Briefing Note to the Standing Committee on Finance
41st Parliament, 2nd Session

Mobile Payments and Consumer Protection in Canada- Executive Summary

Financial Consumer Agency of Canada
Lucie Tedesco, Commissioner
February 27, 2014

This is a summary. To read the research report in its entirety, see:
http://www.fcac-acfc.gc.ca/Fra/ressources/rechercheSondages/Documents/FCAC_Mobile_Payments_Consumer_Protection_accessible_FR.pdf

The introduction of mobile payments (m-payments) could have an impact on Canadian financial consumers. The consumer protections that apply to m-payments depend on the source of funds and the type of firm(s) providing the service. Since m-payments attract a variety of service providers, the consumer protection obligations vary across the market. As a result, not all m-payments in Canada are protected equally. By bringing a new medium as well as new business models and participants into the market, m-payments could pose new risks for consumers and could alter the application of the existing consumer protection framework.

Risk of uneven protection. M-payments involve a number of industries acting together. Inconsistencies in the consumer protection framework result when obligations differ according to the type of entity offering a product or service. In certain member countries of the Organisation for Economic Co-operation and Development, there has been a call for minimum consumer protection standards to apply to all m-payment sources. ***It would be beneficial for policy makers in Canada to further consider implementing minimum consumer protection standards that would apply uniformly across the m-payments ecosystem.***

In a number of jurisdictions outside Canada, legislation has been written that applies to financial institutions and "other entities"; the result is that all providers are subject to the same obligations. Our analysis indicates that Canadian consumers would be likely to benefit from regulation that is inclusive of all m-payment service providers regardless of the type of entity, and that is harmonized across Canadian jurisdictions. More evidence may be required to initiate such a policy reform. It will be important to monitor the business practices of the differing entities to assess the consumer protection practices of all participants**.** Such monitoring will provide evidence about the degree to which the gaps in the Canadian consumer protection framework are problematic for consumers, and the way these gaps can best be addressed.

Disclosure risks. Our analysis indicates that, while all the issuers of sources of funds are required to provide a contract or an agreement to terms, not all are subject to the same level of disclosure requirements. Canadian regulations also do not require disclosure to be optimized for mobile devices. These devices are well suited to providing mechanisms such as just-in-time disclosures, dashboards for reviewing disclosure settings, and icons that signal when an application is collecting geo-tracking data. ***Canadian policy makers are invited to consider whether it is appropriate for service providers to be required to disclose terms of agreement and privacy policies in a manner that is optimized for mobile***

devices and that is consistent across the market.

Risks of fraud and misuse of consumer assets. Ambiguity could arise around the application of zero-liability provisions if personal identification numbers are not required to secure mobile devices or authenticate payment. Generally, existing Canadian obligations provide a good foundation for protecting consumer assets against liability for fraud and misuse. However, modifications or further commitments may be required to ensure that the consumer protections remain technologically relevant and appropriate given the introduction of new media and intermediaries. ***Further monitoring and policy analysis is required to determine whether legislative reforms are required to address potential ambiguities, such as those related to liability for loss.***

The addition of fraudulent charges to mobile phone bills by third parties ("cramming") has been identified as a risk in Canada and many other jurisdictions. The introduction of the Wireless Code in December 2013 will further clarify the responsibilities of service providers and consumers related to cramming and other direct-to-carrier billing practices. ***The Code will require the clear disclosure of third-party charges on a bill, along with information outlining the processes for blocking such charges. It will also require that consumers have access to a clear and consistent process for complaints handling and redress.***

There appears to be a gap in the framework related to the risks associated with mobile wallets based on Near Field Communication (NFC) technology. Security of payment credentials on a mobile device is a major concern for consumers; it is therefore significant that m-payment providers do not have specific obligations related to the use of this technology. The *Canadian NFC Mobile Payments Reference Model* may provide a level of security to m-payment users who access funds issued by a participating financial institution. However, compliance with the Reference Model is voluntary and is not enforced by an oversight agency.

Responsibility for dispute resolution. It is an important principle that consumers should have access to dispute resolution and redress mechanisms. Our analysis indicates that this principle is inconsistently applied to m-payments in Canada since obligations vary by service provider. From experiences in other countries, it appears that consumers would benefit from having all m-payments equally protected; in such a situation, consumers would not be at a disadvantage when settling disputes. This is especially relevant with the type of multi-party business models prevalent in the m-payments ecosystem. Canada has no legislation that appoints a single party to communicate procedures to consumers, and to act as a point of contact for ensuring appropriate redress. It may be necessary to prescribe rules to providers in the m-payments market and to assign clear responsibility for dispute resolution. ***Policy makers might consider which service providers are best positioned to undertake this central, point-of-contact role in Canada.***

Financial consumer education. For a protection regime to be effective, consumers must be knowledgeable about their rights and responsibilities. Knowledgeable consumers are empowered and better able to make informed decisions. Informed consumers are likely to be better prepared to identify key information within disclosure statements and to seek out resources that will help them to

understand complex information. FCAC is currently developing material on this topic for Canadians, including information and tips on protecting financial information when doing online banking and making mobile payments, filing a complaint about an m-payment or a wireless service provider, and who to contact after experiencing a problem with an m-payment or online banking transaction. This information will be available on FCAC's website (http://www.fcac-acfc.gc.ca/Eng/Pages/home-accueil.aspx) by the end of March, 2014.

Profiling. Evidence from the United States and other jurisdictions indicates that service providers are selling user data to third-party marketers, who then target consumers with advertising based on demographic, behavioural and geographic information. Known as profiling, this technique involves aggregating large amounts of consumer data and mining it to predict and shape consumer behaviour. Profiling could reinforce the uneven playing field between corporations and consumers. The exploitation of this asymmetry can lead to significant consumer protection concerns when harmful products are marketed to vulnerable consumers, including children.

Privacy. There is a good foundation for the protection of consumers' privacy in the context of m-payments under the *Personal Information Protection and Electronic Documents Act*. However, it is apparent that consumers are not generally aware of the profiling strategies used in the m-payments ecosystem. While evidence suggests that consumers are increasingly comfortable with profiling in e-commerce, it appears that this is not the case when it comes to profiling on mobile devices that includes geo-tracking: generally, consumers are uneasy about this practice at present. ***A first step may be to inform consumers about mobile profiling to make the practice generally more transparent. A second step could be to inform consumers of their rights related to profiling and the ways to change the preferences on their mobile devices.***

Malware. In the near term, there may be a gap in consumer protection from malware threats, which can place consumers at risk of identity theft and fraud. Mobile phones expose consumers to greater risk of identity theft and fraud from malware and other forms of malicious software that breach security without the user's knowledge or consent. Consumer protections against malware threats are not comprehensive in Canada at present. These are addressed, to a certain extent, via the *Criminal Code,* the *Competition Act* and other legislation. To further address matters related to security and privacy of m-payments in Canada, pending anti-spam legislation and accompanying regulations will extend *Competition Act* provisions concerning false and misleading marketing to electronic messages. ***When it comes into force, the anti-spam legislation could provide a solid foundation for addressing these threats. In the meantime, the best approach to mitigate the risks is to make consumers more aware of malware threats and the ways they can best protect themselves.***