights, afin de promouvoir le partage des données financières des consommateurs avec des tiers.

Singapour

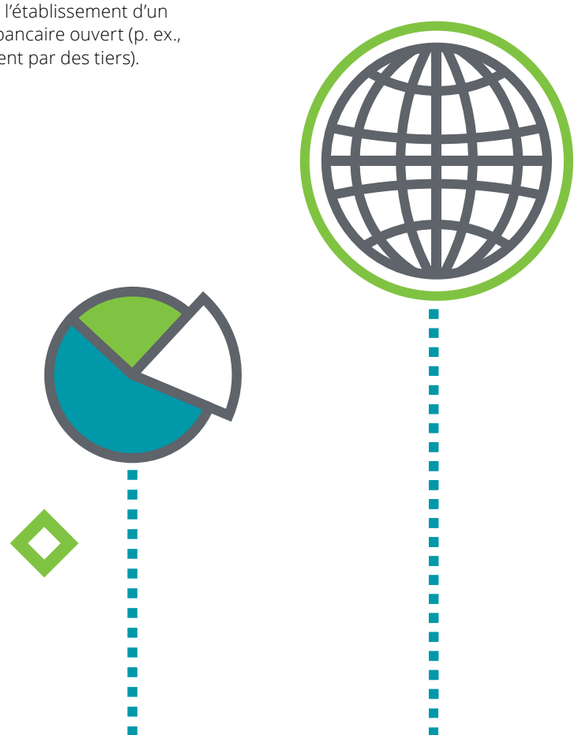
La Monetary Authority of Singapore (MAS), qui est la banque centrale de la Cité-État et défend de manière très progressiste l'innovation dans les services financiers, a établi un robuste environnement de système bancaire ouvert sans élaborer de législation contraignante pour régir l'accès aux données par des tiers. Cela s'explique en partie par la situation unique du marché de Singapour. La forte concurrence qui règne dans le secteur bancaire a poussé les plus grandes institutions financières du pays, dont DBS et OCBC Bank, à entreprendre une démarche proactive visant à être parmi les premières à utiliser la technologie d'API ouvertes. En effet, elles sont aujourd'hui des leaders à l'échelle mondiale dans le domaine du partage des données. DBS, par exemple, permet aux développeurs d'accéder à plus de 200 API, couvrant des produits et des services allant des cartes de paiement aux primes, en passant par les prêts. La MAS entretient également une forte relation et une grande collaboration avec les banques de Singapour, ce qui réduit la nécessité d'une législation normative pour atteindre certains résultats dans le marché. Pour illustrer cette collaboration et le point de vue progressiste de la banque centrale à l'égard du secteur bancaire, mentionnons la création de l'API Playbook. Ce guide contient plus de 400 API recommandées pour le développement dans les services bancaires, dont les applications dépassent largement le système bancaire ouvert (c.-à-d. l'ouverture des données aux tiers) et couvrent tous les aspects de la chaîne de valeur des services bancaires, de la première ligne aux services d'arrière-plan.

Créer un cadre pour régir un système bancaire ouvert au Canada | Points à considérer pour un cadre de système bancaire ouvert au Canada

Le contexte canadien

Un cadre régissant un système bancaire ouvert au Canada devrait résolument être conçu en fonction des caractéristiques uniques du pays, notamment les suivantes :

- Un système de services financiers solide qui n'a pas connu de défaillance systémique ou qui ne dépend pas de fonds publics.
- Un régime réglementaire double où les organismes fédéraux et provinciaux gouvernent différentes entités, avec un nombre gérable d'institutions. Cela ajoute de la complexité à l'élaboration d'approches normalisées et à la gestion des acteurs du système bancaire ouvert (si l'on compare avec les territoires qui peuvent exercer une surveillance centrale).
- Gouvernance insuffisante des entités non traditionnelles qui ne correspondent pas aux définitions actuelles d'« institutions financières », ce qui peut poser de nouvelles sources de risques sans que les consommateurs ne soient protégés, ou exposer l'écosystème des services financiers aux institutions étrangères.
- Efforts continus pour renforcer la législation canadienne sur la protection des renseignements personnels par la voie d'amendements proposés à la LPRPDE, qui pourraient servir de garde-fous dans un cadre de système bancaire ouvert en ce qui a trait à l'utilisation autorisée, à la gestion des données et aux exigences de divulgation.
- Efforts de modernisation des paiements continus dans le but d'améliorer l'infrastructure canadienne de paiement, ce qui peut faciliter l'établissement d'un cadre de système bancaire ouvert (p. ex., initiation de paiement par des tiers).



Créer un cadre pour régir un système bancaire ouvert au Canada | Points à considérer pour un cadre de système bancaire ouvert au Canada

En raison de cette situation unique, un cadre régissant un système bancaire ouvert au Canada devrait :

Être axé sur la création de valeur pour les Canadiens
Le système bancaire ouvert offre l'occasion d'établir un cadre de gouvernance pour les fournisseurs de services financiers non traditionnels (avec d'autres initiatives concomitantes au Canada) et de stimuler l'innovation.

Accroître la transparence et le contrôle des données des consommateurs
Le système bancaire ouvert devrait être un mouvement global indépendant du secteur dont la priorité serait de redonner le contrôle des données aux consommateurs.

Atténuer les risques liés au partage des données
Les méthodes actuelles de partage des données financières menacent la sécurité et la stabilité du système des services financiers en demandant aux consommateurs de partager leurs identifiants de connexion bancaires avec des tiers.

Préserver la stabilité de notre système de services financiers.
Punir des institutions en particulier ne devrait pas être le principal objectif du système bancaire ouvert.

Ces objectifs particuliers indiquent que la conception d'un cadre de système bancaire ouvert au Canada devrait différer des approches adoptées dans les autres territoires. Bien que certains éléments puissent convenir au Canada, celui-ci devrait s'efforcer d'élaborer une infrastructure de système bancaire ouvert à partir de zéro, et en fonction de la situation qui lui est propre.

Principes de conception d'un cadre de système bancaire ouvert

Dans son budget de 2018, le gouvernement du Canada a indiqué qu'il examinerait les avantages du système bancaire ouvert pour évaluer s'il pourrait entraîner des retombées positives pour les Canadiens. Mais quels genres de retombées ? La réponse à cette question comporte deux volets.

D'abord, un cadre de système bancaire ouvert bien conçu devrait soutenir l'évolution continue de l'innovation dans l'écosystème des services financiers. Ensuite, un système bancaire ouvert devrait continuer de protéger, de maintenir et de renforcer la sécurité et la solidité réputées du système financier canadien.

Pour générer de tels résultats, le Canada doit concevoir son système bancaire ouvert en suivant certains principes directeurs essentiels :

1. Valeur :

Procurer une valeur réelle aux Canadiens sans imposer un fardeau excessif aux acteurs du marché (p. ex., coûts, risques).

2. Transparence :

S'assurer que les consommateurs sont parfaitement au fait de leurs droits et de leurs responsabilités en ce qui concerne le transfert, la possession et l'utilisation de leurs données.

3. Sécurité :

Établir un équilibre entre la commodité pour les consommateurs et la sécurité.

4. Adoption :

Établir un équilibre entre le coût net pour l'économie, la participation, et la rapidité de mise en marché et l'étendue des produits et/ou des données.

Bien que de nombreux facteurs doivent être pris en considération pour la mise en place d'un cadre de système bancaire ouvert au Canada, ces quatre principes directeurs devraient être à la base de toutes les décisions.

Un cadre de système bancaire ouvert pour le Canada

Aperçu du cadre

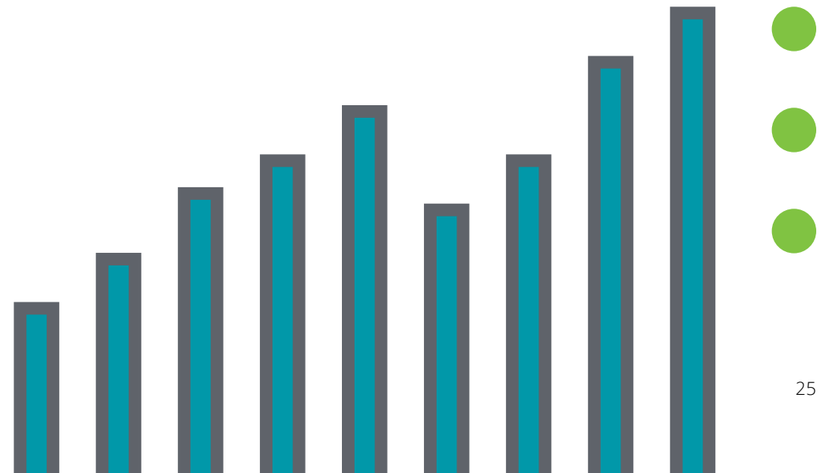
Afin d'établir un cadre efficace pour régir un système bancaire ouvert au Canada, les parties prenantes doivent prendre en considération les choix qui ont été faits dans les autres territoires, examiner les résultats obtenus et évaluer leur pertinence pour le contexte unique du Canada.

