

**Note d'information pour le Comité permanent des finances  
41<sup>e</sup> législature, 2<sup>e</sup> session**

***Les paiements mobiles et la protection des consommateurs au Canada- Résumé***

**Agence de la consommation en matière financière du Canada**

**Lucie Tedesco, commissaire**

**27 février 2014**

***Ceci est un résumé. Pour lire le document de recherche au complet, voir :***

<http://www.fcac->

[acfc.gc.ca/Fra/ressources/rechercheSondages/Documents/FCAC\\_Mobile\\_Payments\\_Consumer\\_Protection\\_accessible\\_FR.pdf](http://www.fcac-acfc.gc.ca/Fra/ressources/rechercheSondages/Documents/FCAC_Mobile_Payments_Consumer_Protection_accessible_FR.pdf)

L'instauration des paiements mobiles pourrait avoir des répercussions sur les consommateurs canadiens de produits et services financiers. Les mécanismes de protection des consommateurs qui s'appliquent à ces paiements dépendent de la source sous-jacente des fonds et du type d'entreprise fournissant le service. Étant donné que les paiements mobiles suscitent l'intérêt de divers fournisseurs de services, les obligations en matière de protection des consommateurs varient sur le marché, ce qui explique la protection inégale des paiements mobiles au Canada. En introduisant un nouveau moyen ainsi que de nouveaux modèles d'affaires et participants sur le marché, les paiements mobiles pourraient poser de nouveaux risques pour les consommateurs et modifier l'application du cadre actuel de protection des consommateurs.

**Risques de protection inégale.** Le milieu des paiements mobiles comprend un certain nombre de secteurs d'activité qui travaillent ensemble. Des incohérences existent dans le cadre de protection des consommateurs lorsque les obligations diffèrent selon le type d'entité qui offre un produit ou un service. Dans certains pays membres de l'Organisation de coopération et de développement économiques, on a réclamé que des normes minimales de protection des consommateurs s'appliquent à toutes les sources de paiement mobile. ***Au Canada, il serait utile que les décideurs envisagent de façon plus poussée la mise en œuvre de normes minimales de protection des consommateurs, qui s'appliqueraient uniformément dans tout le marché des paiements mobiles.***

Dans plusieurs administrations hors du Canada, des textes de loi ont été rédigés et ils s'appliquent aux institutions financières et à « d'autres entités »; tous les fournisseurs sont donc soumis aux mêmes obligations. Notre analyse révèle que les consommateurs canadiens bénéficieraient d'une réglementation qui tient compte de tous les fournisseurs de services de paiement mobile sans égard au type d'entité et qui est harmonisée à l'échelle des administrations canadiennes. Une telle réforme stratégique pourrait exiger davantage de données probantes. Vu la variation sur le marché, il sera important de surveiller les pratiques d'affaires des différentes entités en vue d'évaluer les pratiques de protection des consommateurs de tous les participants. Une surveillance de ce type apportera des éléments d'information sur la mesure dans laquelle les lacunes du cadre de protection des consommateurs canadiens posent des problèmes aux consommateurs, et sur la meilleure façon d'y remédier.

**Risques associés à la divulgation.** D'après notre analyse, bien que les émetteurs de sources de fonds soient tenus de fournir un contrat ou une entente sur les modalités, ils ne sont pas tous assujettis au

même niveau d'exigence en matière de divulgation. Par ailleurs, la réglementation canadienne n'exige pas que la divulgation soit optimisée pour les appareils mobiles. Ces appareils se prêtent bien à des fonctionnalités comme la divulgation en temps opportun, les « tableaux de bord » permettant d'examiner les paramètres de divulgation et les icônes indiquant qu'une application recueille des données de géolocalisation. ***Nous invitons les décideurs canadiens à se pencher sur la question de savoir s'il convient que les fournisseurs de services soient tenus de divulguer les modalités d'une entente et les politiques sur la protection des renseignements personnels, d'une manière qui soit optimisée pour les appareils mobiles et uniforme à l'échelle du marché .***

**Risques de fraude et de mauvais usage des biens des consommateurs.** Une ambiguïté pourrait surgir au sujet de l'application des dispositions relatives à la responsabilité zéro si des numéros d'identification personnels ne sont pas demandés pour sécuriser les appareils mobiles ou authentifier les paiements. De façon générale, les obligations canadiennes en vigueur constituent une solide assise pour la protection des biens des consommateurs contre la fraude et le mauvais usage. Toutefois, des modifications ou d'autres engagements pourraient être nécessaires pour que les mécanismes de protection des consommateurs demeurent à jour sur le plan technologique et valables compte tenu de l'apparition de nouveaux médias et intermédiaires. ***Une surveillance et une analyse des politiques plus poussées s'imposent afin de déterminer s'il est nécessaire d'effectuer des réformes législatives pour dissiper les éventuelles ambiguïtés, comme celles liées à la responsabilité en cas de perte.***

L'inscription de montants frauduleux sur les factures de téléphone mobile par des tierces parties (« bourrage de facture ») est considérée comme un risque au Canada et dans de nombreux autres pays. L'adoption du Code sur les services sans fil en décembre 2013 apportera de nouvelles précisions sur les responsabilités des fournisseurs de services et des consommateurs concernant le bourrage de facture et d'autres pratiques de facturation directe par l'entreprise de télécommunications. ***Le Code exigera que les frais de tierces parties soient clairement indiqués sur les factures, et que des renseignements expliquant le processus de blocage de tels montants y soient donnés. Il exigera également que les consommateurs aient accès à une procédure claire et cohérente de traitement des plaintes et de recours.***

Il semble y avoir une lacune dans le cadre lié aux risques associés aux portefeuilles mobiles fondés sur la technologie de la communication en champ proche (NFC). La sécurité des authentifiants sur un appareil mobile inquiète énormément les consommateurs; il est donc préoccupant que les fournisseurs de services de paiement mobile n'aient pas d'obligations particulières relatives à l'utilisation de cette technologie. Le modèle de référence, soit le *Canadian NFC Mobile Payments Reference Model*, peut procurer un niveau de sécurité aux utilisateurs des paiements mobiles qui ont accès à des fonds émis par une institution financière participante. Toutefois, la conformité au modèle de référence est facultative et n'est pas assujettie à la surveillance d'un organisme.