Les champs de décision pour la conception du système bancaire ouvert peuvent être divisés en trois grandes catégories :

1. Étendue du système bancaire ouvert

2. Normes

3. Modèle commercial et modèle de responsabilité



1. Étendue du système bancaire ouvert

Les choix faits dans d'autres territoires concernant l'étendue du système bancaire ouvert peuvent aider à définir les types de comptes et les types d'entités à partir desquels le système établira l'accès aux données, de quelle façon cet accès peut changer au fil du temps et les méthodes qui pourront être utilisées pour accéder à ces données.

En vue de l'élaboration d'un cadre pour un système bancaire ouvert, le Canada devrait répondre aux questions suivantes :

- Quels produits devraient être couverts ?
- Les comptes hors ligne devraient-ils être couverts ?
- Quels types d'utilisateurs devraient être couverts ?
- Quels types de données devraient être inclus ?
- Pendant combien de temps les données devraient-elles être disponibles ?
- Qui devrait ouvrir l'accès à ses données ?
- Comment le déploiement devrait-il être exécuté ?
- Quels types de destinataires de données seront autorisés ?
- Quels droits d'accès devrait-on accorder aux destinataires de données ?

Créer un cadre pour régir un système bancaire ouvert au Canada | Un cadre de système bancaire ouvert pour le Canada

Quels produits devraient être couverts ?

Choix faits dans d'autres territoires :

L'une des premières étapes de l'établissement d'un cadre de système bancaire ouvert consiste à déterminer les types de produits financiers qu'il doit inclure. À ce jour, la plupart des systèmes bancaires ouverts sont axés sur trois principaux domaines :

1. Comptes d'opérations
- Exemples : débit, crédit, épargne
- Répercussions du système bancaire ouvert : permet plus de cas d'utilisation pour la gestion des finances personnelles et l'approbation

2. Produits d'épargne/de prêt
- Exemples : CPG, CELI, prêts hypothécaires, marges de crédit
- Répercussions du système bancaire ouvert : permet des cas d'utilisation facilitant le changement et la comparaison de produits

3. Éventail de produits financiers
- Exemples : produits de gestion de patrimoine et d'assurance
- Répercussions du système bancaire ouvert : permet plus de cas d'utilisation de gestion financière intégrée

---

Idéalement, un système bancaire ouvert offre la possibilité d'augmenter la gamme de produits offerts sur le marché et de générer un plus vaste éventail de cas d'utilisation. Cela dit, atteindre cet objectif présente des défis, et avant de décider quels produits inclure dans son cadre, le Canada devra mener une évaluation attentive de cet aspect.

Par exemple, certains produits financiers – comme les produits de gestion de patrimoine et d'assurance – entraîneront inévitablement un fardeau supplémentaire pour les générateurs de données qui cherchent à rendre les données accessibles à des tiers. Contrairement aux comptes d'opération, qui sont mis à jour de façon continue, ces produits peuvent ne pas être entièrement numérisés ou peuvent nécessiter de nouvelles formes d'accès en ligne. Cela pourrait entraîner une restructuration longue et coûteuse du système.

Un cadre de système bancaire ouvert doit également avoir une portée bien définie. Cela signifie que les parties prenantes devront décider de réguler les fonctions au moyen d'une approche fondée sur les produits (définissant les types de comptes précis inclus ou non dans le système) ou d'une approche fondée sur les activités (définissant les actions précises visées par le système). Une approche fondée sur les activités a l'avantage d'exiger une participation plus équitable des institutions, mais si les organismes de réglementation veulent éviter toute confusion à propos des institutions qui sont admissibles, les critères doivent être clairement définis.

Parmi les territoires qui ont déjà adopté un système bancaire ouvert, le R.-U. et l'Australie ont retenu une approche fondée sur les comptes, alors que l'UE définit l'étendue du système sur la base des activités (p. ex., tous les comptes de paiement en ligne). Comme celle du R.-U. et de l'Australie, la définition de l'UE inclut des comptes-chèques, des cartes de crédit, etc., mais peut également viser d'autres comptes comparables comme des portefeuilles électroniques (p. ex., PayPal).

Les comptes hors ligne devraient-ils être couverts ?

Choix faits dans d'autres territoires :

Le cadre de système bancaire ouvert canadien devrait-il inclure seulement les produits financiers en ligne, ou viser également les comptes hors ligne ? Pour répondre à cette question, nous devons examiner deux facteurs clés :

1. Étendue sur le plan des clients :
En 2016, 90 % des Canadiens bénéficiaient d'un accès régulier à Internet, et 80 % utilisaient une forme ou une autre de services bancaires en ligne – des chiffres qui devraient augmenter au fil du temps . Comme les services du système bancaire ouvert seront probablement fournis par des moyens numériques, cela signifie que la majorité des Canadiens y aura accès, mais pas la totalité. En ignorant les consommateurs qui n'ont pas accès à des services bancaires en ligne, le système bancaire ouvert exclurait inévitablement les personnes les plus vulnérables de la société, notamment les personnes âgées et à faible revenu.

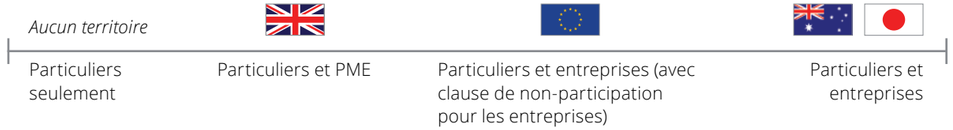
2. Étendue sur le plan des travaux :
afin d'inclure les produits hors ligne dans le système bancaire ouvert, les institutions devraient s'assurer que les données actuelles deviennent accessibles de façon numérique – un effort qui exigerait non seulement l'établissement de processus numériques, mais aussi l'intégration des clients dans une plateforme en ligne afin de simplifier l'authentification. Bien que cela permette de s'assurer que tous les Canadiens ont accès au système bancaire ouvert, cela augmenterait inévitablement le coût et la complexité de la mise en œuvre, ce qui allongerait le délai de lancement.

Pour déterminer s'il serait justifié d'augmenter de la sorte la complexité et les coûts du processus pour les institutions financières, il sera crucial de mieux comprendre combien de Canadiens seraient involontairement exclus d'un système bancaire ouvert qui ne viserait pas les données non numériques, et de mieux connaître les besoins particuliers de ces Canadiens.

Créer un cadre pour régir un système bancaire ouvert au Canada | Un cadre de système bancaire ouvert pour le Canada

Quels types d'utilisateurs devraient être couverts : particuliers ou entreprises ?

Choix faits dans d'autres territoires :



Chaque type d'utilisateur exigera de faire un compromis entre le coût et la complexité de la mise en œuvre, et la valeur pour les consommateurs. À l'heure actuelle, différents utilisateurs reçoivent différents niveaux de services : les titulaires de comptes de détail (c.-à-d., comptes personnels) obtiennent en grande partie des produits et des services traditionnels, alors que les titulaires de comptes pour grandes entreprises profitent déjà de certains des avantages que les nouvelles solutions offriraient dans le cadre d'un système bancaire ouvert (p. ex., gestion de la trésorerie et conseils personnalisés). D'autre part, les clients utilisant des comptes bancaires pour petites et moyennes entreprises (PME) obtiennent une combinaison de produits traditionnels et des services facilement personnalisables, ce qui correspond à leur situation, à mi-chemin entre les particuliers et les grandes entreprises.

Les différents comptes d'utilisateurs présentent également différents niveaux d'accès numérique et d'intégration (intégrations exécutées par des API ou sur mesure). À l'échelle mondiale, les comptes personnels ont été massivement numérisés, et les clients peuvent habituellement visualiser la majeure partie ou la totalité des comptes et des produits qu'ils détiennent auprès d'une institution par la voie d'un portail Internet ou mobile unique, ce qui permet d'ouvrir l'accès à ces données de façon relativement simple en utilisant les API. Cependant, dans le cas des comptes d'entreprise, la mesure dans laquelle les banques ont établi des points d'accès uniques aux produits et aux fonds des entreprises est très variable. En raison de cette situation, appliquer le système bancaire ouvert à l'éventail des comptes d'une société peut poser des défis technologiques et réglementaires.

D'un point de vue mondial, la vaste majorité des initiatives de système bancaire ouvert et des réglementations en cette matière se sont concentrées sur des cas d'utilisation concernant les comptes de particuliers et les comptes de PME. Cela s'explique principalement par le fait que la mise en œuvre technique pour ces utilisateurs est souvent plus facile, et que la démocratisation des données des particuliers cadre davantage avec les catalyseurs du système bancaire ouvert dans la plupart des pays. Toutefois, l'Australie a inclus dans son cadre une disposition permettant d'inclure tous les types de comptes – incluant les comptes d'entreprise –, bien que certains détails doivent être peaufinés par la Competition and Consumer Commission (ACCC) de l'Australie.

Quels types de données devraient être inclus ?

Choix faits dans d'autres territoires :

Données publiques

Données générées par les clients

Données sur les soldes

Choix faits dans d'autres territoires :

Données d'opérations

Données de vérification de l'identité

Données regroupées

L'examen des cadres de l'ensemble des territoires sur le plan des données couvertes a permis de cerner certains types de données :

- **Données publiques :** l'information qui est déjà accessible en ligne et peut être librement utilisée, réutilisée et redistribuée par n'importe quelle entité (p. ex., évaluations des consommateurs et renseignements sur les produits accessibles au public). Au Canada, la majeure partie de ces renseignements est déjà accessible par la voie d'autres écosystèmes de partage des données (p. ex., les API de Google, de Yelp et de Foursquare).
- **Données générées par les clients :** renseignements personnels et financiers fournis directement par le client à une entité de services financiers (p. ex., adresse personnelle et coordonnées).
- **Données sur les soldes :** information concernant le montant d'argent présent dans un compte de dépôt détenu par le client à un moment donné (p. ex., solde d'un compte de portefeuille électronique).
- **Données d'opérations :** information générée lorsqu'une opération est effectuée dans le compte d'un client (p. ex., retraits, virements et dépôts). Avec les données des clients et les données sur les soldes, les données d'opérations permettent la majorité des cas d'utilisation d'un système bancaire ouvert.
- **Résultats de vérification d'identification :** confirmation de l'identité d'un client par l'intermédiaire d'un processus de validation au moyen de renseignements personnels et financiers (p. ex., résultats d'une vérification par rapport aux renseignements sur le client). Au Canada, d'autres solutions d'identité numérique sont actuellement en cours d'élaboration (p. ex., Verified.me).
- **Données regroupées :** compilation de renseignements sur de nombreux clients qui doivent être anonymisés et/ou résumés (p. ex., soldes moyens de comptes liés à une tranche d'âge ou à un code postal). De tels renseignements permettraient de nouveaux cas d'utilisation (p. ex., comparaison avec des personnes appartenant au même groupe), mais exigeraient beaucoup plus d'efforts de la part des générateurs de données.

Du point de vue du partage des données, les données générées par les clients, les données sur les soldes et les données d'opérations correspondent aux données des clients.

L'inclusion des données publiques, des résultats de vérification d'identité et des données regroupées favoriserait la concurrence dans le marché, mais la complexité supplémentaire et les obligations potentielles associées au partage de ces données, et le fait de devoir protéger l'information sur les concurrents qui pourrait être tirée de ces données, devraient être examinés avec soin.

Il est également important de noter que les cadres de système bancaire ouvert adoptés par les autres territoires permettent aux institutions d'établir des ententes commerciales privées pour exclure certaines données des politiques régissant les données accessibles aux tiers.

Créer un cadre pour régir un système bancaire ouvert au Canada | Un cadre de système bancaire ouvert pour le Canada

Combien de temps les données devraient-elles être disponibles ?

Choix faits dans d'autres territoires :

Aucune exigence liée aux données historiques

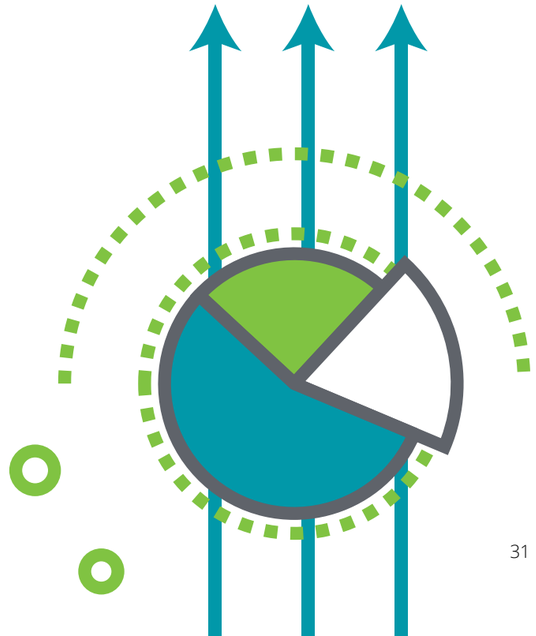
Période flottante établie pour les données historiques

Date de démarrage établie

** Remarque : Peut varier selon le type de données.*

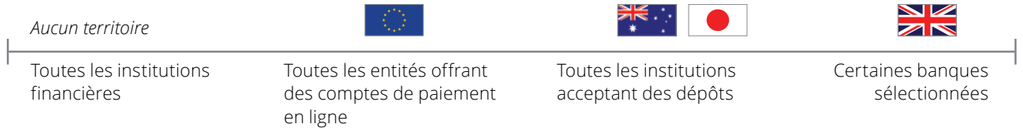
Différents territoires ont adopté différentes approches concernant les exigences imposées aux générateurs de données à l'égard des données historiques. L'une de ces approches consiste à imposer une date de démarrage (c.-à-d., la date à partir de laquelle les données doivent être accessibles au lancement public du cadre de fonctionnement du système bancaire ouvert), alors qu'une autre comporte une exigence de roulement (c.-à-d. la quantité de données historiques – en mois ou en années – qui doivent être fournies à partir de la date de la demande de données). Certains territoires, comme le R.-U., ont également fait des choix concernant le type de données (p. ex., les données regroupées doivent être partagées en fonction d'une période de 25 mois glissants, alors que les données d'opérations sont soumises à une exigence liée à une date de démarrage).

Pour établir ses propres règles concernant ces aspects, le Canada doit évaluer le compromis à faire entre la valeur offerte aux Canadiens et le fardeau imposé aux générateurs de données. Par exemple, bien que des données historiques échelonnées sur une plus grande période puissent permettre de dégager des tendances pour donner aux clients de précieux conseils relativement aux dépenses et à l'épargne, il est possible que de nombreuses institutions disposent d'une quantité limitée de données disponibles dans leurs ensembles de données numériques existants.



Qui devrait ouvrir l'accès à ses données ?

Choix faits dans d'autres territoires :



L'exigence liée à l'ouverture de l'accès aux données peut être établie en fonction de l'institution (p. ex., institutions financières faisant partie d'une certaine catégorie, comme les banques de l'annexe I et les banques de l'annexe II) ou en fonction de l'activité (p. ex., toutes les institutions offrant aux Canadiens les fonctions mentionnées à la page 27).

Une approche fondée sur les activités permet de s'assurer que le cadre est suffisamment flexible pour s'adapter à de nouveaux types d'institutions non traditionnelles pouvant émerger au fil du temps, et peut favoriser des conditions plus homogènes où tous les acteurs offrant des produits et des services sont tenus de rendre les données accessibles, peu importe leur catégorie juridique. Cependant, cela crée un environnement de gouvernance plus vague, car la ligne séparant les institutions visées par le cadre et les autres s'estompe (p. ex., le portefeuille numérique de PayPal peut-il être considéré comme un compte de dépôt ?). De plus, les systèmes actuels de réglementation financière au Canada sont basés sur les institutions, ce qui signifie que des exigences établies en fonction des activités nécessiteraient de modifier la portée des organismes de réglementation actuels ou de créer un nouvel organisme de réglementation.

Il est également important de déterminer si le cadre de fonctionnement du système bancaire ouvert agira comme un cadre autonome au sein des services financiers ou fera partie d'un cadre général de données ouvertes couvrant tous les secteurs. Si la dernière option est privilégiée, le concept de réciprocité des données pourrait être utilisé pour permettre à d'autres organisations de participer au système de données ouvertes.

L'Australie explore activement le concept de réciprocité, où les destinataires de données détenant des données équivalentes aux données financières échangées avec eux par les « détenteurs de données » (ce terme est toujours en cours de définition par la Competition and Consumer Commission de l'Australie) seraient tenus de les partager avec les détenteurs de données à la demande d'un client. Notons que la réciprocité est examinée dans le but d'améliorer l'*accessibilité des données* (et non strictement pour augmenter l'*accès aux données*) et est basée sur le principe du consentement explicite du client. En vertu d'un cadre de réciprocité proposé, les détenteurs de données ne seraient pas autorisés à demander unilatéralement des données aux destinataires de données; ils pourraient uniquement le faire dans les situations où les clients auraient demandé aux destinataires de données de partager leurs données équivalentes.

Créer un cadre pour régir un système bancaire ouvert au Canada | Un cadre de système bancaire ouvert pour le Canada

Comment le déploiement devrait-il être exécuté ?

Choix faits dans d'autres territoires :

Au-delà de la couverture des comptes, les différents territoires ont également utilisé diverses façons de mettre en œuvre leurs réglementations de système bancaire ouvert. Pour déterminer quelle approche conviendrait le mieux au Canada, les parties prenantes doivent se poser deux questions clés :

1. **De combien de temps disposeront les générateurs de données pour se conformer aux normes techniques sur lesquelles est fondé le système bancaire ouvert ?**

Les organismes de réglementation doivent trouver le juste milieu entre la volonté de lancer rapidement le système bancaire ouvert et la nécessité d'accorder suffisamment de temps aux institutions pour se conformer et éviter de mettre en péril la sécurité des données des utilisateurs.