**Responsabilité du règlement des différends.** Il est important que les consommateurs aient accès à des mécanismes de règlement des différends et de recours. Notre analyse révèle que ce principe n'est pas appliqué uniformément aux paiements mobiles au Canada, car les obligations varient d'un fournisseur de services à un autre. À en juger par les expériences d'autres pays, il serait dans l'intérêt des

consommateurs que tous les paiements mobiles bénéficient d'une même protection. Ainsi, les consommateurs ne seraient pas désavantagés dans le contexte du règlement des différends. C'est particulièrement pertinent vu les types de modèles d'affaires multipartites que l'on trouve sur le marché des paiements mobiles. Le Canada n'a aucune loi qui prévoit la nomination d'une seule partie chargée de communiquer les procédures aux consommateurs, et d'agir de point de contact pour les recours. Il faudra peut-être prescrire des règles aux fournisseurs du marché des paiements mobiles et attribuer une responsabilité claire pour ce qui est du règlement des différends. ***Les décideurs pourraient se pencher sur la question de savoir quels fournisseurs de services sont les mieux placés pour jouer ce rôle central de point de contact au Canada.***

**Éducation des consommateurs de produits et services financiers.** Pour qu'un régime de protection soit efficace, les consommateurs doivent connaître leurs droits et leurs responsabilités. Le fait d'être bien renseigné donne aux consommateurs les moyens d'agir et améliore leur capacité à prendre des décisions éclairées. Les consommateurs bien renseignés sont susceptibles de mieux comprendre l'information clé des documents de divulgation et de chercher les ressources qui les aideront à comprendre l'information complexe. L'ACFC élabore actuellement des documents d'information à ce sujet pour les Canadiens. Ces documents comprennent de l'information et des conseils sur la protection des renseignements financiers dans le cadre des opérations bancaires en ligne et des paiements mobiles, sur la marche à suivre pour déposer une plainte relative à un fournisseur de services de paiement mobile ou sans fil et sur les personnes avec lesquelles communiquer en cas de problème concernant les paiements mobiles ou les opérations bancaires en ligne. Ces documents seront affichés sur le site Web de l'ACFC (<http://www.fcac-acfc.gc.ca/Fra/Pages/home-accueil.aspx>) d'ici la fin de mars 2014.

**Profilage.** D'après des sources d'information des États-Unis et d'autres pays, les fournisseurs de services vendent des données sur les utilisateurs à des tiers chargés de marketing, qui ciblent les consommateurs en s'appuyant sur des renseignements démographiques, comportementaux et géographiques. Cette technique, appelée profilage, consiste à regrouper d'importantes quantités de données sur les consommateurs et à les analyser afin de prévoir et d'établir le comportement des consommateurs. La technique du profilage pourrait renforcer le manque d'uniformité des règles du jeu entre les sociétés et les consommateurs. L'exploitation de cette asymétrie peut donner lieu à de sérieuses inquiétudes concernant la protection des consommateurs lorsque des produits nocifs sont offerts à des consommateurs vulnérables, y compris les enfants.

**Protection des renseignements personnels.** La protection des renseignements personnels des consommateurs dans le contexte des paiements mobiles est solidement établie en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Il semble toutefois que les consommateurs ne soient généralement pas au courant des stratégies de profilage utilisées sur le marché des paiements mobiles. Selon les données disponibles, les consommateurs sont de plus en plus à l'aise avec la notion de profilage dans le contexte du commerce électronique. Cependant, il semble que ce ne soit pas le cas pour le profilage associé aux appareils mobiles, qui comprend la géolocalisation : la plupart des consommateurs ne sont pas à l'aise avec cette pratique à l'heure actuelle. ***Dans un premier temps, on pourrait informer les consommateurs du profilage axé sur les***

***appareils mobiles afin de rendre cette pratique généralement plus transparente. Dans un deuxième temps, on pourrait les informer de leurs droits liés au profilage et des façons de changer les préférences sur leurs appareils mobiles.***

**Maliciels.** À court terme, la protection des consommateurs contre les menaces attribuables à des maliciels est insuffisante, ce qui peut présenter un risque de vol d'identité et de fraude pour ceux-ci. Les téléphones mobiles exposent les consommateurs à un plus grand risque de vol d'identité et de fraude dû à des maliciels et à d'autres formes de logiciels malveillants qui contreviennent à la sécurité sans que l'utilisateur le sache ou y consente. À l'heure actuelle au Canada, les consommateurs ne sont pas pleinement protégés contre les menaces attribuables à des maliciels. Des mécanismes de protection sont prévus dans une certaine mesure par le *Code criminel*, la *Loi sur la concurrence* et d'autres lois. Pour mieux régler les questions liées à la sécurité des paiements mobiles et à la protection des renseignements personnels au Canada, une loi anti-pourriel et la réglementation afférente élargiront la portée des dispositions de la *Loi sur la concurrence* concernant le marketing faux et trompeur aux messages électroniques. ***Lorsqu'elle sera en vigueur, la loi anti-pourriel pourrait constituer une base solide pour contrer ces menaces. Entre-temps, la meilleure approche pour atténuer les risques consiste à sensibiliser davantage les consommateurs aux menaces que posent les maliciels et aux meilleurs moyens de se protéger.***