Les organismes de réglementation doivent également être conscients que, dans les marchés où une forme de système bancaire ouvert a déjà été déployée, des risques de conformité inégaux ou non favorables aux besoins des consommateurs exposent ces derniers à des solutions qui ne sont pas optimales, ce qui peut faire fuir des clients qui, dans d'autres circonstances, auraient pu être les premiers adeptes du système.

2. **Au déploiement, devrait-on établir des échéanciers différents selon le type d'entité ?**

Notons que plusieurs territoires (comme le R.-U. et l'Australie) ont consciemment décidé d'imposer le système bancaire ouvert aux banques déjà en place avant de l'étendre aux autres types d'institutions financières, effectuant un déploiement par étape. Une telle approche permet notamment au cadre d'évoluer de façon sécuritaire – sans exposer l'écosystème des services financiers au risque inutile que posent les institutions financières de plus petite envergure, aux ressources informatiques plus limitées – en plus de permettre à la fonction punitive du cadre de s'appliquer. Ces territoires ont mis en place un système bancaire ouvert notamment pour favoriser la concurrence à l'égard des grandes banques. L'Australie a également décidé d'effectuer un déploiement du système par étape selon le type de produits, en faisant en sorte que les données des comptes d'opération de base soient rendues accessibles en premier, suivies par les données sur les produits plus complexes (p. ex., prêts hypothécaires). L'UE, par contre, a plutôt choisi de mettre en place le système bancaire ouvert simultanément pour toutes les parties accréditées.

Avant d'en venir à une décision, le Canada devra évaluer avec soin les avantages des deux options, de même que les raisons pour lesquelles il souhaite établir le système bancaire ouvert.

Quels types de destinataires de données seront autorisés ?

Choix faits dans d'autres territoires :

Aucun territoire

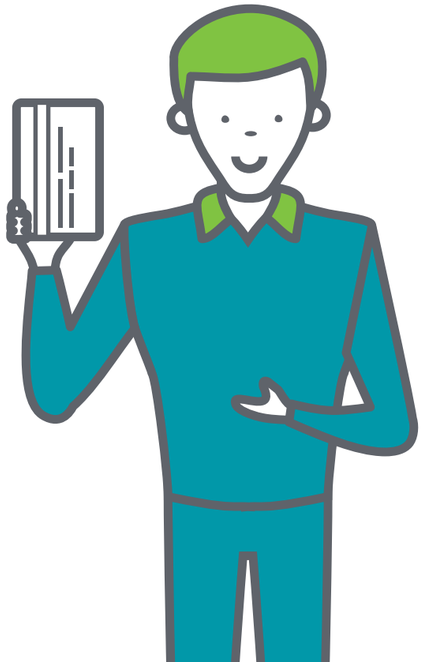
Utilisateurs de données seulement — Utilisateurs et transporteurs de données

Un élément semble uniforme parmi les territoires : seules les entités qui respectent les critères d'accréditation en échelons établis en fonction des risques par l'organisme dirigeant central se voient accorder l'accès aux données des clients (les critères d'accréditation sont présentés en détail à la page 51).

De plus, il existe seulement deux types de destinataires des données : les utilisateurs de données et les transporteurs de données. Les utilisateurs de données sont les utilisateurs finaux des données financières des clients (p. ex., les entreprises de technologie financière et d'autres fournisseurs tiers), alors que les transporteurs de données sont des intermédiaires qui facilitent la circulation des données pour les utilisateurs. Le principal élément qui les distingue est que ces derniers ne créent pas de valeur sur la base du stockage de données.

Si les utilisateurs de données sont essentiels au système bancaire ouvert, la présence de transporteurs de données n'est pas absolument nécessaire. En effet, ceux-ci ont tendance à présenter un risque élevé pour l'écosystème, car ils agissent en tant que source centrale de grands volumes de données, entraînant la possibilité qu'une seule violation menace d'innombrables générateurs de données et clients. Toutefois, ces acteurs procurent également de la valeur à l'écosystème en permettant l'interopérabilité entre les institutions financières, et entre divers territoires présentant des systèmes bancaires ouverts différents. Dans la plupart des territoires, la réglementation ne fait pas de distinction entre les utilisateurs de données et les transporteurs de données. Les transporteurs doivent ainsi être accrédités selon les mêmes critères que les utilisateurs (p. ex., au R.-U., les transporteurs de données doivent être accrédités en tant que fournisseurs de services d'information sur les comptes).

Fondamentalement, la valeur des transporteurs de données dépend du niveau de normalisation des mécanismes de transfert de données utilisés par les divers générateurs de données visés par le cadre. Cette question est examinée de façon plus détaillée à la page 39.



Créer un cadre pour régir un système bancaire ouvert au Canada | Un cadre de système bancaire ouvert pour le Canada

Facteur qui concerne le marché canadien : gouvernance des fournisseurs de services de paiement non traditionnels

La réglementation actuelle des services de paiement au Canada vise principalement à régir les systèmes de paiement majeurs ayant une importance systémique à l'échelle nationale, comme le Système de transfert de paiement de grande valeur (STPGV) et le Système automatisé de compensation et de règlement (SACR), et surveille relativement peu les fournisseurs de services de paiement non traditionnels.

Le nouveau cadre de surveillance des paiements de détail vise à s'assurer que les fournisseurs de services de paiement non traditionnels sont régis efficacement afin de préserver la sécurité et la solidité de l'écosystème de paiements canadien, de favoriser l'efficacité et l'innovation dans le domaine des paiements et de protéger les intérêts des utilisateurs finaux.

Le processus d'accréditation du système bancaire ouvert est susceptible de toucher la plupart de ces entités, alors il est important de coordonner le cadre de surveillance des paiements de détail et le régime de système bancaire ouvert. Cela permettra d'éviter l'émergence de conflits et de chevauchement entre les législations et d'optimiser l'attribution des ressources et des responsabilités parmi les organismes de réglementation.

Quels droits d'accès devrait-on accorder aux destinataires de données ?

Choix faits dans d'autres territoires :

Pour établir son cadre régissant un système bancaire ouvert, le Canada devra également tenir compte de la façon dont les destinataires de données accéderont finalement aux données des clients. Selon les systèmes existants, il y a essentiellement deux façons d'accéder aux données :

- **L'accès en lecture,** qui permet aux destinataires de données d'obtenir des copies des données financières des clients et de les utiliser pour des activités comme le regroupement des données; ou
- **L'accès en écriture,** qui permet aux destinataires de données d'apporter des modifications aux données financières des clients détenues par d'autres institutions.

L'accès en écriture permettrait aux destinataires de données d'agir au nom des clients dans des domaines comme l'initiation de paiement, la fermeture/l'ouverture de compte et la modification de renseignements (p. ex., changement d'adresse). Même si ce mode d'accès offrirait évidemment de nombreuses possibilités pour les institutions financières, il présenterait également de nouveaux aspects complexes, notamment sur le plan de la sécurité.

Comme les destinataires de données seraient en mesure d'apporter des changements aux comptes des clients et de transférer des fonds en leur nom, les institutions devraient prendre des mesures extraordinaires pour atténuer les risques de violation de données. Les générateurs de données devraient établir des systèmes complexes pour assurer la sécurité des renseignements des clients, ce qui exigerait du temps pour la mise en œuvre.

Le cadre de surveillance des paiements de détail et les initiatives de modernisation des paiements incluent déjà des mesures pour surmonter les problèmes liés à l'accès en écriture, ce dont devrait tenir compte le cadre de fonctionnement du système bancaire ouvert dans son étendue afin d'éviter un dédoublement des travaux ou une contradiction dans les orientations.

Créer un cadre pour régir un système bancaire ouvert au Canada | Un cadre de système bancaire ouvert pour le Canada

Facteur qui concerne le marché canadien : modernisation des services de paiement canadiens

Pendant que le secteur envisage la mise en place d'un système bancaire ouvert, Paiements Canada entreprend également de remanier le secteur bancaire canadien par la modernisation des deux principaux systèmes de paiement au Canada, soit le Système de transfert de paiement de grande valeur (STPGV) et le Système automatisé de compensation et de règlement (SACR). Le STPGV sera remplacé par Lynx, un système de paiements de valeur élevée traitant des paiements en temps réel avec certitude de règlement. Le SACR sera remplacé par le Swystème de paiement en temps réel (RTR) et le Moteur d'optimisation du règlement (MOR).

Le RTR facilitera le transfert de fonds de faible valeur en temps réel et soutiendra le développement de services de recouvrement (services à valeur ajoutée offerts par des tiers et déployés dans l'infrastructure du RTR), ce qui stimulera ultimement les innovations dans le domaine des paiements. Le MOR permettra d'améliorer la compensation de lots d'effets moins urgents et des paiements électroniques, assurant des services de paiement rapides et commodes pour les entreprises au Canada. Par cet effort de modernisation – et avec le cadre de surveillance des paiements de détail (présenté plus en détail à la page 35) –, l'initiation de paiement par des tiers devrait être régie en dehors du cadre de fonctionnement du système bancaire ouvert.

L'adoption de la norme ISO 20022 est un autre élément clé de l'initiative de modernisation, qui enrichira les données transmises avec les paiements. Pendant la conception du système bancaire ouvert, il faudra examiner soigneusement le rapport entre l'étendue du système et les données supplémentaires recueillies par l'intermédiaire de la norme ISO.

De plus, alors que le Canada s'apprête à lancer le RTR, il serait prudent d'évaluer comment les risques associés aux pratiques du grattage d'écran sont atténués en amont afin de réduire la vulnérabilité à l'égard de la fraude (p. ex., le partage des identifiants de connexion).

2. Normes

L'examen des décisions prises par d'autres territoires en ce qui a trait au niveau de normalisation peut aider à déterminer dans quelle mesure les normes techniques canadiennes (le cas échéant) doivent être normatives et centralisées, et quelle doit être la structure globale de la surveillance du système.

Pendant l'élaboration d'un cadre pour un système bancaire ouvert, le Canada devrait répondre aux questions suivantes :

- Comment devrait-on élaborer les normes de partage des données ?
- Comment devrait-on gérer le consentement et l'authentification ?
- Comment devrait-on organiser la surveillance du système ?
- Qui devrait participer à la surveillance ?

Comment devrait-on élaborer les normes de partage des données ?

Choix faits dans d'autres territoires :

La normalisation du partage des données devrait être équilibrée en favorisant la concurrence entre les nouveaux venus et les acteurs existants tout en assurant la sécurité et l'intégrité opérationnelle de l'ensemble du système financier.

Dans ce domaine, les organismes de réglementation ont deux principales options :

1. **Normes définies de façon centralisée :**
   les organismes de réglementation peuvent élaborer des normes techniques très directives, imposant des technologies et des processus précis pour le partage des données et contrôlant la conformité de manière stricte.

2. **Normes définies par les générateurs :**
   les organismes de réglementation peuvent définir des politiques générales de partage des données, tout en permettant aux institutions financières et aux tiers d'élaborer de façon indépendante des normes, des technologies et des processus à l'appui.

Bien que le fait d'élaborer des normes directives en matière de partage des données puisse favoriser une plus grande sécurité du système, une meilleure interopérabilité entre les acteurs et une réduction des coûts de développement et d'intégration, des normes strictes peuvent imposer un fardeau de conformité excessif à certains joueurs (tant les institutions financières que les tiers) qui n'auront pas nécessairement les ressources pour assurer leur développement dans ce contexte.

De plus, des normes trop directives peuvent nuire à la capacité de l'écosystème d'adopter rapidement des technologies de partage des données nouvelles et plus efficaces, car cela exigerait une réécriture importante des textes normatifs.

D'autre part, l'élaboration de politiques de partage des données générales (p. ex., un code de conduite) qui laisserait aux acteurs du secteur la responsabilité de créer des normes, des technologies et des processus permettrait une plus grande souplesse et une meilleure capacité de réaction, et pourrait accélérer l'adoption du système bancaire ouvert. De plus, cela permettrait de s'assurer que l'approche à l'égard du partage des données se fonde sur les connaissances des plus grands experts du secteur. Toutefois, cela pourrait entraîner l'émergence de nombreuses normes concurrentes compromettant l'interopérabilité et la sécurité du système, et augmenterait les coûts de développement et d'intégration de tous les acteurs (qui devront peut-être élaborer de nombreux processus de partage des données pour intégrer différents partenaires).

Pour trouver un équilibre entre la promotion de la concurrence et de l'innovation et la sécurité et l'intégrité du système, le mouvement du système bancaire ouvert canadien doit envisager l'adoption d'une approche hybride. Cela signifie l'élaboration d'une norme centrale imposant certains critères minimaux pour le partage des données (pour assurer une interopérabilité de base et protéger les données des clients), mais laissant les principales décisions de conception à la discrétion des acteurs individuels et/ou des consortiums du secteur.

Comment devrait-on gérer le consentement et l'authentification ?

Authentification

Choix faits dans d'autres territoires :

Consentement

Choix faits dans d'autres territoires :

Un modèle de partage des données efficace devrait inclure des processus sécuritaires et simples pour l'authentification et le consentement des clients.

En matière de gestion de l'authentification des clients, deux options principales existent : la responsabilité peut être assumée par les générateurs de données ou par les utilisateurs de données. Confier la gestion de l'authentification aux utilisateurs de données peut créer une expérience utilisateur plus agréable, car le processus de connexion serait alors complètement intégré dans les interfaces des tiers et concorderait à leur conception de l'expérience client. Cela dit, cette option peut également poser des risques supplémentaires pour les clients, car ils devraient échanger leurs identifiants de connexion aux services bancaires avec tous les tiers avec lesquels ils décident de faire affaire. De plus, cela obligerait les destinataires de données à élaborer des processus d'authentification sécuritaires, ce qui pourrait constituer un obstacle à l'entrée pour les tiers fournisseurs de petite taille en raison de la complexité et du temps associés à un tel processus.

Si l'authentification doit être assumée par les générateurs de données, trois modèles sont possibles :

- **Intégrée :** au moment de l'authentification, le client doit entrer ses identifiants de connexion aux services bancaires dans un « widget » hébergé et exploité par le générateur de données, qui est intégré directement dans l'interface d'un tiers;
- **Redirigée :** au moment de l'authentification dans la plateforme d'un tiers, le client est redirigé vers le site Web de son générateur de données (le portail de services bancaires en ligne), où il doit entrer ses identifiants de connexion; une fois qu'il a confirmé son identité, il est de nouveau redirigé vers le destinataire de données; ou
- **Découplée :** au moment de l'authentification, le client doit accéder au portail en ligne du générateur de données; après avoir confirmé son identité, le client récupère et copie manuellement le code pour le copier dans le site Web du tiers.

Chacune de ces méthodes représente un compromis différent entre l'expérience client et la sécurité. L'approche intégrée est pratique pour les clients, mais elle présente un risque d'hameçonnage plus élevé. L'approche redirigée est la plus couramment utilisée par les services offerts sur Internet (p. ex., Facebook), et les clients connaissent bien ce processus. L'approche découplée est beaucoup moins utilisée, car elle exige des manipulations de la part des clients et peut nuire à l'adoption d'un service. Cependant, elle présente moins de risques d'hameçonnage que les deux autres modèles.

Hameçonnage

L'hameçonnage est une fraude d'ingénierie sociale où des individus malveillants tentent d'obtenir des renseignements de nature sensible par des moyens trompeurs. Par exemple, un individu malintentionné conçoit un site Web d'un faux fournisseur qui redirige le client vers une page ayant l'apparence de l'interface de sa banque et lui permet de voler les identifiants de connexion et d'autres renseignements personnels du client pour voler son argent par la suite.

Éléments d'authentification

L'authentification peut reposer sur la combinaison de deux éléments prouvant l'identité :

- Élément lié à la connaissance (p. ex., mot de passe);
- Élément lié à la possession (p. ex., clé, téléphone mobile);
- Élément inhérent (p. ex., empreinte digitale).

Le fait d'exiger plus d'un élément d'identification constitue en l'authentification à facteurs multiples, laquelle augmente la sécurité du processus d'authentification, mais nuit à l'expérience de l'utilisateur (p. ex., en lui demandant de recevoir un code sur son appareil mobile et de l'entrer dans le système). Les précédents établis dans d'autres territoires indiquent qu'il est prudent d'exiger plus d'un élément d'identification.

Facteur qui concerne le marché canadien : rôle d'une fonctionnalité d'identité numérique

L'identité numérique consiste à stocker électroniquement une information permettant aux personnes de s'identifier en ligne sans devoir continuellement présenter une pièce d'identité physique. Si une forme standard d'identité numérique était conçue et imposée au Canada, les interfaces en ligne des banques n'auraient pas à comporter un processus d'authentification complet. La fonctionnalité offrant un service d'identité numérique pourrait agir en tant que gestionnaire central de l'authentification, ce qui améliorerait la sécurité et l'expérience de l'utilisateur et réduirait les coûts de l'authentification pour les acteurs du marché.

Sur le plan de l'aspect évolutif du système bancaire ouvert, il serait important d'évaluer dans quelle mesure l'identité numérique pourrait aider les banques et les autres générateurs de données à gérer les risques liés à l'authentification, permettre une analyse plus approfondie des fraudes et créer une expérience client plus agréable.

Créer un cadre pour régir un système bancaire ouvert au Canada | Un cadre de système bancaire ouvert pour le Canada

En vertu du système bancaire ouvert, les clients auront le contrôle de leurs propres données et devraient pouvoir fournir des directives précises concernant leur transfert et leur utilisation. L'obtention du consentement à l'égard de l'utilisation des données pourrait être assumée par les générateurs de données, par les destinataires de données ou par les deux.

Peu importe le modèle choisi en matière de consentement, l'objectif ultime doit être d'assurer que les opérations sont transparentes et que le consentement du client est valable et éclairé. Un processus solide de consentement du client devrait également dépasser les exigences de la LPRPDE – notamment en ce qui concerne le caractère explicite du consentement et le respect de la loi –, car les normes à cet égard ne sont pas suffisamment élaborées dans la législation actuelle, qui est plutôt récente.

Pour y parvenir, le mouvement du système bancaire ouvert canadien devrait s'inspirer des meilleures pratiques des autres territoires. Les messages de demande de consentement devraient être simples – idéalement rédigés dans un langage simple et de manière concise tout en présentant tous les renseignements importants dans un seul écran. Cela permettrait de s'assurer que le processus d'authentification et le processus de consentement ne nuiraient pas à l'adoption du système bancaire ouvert.

De plus, les clients devraient pouvoir retirer leur consentement en tout temps. Conformément à l'esprit visant à redonner aux clients le contrôle de leurs données, ceux-ci devraient également pouvoir en révoquer l'accès s'ils le souhaitent. Cependant, ce principe ne devrait pas s'appliquer aux données qui sont déjà détenues par le générateur de données, car les cadres réglementaires actuels ont souvent besoin de ces données aux fins de la lutte contre le blanchiment d'argent.

Facteur qui concerne le marché canadien : modification de la LPRPDE

La mise en place d'un système bancaire ouvert nécessite une réforme des lois sur la protection des renseignements personnels. Bien que les lois actuelles dictent la façon dont les renseignements doivent être conservés, stockés et utilisés, le cadre de système bancaire ouvert devra comporter des règlements plus étendus, précisant notamment la façon dont les données doivent être partagées entre les institutions financières et les fournisseurs tiers.

Un processus de consultation est en cours au Canada en vue de modifier la LPRPDE, laquelle serait ensuite alignée sur une bonne partie des changements apportés au Règlement général sur la protection des données (RGPD) de l'Union européenne. Le RGPD impose aux institutions financières l'obligation d'effacer les données des clients (les données recueillies directement auprès des clients et les données obtenues de tiers) à la demande des clients si l'une ou l'autre des six conditions suivantes est remplie :

1. les données personnelles ne sont plus nécessaires aux fins pour lesquelles elles ont été recueillies ou autrement traitées;

2. la personne concernée par les données retire son consentement […];

3. la personne concernée par les données s'oppose au traitement […] et il n'existe aucune considération légitime impérieuse d'effectuer le traitement […];

4. les données personnelles ont subi un traitement illicite;

5. les données personnelles ont été effacées conformément à une obligation juridique […];

6. les données personnelles ont été recueillies relativement à l'offre des services de la société de l'information […].

Le RGPD couvre les documents électroniques et physiques et inclut les fichiers de sauvegarde. Cependant, le droit à l'oubli peut être renversé ou retardé pour une partie ou l'ensemble des catégories de données en raison des obligations réglementaires imposées à l'entité qui contrôle les données (p. ex., tenue des dossiers à des fins comptables ou fiscales).

Dans l'élaboration d'un système bancaire ouvert au Canada, il faut prendre soin de s'assurer que le cadre est conforme à tous les changements apportés à la LPRPDE, et que le cadre et la LPRPDE ne présentent aucune lacune flagrante relativement au partage consensuel des données dans les services financiers.

Dans d'autres territoires, comme en Australie, des dispositions précises ont été incluses dans les politiques relatives au système bancaire ouvert pour compléter les lois actuelles en matière de protection des renseignements personnels, notamment en ce qui concerne la précision du consentement et le droit à l'oubli.

Créer un cadre pour régir un système bancaire ouvert au Canada | Un cadre de système bancaire ouvert pour le Canada

Comment devrait-on organiser la surveillance du système ?

Choix faits dans d'autres territoires :

Un cadre de système bancaire ouvert nécessitera deux phases de gouvernance : la première pour définir le système global, et la seconde pour effectuer la surveillance opérationnelle continue (en agissant comme un organisme de règlement des litiges traitant les questions de responsabilité entre les générateurs de données, les destinataires de données et les clients).

Les responsabilités de chaque structure de gouvernance seront uniques. Voici quelques exemples de ce qu'elles devraient comprendre :

Phase 1 :
Définition du système bancaire ouvert

- Élaborer les normes de partage des données auxquelles les générateurs de données doivent se conformer pour rendre les données des clients accessibles;
- Élaborer les critères d'accréditation précis déterminant quels destinataires de données sont autorisés à demander des données aux générateurs de données;
- Définir le cadre de responsabilité qui décrit clairement les rôles et les responsabilités des générateurs de données, des destinataires de données et des clients.

Phase 2 :
Exploitation du système bancaire ouvert

- Effectuer une surveillance continue des générateurs de données et des destinataires de données accrédités (p. ex., vérifier régulièrement les destinataires des données pour s'assurer qu'ils répondent aux critères d'accréditation);
- Agir en tant qu'organisme central de règlement des litiges traitant les plaintes des clients et les questions de responsabilité;
- Soutenir l'élaboration du matériel d'information et voir à l'éducation des clients;
- Exiger un produit d'assurance obligatoire, semblable à la Société d'assurance-dépôts du Canada, qui pourra verser des indemnités en cas de sinistre préjudiciable entraînant la défaillance complète d'un destinataire de données (ce programme pourrait être financé par la voie de frais obligatoires prévus dans le cadre du processus d'accréditation);
- Créer un système de gestion de l'identité numérique, du consentement et de l'authentification;
- Gérer le recouvrement des divers coûts variables engagés par les générateurs de données pour rendre les données accessibles aux tiers.

Les responsabilités de gouvernance et de surveillance du système bancaire ouvert peuvent être :

- centralisées dans une fonction de gouvernance consolidée;
- réparties entre les générateurs de données, les destinataires de données et des organisations du secteur représentant les consommateurs, qui devraient s'autoréguler par la voie de « codes de conduite » volontaires au sein du secteur;
- divisées selon un modèle à mi-chemin entre les deux approches précédentes, certains aspects de gouvernance étant imposés par une autorité centralisée, et les autres aspects laissés aux acteurs du secteur, qui devraient élaborer des « codes de conduite ».

La répartition idéale des responsabilités entre les diverses parties peut évidemment faire l'objet de discussions, mais les intervenants canadiens devraient garder en tête les principes directeurs mentionnés précédemment lorsqu'ils détermineront la répartition qui convient le mieux au cadre de système bancaire ouvert au Canada.

Voici certaines façons dont ces principes directeurs peuvent être utilisés pour simplifier le processus de prise de décision :

Valeur

Éviter les conflits d'intérêts qui empêchent de créer de la valeur pour les Canadiens. Pour s'assurer que le système bancaire ouvert procure une véritable valeur aux Canadiens, les fonctions de gouvernance doivent représenter les intérêts des consommateurs. En vertu de ce principe, ils devront mettre en place des mesures garantissant que ni les générateurs de données ni les destinataires de données ne sont les seuls à contrôler l'élaboration du cadre d'accréditation, car cela pourrait entraîner la création d'un processus trop complexe (qui restreindrait de façon exagérée la participation des destinataires de données) ou d'un écosystème trop ouvert (qui exposerait l'écosystème des services financiers à des risques excessifs).

Transparence

Veiller à ce que les Canadiens reçoivent une information claire et transparente en ce qui concerne le partage des données. Afin que les Canadiens bénéficient d'une transparence constante dans le contexte du partage des données, il faut mettre en place des normes relatives à l'information qui sera partagée et à la façon dont elle sera utilisée. Ces normes peuvent entraîner la création d'une grille commune pour le partage d'information, comme d'autres territoires l'on fait.

Sécurité

Tirer parti de l'autorité réglementaire pour protéger la sécurité et la solidité du système financier au Canada. Le cadre de gouvernance doit s'assurer que les Canadiens ne sont pas exposés à des risques excessifs. Par exemple, le système doit indiquer les cas où il sera autorisé d'accéder à des ensembles de données par une méthode autre que celles qui sont prévues dans le cadre de système bancaire ouvert pour des données qui pourraient être accessibles par le système bancaire ouvert. Idéalement, le système bancaire ouvert devrait offrir aux consommateurs un accès aux données plus sécuritaire, économique, fiable et convivial, de sorte que les autres options possibles (comme le grattage d'écran) deviendraient trop risquées pour le système.

Adoption

Tirer parti efficacement des divers acteurs de l'écosystème afin de réduire au minimum le dédoublement des efforts. Étant donné la diversité des activités de surveillance qui doivent être exécutées conjointement à l'égard des institutions financières et de l'infrastructure du système (p. ex., le cadre de surveillance des paiements de détail), le cadre de gouvernance devrait être conçu pour réduire au minimum le dédoublement des responsabilités parmi les parties. La centralisation des responsabilités de gouvernance entraînerait des économies d'échelle, mais chaque aspect devrait être évalué au cas par cas afin de réduire le coût total du système. Par exemple, confier à une entité centrale unique la gestion des questions concernant la responsabilité ou le recouvrement des coûts pourrait aider à simplifier ces processus (de façon plus économique) pour tous les acteurs du système bancaire ouvert.

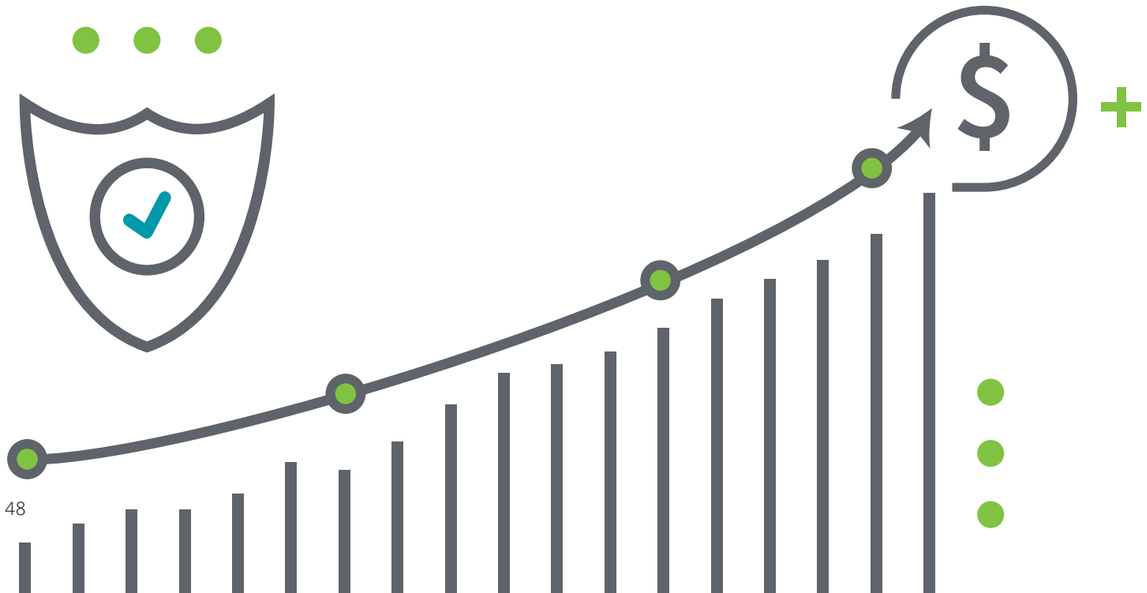
Qui devrait participer à la surveillance ?

Généralement, même les organismes de surveillance centralisés combinent des organismes de réglementation et des acteurs du marché. Par exemple, au R.-U., l'entité de mise en œuvre du système bancaire ouvert a été créée par la Competition and Markets Authority (un organisme de réglementation régissant la concurrence et les marchés), mais est financée par les neuf plus grandes banques du R.-U. Dans l'UE, même si des organismes de réglementation voient à l'accréditation des tiers et à l'élaboration des politiques, la mise en œuvre des politiques fondées sur les principes dans les États membres nécessite la participation d'organisations d'établissement des normes et de consortiums divers (comme le groupe de Berlin).

Le présent rapport vise à présenter différents points à considérer pour la mise en place d'un système bancaire ouvert au Canada, peu importe le modèle de gouvernance et de surveillance choisi et les parties impliquées dans ce processus. Cela dit, les choix qui seront faits en cette matière entraîneront possiblement des résultats différents.

Par exemple, en vertu d'un modèle de gouvernance très centralisé, l'étendue des générateurs de données dépendra probablement des parties constituant l'entité de gouvernance. Ainsi, une entité centrale dirigée par un organisme de réglementation aurait probablement l'autorité d'exiger qu'un large ensemble de participants – incluant des caisses de crédit et des sociétés de fiducie – soit inclus parmi les générateurs de données. D'un autre côté, une entité dirigée par un consortium ou une association sectorielle pourrait compter sur une participation volontaire des institutions financières, ce qui pourrait limiter l'étendue des générateurs de données.

Finalement, un examen plus approfondi du système bancaire ouvert au Canada devra tenir compte du rôle et de la structure de l'organisme central, car ces aspects influeront grandement sur son développement. Ces décisions devraient donc être prises tôt dans le processus.



3. Modèle commercial et modèle de responsabilité

Les choix faits dans d'autres territoires concernant le modèle commercial et le modèle de responsabilité aident à définir la façon dont les coûts et les responsabilités doivent être répartis entre les acteurs du marché.

Pendant l'élaboration d'un cadre pour un système bancaire ouvert, le Canada devrait répondre aux questions suivantes :

- Comment les destinataires des données obtiendront-ils l'accès aux données des générateurs ?
- Comment devrait-on gérer la responsabilité ?
- Quel sera le modèle économique à l'appui ?
- À quelle fréquence devrait-on autoriser les demandes de données ?

Comment les destinataires des données obtiendront-ils l'accès aux données des générateurs ?

Choix faits dans d'autres territoires :

Deux modèles pourraient être utilisés pour faciliter l'accès aux données des générateurs :

1. **Exigences d'accréditation communément reconnues et contrats standards entre les générateurs de données et les destinataires de données.** Dans ce modèle, les destinataires de données devraient obtenir une certification pour démontrer qu'ils répondent aux critères établis (p. ex., en matière de protection des renseignements personnels et de sécurité). Certains éléments concernant la relation entre les générateurs de données et les destinataires de données (p. ex., méthode et modalités de recouvrement des coûts, responsabilités) devraient être définis par un contrat normalisé permettant certaines variations pour tenir compte de la situation particulière de chaque entente de partage des données.

2. **Ententes commerciales bilatérales (entre les générateurs de données et les destinataires de données).** Dans ce modèle, l'accès à l'écosystème et certains autres éléments seraient définis dans des ententes bilatérales établies entre les générateurs de données et les destinataires de données, où les parties auraient l'entière latitude de négocier les modalités de l'entente.

Un cadre d'accréditation communément accepté simplifierait le processus d'obtention de l'accès aux données et permettrait ultimement à un plus grand nombre de tiers de faire partie de l'écosystème de services bancaires ouverts. Cependant, un tel cadre offrirait moins de souplesse à l'égard des dynamiques changeantes du marché, et exigerait des mises à jour continues pour refléter le plus exactement possible l'environnement global du Canada.

Des ententes commerciales permettraient de s'adapter plus rapidement à des conditions changeantes, mais pourraient restreindre l'efficacité du système (p. ex., les entreprises d'agrégation de données devraient négocier des ententes bilatérales avec chaque institution financière participant au système bancaire ouvert en tant que générateur de données).

Si le Canada opte pour un système fondé sur une politique d'accréditation centralisée, il devrait s'inspirer des autres territoires pour l'élaboration des éléments suivants :

- **Protocoles de sécurité et de protection des renseignements confidentiels :** gérer de façon responsable les données personnelles et financières, et s'assurer que les destinataires des données n'entraînent pas l'émergence de risques excessifs dans le système.
- **Assurance indemnité :** fournir aux générateurs de données l'assurance raisonnable que les destinataires de données seront en mesure de payer si des problèmes de responsabilité surviennent.
- **Processus défini de gestion des plaintes des consommateurs :** fournir aux consommateurs une assurance raisonnable que les tiers accrédités pourront les aider en cas de problème.
- **Mesures d'atténuation pour les perturbations importantes :** veiller à mettre en place des protocoles appropriés en cas de défaillances, de manquements à la sécurité ou d'autres événements empêchant la continuité des activités dans le système.

L'utilisation prévue des données est un sujet qui fait l'objet de vifs débats dans d'autres territoires où un système bancaire ouvert est déjà en place. Inclure les cas d'utilisation parmi les critères pourrait aider à protéger les consommateurs contre les individus malintentionnés; cependant, cela peut restreindre l'entrée de fournisseurs tiers présentant de nouveaux modèles commerciaux et nuire à l'innovation dans le marché.

Comment devrait-on gérer la responsabilité ?

Choix faits dans d'autres territoires :

En règle générale, un système bancaire ouvert devrait réduire les risques dans le système en faisant en sorte qu'on ait moins recours à la méthode du grattage d'écran, qui oblige les consommateurs à communiquer leurs identifiants de connexion. Cependant, le système bancaire ouvert peut entraîner un transfert de responsabilité des clients (que le grattage d'écran amène à enfreindre l'entente qu'ils ont avec leur banque) aux autres acteurs du système. Par conséquent, un cadre de responsabilité clairement défini est essentiel pour obtenir l'adhésion des générateurs de données et des destinataires de données.

Toutefois, ce type de cadre de responsabilité dépend grandement de diverses autres décisions relatives au cadre. Voici certains choix qui ont été faits dans d'autres territoires :

- Si l'on se réfère aux systèmes bancaires ouverts déjà établis, le cadre de responsabilité devrait être compatible avec les autres réglementations existantes, et non les remplacer. Cela éviterait d'élaborer des exigences chevauchant la réglementation actuelle ou entrant en conflit avec elle, et permettrait de s'assurer que tous les acteurs ont une compréhension commune des rôles et des responsabilités de chacun.

- En ce qui concerne les atteintes non intentionnelles à la sécurité des données, de nombreux territoires ont décidé d'attribuer la responsabilité à la partie responsable de l'atteinte (dans la vaste majorité des cas, le destinataire de données). Dans ce type de scénario, le destinataire de données dispose généralement d'une assurance responsabilité adéquate en cas d'atteinte à la sécurité des données, et le programme d'accréditation des destinataires de données, le cas échéant, inclut une norme en matière de sécurité et une norme en matière d'assurance responsabilité. Ce cadre rehausse la confiance des consommateurs dans le système bancaire ouvert, même après un hypothétique incident d'atteinte à la sécurité des données.

- Pour les cas où des entreprises font intentionnellement une utilisation abusive des données de clients, par exemple lorsque des acteurs malintentionnés ont obtenu une accréditation, certains territoires attribuent la responsabilité à l'organisme ayant accordé et/ou prolongé cette accréditation.

- À l'heure actuelle, de nombreux territoires permettent aux générateurs de données de rompre une relation avec un destinataire de données s'ils soupçonnent une atteinte non intentionnelle à la sécurité des données ou une utilisation abusive des données. Ces générateurs de données sont tenus de signaler rapidement les cas présumés de violation ou d'utilisation abusive aux autres générateurs de données et/ou à l'organisme chargé de l'accréditation afin d'atténuer les répercussions du manquement.

- Pour de nombreux territoires ayant un système bancaire ouvert, les acteurs du système devraient être responsables de leurs actions, mais pas des actions des autres (p. ex., les générateurs de données ne devraient pas être tenus responsables des pertes causées par les destinataires des données). Ainsi, bien que les fournisseurs de comptes soient désignés comme les premiers intervenants en cas de perte, de nombreux territoires ont mis en place des contrôles leur permettant d'exercer des recours contre des tiers responsables d'un incident. Cela permet de s'assurer que les fournisseurs de comptes ne portent pas injustement tout le fardeau de la responsabilité, et favorise une plus grande adhésion de leur part dans le système bancaire ouvert. Certains territoires imposent également aux tiers fournisseurs des exigences de fonds et/ou des assurances indemnités pour protéger les fournisseurs de comptes.

- Dans de nombreux territoires, les générateurs de données sont tenus de communiquer fidèlement toute information applicable aux destinataires de données, mais ne sont pas tenus responsables des erreurs ou des inexactitudes dans les données transférées.

Créer un cadre pour régir un système bancaire ouvert au Canada | Un cadre de système bancaire ouvert pour le Canada

Quel sera le modèle économique à l'appui ?

Choix faits dans d'autres territoires :

Pour rendre les données accessibles, les générateurs de données sont susceptibles d'engager des coûts fixes initiaux, de même que des coûts variables courants. Un cadre de système bancaire ouvert doit préciser si les générateurs de données sont autorisés à récupérer leurs coûts variables, par exemple en imposant des frais minimaux aux destinataires de données. Pour évaluer si une telle option conviendrait au cadre de système bancaire ouvert du Canada, les intervenants doivent tenir compte de différents facteurs :

- **Équité pour les générateurs de données :** au-delà des coûts directs nécessaires pour rendre les données accessibles, les générateurs de données peuvent devoir assumer des dépenses indirectes supplémentaires (comme pour gérer les plaintes des clients). La réglementation devrait permettre de s'assurer qu'ils sont en mesure d'assumer leurs fonctions sans être injustement accablés par le processus.

- **Comparaison avec la situation actuelle des destinataires de données :** les solutions fondées sur les API sont susceptibles d'exiger moins de ressources (et, donc, d'être moins coûteuses) que les solutions que les destinataires de données utilisent aujourd'hui. Par conséquent, les coûts assumés par les destinataires de données pour accéder aux données financières des clients devraient être inférieurs aux coûts actuels.

- **Barrière à l'entrée :** l'imposition de frais pour accéder aux données peut constituer une barrière à l'entrée dans le marché. Cela peut entraîner des conséquences négatives (comme freiner l'innovation) ou des résultats positifs (comme décourager les cas d'utilisation générant peu de valeur), selon l'importance des frais de transfert de données.

À quelle fréquence devrait-on autoriser les demandes de données ?

Choix faits dans d'autres territoires :

** Remarque : Aucune information disponible concernant les limites de demandes de données au Japon.*

Au R.-U., les destinataires de données ne peuvent faire plus de quatre demandes de données par période de 24 heures, à moins que les générateurs de données et les destinataires s'entendent sur une fréquence plus élevée. Toutefois, les clients peuvent faire autant de demandes de données qu'ils le veulent sans restriction, ce qui correspond généralement au niveau d'accès actuellement offert par les services bancaires en ligne, par exemple, dans les situations où les clients ont accès à leurs données bancaires 24 heures sur 24 et 7 jours sur 7 par la voie de l'interface en ligne de leur banque. Cette distinction entre les demandes de données présentées par les destinataires (dont le nombre est souvent restreint) et par les clients (souvent illimitées) est faite dans de nombreux territoires.

Le fait d'autoriser un nombre plus important de demandes peut générer des cas d'utilisation supplémentaires (p. ex., un outil de surveillance des soldes des comptes pouvant avertir les utilisateurs quand un découvert est sur le point de se produire) et imposer un fardeau plus important aux générateurs de données (pour le transfert des données, par exemple). Pour éviter que les générateurs de données soient submergés de demandes, des frais peuvent être imposés aux destinataires de données pour chaque demande, ou une limite peut être fixée quant au nombre de demandes autorisées.

Conclusion

Dans la modernisation de son écosystème de services financiers, le Canada se trouve à un point d'inflexion. Avec la modernisation des paiements en cours et la révision attendue des méthodes de protection des renseignements confidentiels par la voie de la LPRPDE, les services bancaires ouverts constituent le troisième pilier d'un environnement qui générera de nouvelles attentes chez les consommateurs à l'égard de la prestation et de la consommation des services financiers.

Si les prévisions se concrétisent, le secteur des services financiers et les futurs consommateurs pourront tous tirer profit d'un mouvement plus libre des clients entre les organisations, d'expériences financières personnalisées et sur mesure et de l'automatisation de procédures et de tâches traditionnellement longues.

Cependant, ce mouvement ne transformera pas instantanément l'écosystème des services financiers. Les changements majeurs découlant du système bancaire ouvert se feront plutôt graduellement, ce qui signifie que de grandes possibilités existent tant pour les nouveaux venus souhaitant faire leur place dans le marché que pour les acteurs actuels. Pendant cette transition, les institutions financières bien établies auraient tout à gagner à revoir leurs solutions bancaires actuelles si elles veulent jouer un rôle de premier plan dans le remodelage du marché.

Le système bancaire ouvert n'est qu'une étape d'un mouvement plus large reposant sur la volonté de redonner aux clients le contrôle de leurs propres données. Le droit de contrôle des données des consommateurs dépasse les données financières, ce qui signifie que le système bancaire ouvert pavera la voie aux autres secteurs. En faisant le premier pas de manière délibérée et calculée, le système bancaire ouvert peut agir en tant que modèle, ce qui illustre le rôle prédominant que jouent les services financiers dans la société canadienne et, par-dessus tout, dans la protection des consommateurs.

Notes

[1] ZDNet, "Westpac predicts Open Banking to cost AU$200m to implement," by Asha McLean, October 12, 2018, https://www.zdnet.com/article/westpac-predicts-open-banking-to-cost-au200m-to-implement, consulté le 18 mars 2019.

[2] Competition & Markets Authority, "Making banks work harder for you," August 9, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/544942/overview-of-the-banking-retail-market.pdf, consulté le 18 mars 2019.

[3] Australian Government, "Review into Open Banking in Australia," 2017, https://static.treasury.gov.au/uploads/sites/1/2017/08/Review-into-Open-Banking-IP.docx, consulté le 18 mars 2019.

[4] The Government of Japan, "Drive Innovation and Trade," https://www.japan.go.jp/abenomics/innovation/index.html, consulté le 18 mars 2019.

[5] Abacus Data, prepared for Canadian Bankers Association, "How Canadians Bank," 2016, https://www.cba.ca/Assets/CBA/Documents/Files/Article%20Category/PDF/info-howCanadiansBank-poll-2016-fr.pdf, consulté le 18 mars 2019.

Personnes-ressources

Rob Galaski
Associé directeur mondial
Services bancaires et marchés financiers
rgalaski@deloitte.ca

Todd Roberts
Associé
Leader, Paiements Canada
toddroberts@deloitte.ca

Hwan Kim
Leader canadien
Système bancaire ouvert
hwankim@deloitte.ca

www.deloitte.ca

Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans de nombreux secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500[MD] par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Pour en apprendre davantage sur la façon dont les quelque 264 000 professionnels de Deloitte ont une influence marquante – y compris les 9 400 professionnels au Canada – veuillez nous suivre sur **LinkedIn, Twitter** ou **Facebook**.

Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir **www.deloitte.com/ca/apropos**.

© Deloitte S.E.N.C.R.L./s.r.l. et ses sociétés affiliées.

Conçu et produit par le Service de conception graphique de Deloitte, Canada. 18-5879T