



Financial Consumer
Agency of Canada

Agence de la consommation
en matière financière du Canada

Mobile Payments and Consumer Protection in Canada

Steve Trites, Charles Gibney and Bruno Lévesque

Research Division, Financial Consumer Agency of Canada

December 2013

Canada 

The Financial Consumer Agency of Canada's Research Division is responsible for monitoring and evaluating trends and emerging issues that may impact consumers of financial products and services. FCAC research papers are theoretical or empirical works in progress. The views expressed in this paper are those of the authors. Responsibility for these views should not be attributed to FCAC.

Table of Contents

Executive Summary	6
Acknowledgements	9
1. Introduction	10
1.1. Mobile payments: the basics	11
1.1.1. Customer-to-business m-payment model	12
1.1.2. Peer-to-peer m-payment model	14
2. The Canadian landscape	16
2.1. Lessons learned from international jurisdictions	17
2.2. Ecosystem cooperation	19
2.3. Key industry participants	20
2.3.1. Banks	21
2.3.2. Mobile network operators	21
2.3.3. Credit card network operators	22
2.4. Auxiliary participants	22
2.4.1. Non-bank prepaid issuers	22
2.4.2. Mobile wallet issuers	23
3. Framework for analysis	25
3.1. Financial consumer protection principles	25
3.2. Applying protection principles to m-payments	26
3.2.1. Disclosure and transparency	27
3.2.2. Protection of consumer privacy	28
3.2.3. Protection of consumer data	30
3.2.4. Protection of consumer assets against fraud and misuse	31
3.2.5. Complaints handling and redress	33
4. Analysis of consumer protection and m-payments in Canada	34
4.1. Consumer protection framework	34
4.2. Disclosure and transparency obligations	35
4.2.1. Disclosure—bank-issued credit cards	35

4.2.2.	Disclosure—bank-issued debit cards	36
4.2.3.	Disclosure—new bank product or service	37
4.2.4.	Disclosure—credit cards issued by non-FRFIs	39
4.2.5.	Disclosure—debit cards issued by non-FRFIs	39
4.2.6.	Disclosure—companies offering direct-to-carrier billing	40
4.2.7.	Summary of disclosure obligations.....	41
4.3.	Protection of consumer privacy.....	43
4.3.1.	Addressing risks associated with privacy disclosure	43
4.3.2.	Addressing privacy risks.....	45
4.3.3.	Summary of privacy protection	46
4.4.	Protection of consumer data from malware	46
4.4.1.	Pending anti-spam legislation.....	47
4.4.2.	Summary of protection against malware threats.....	48
4.5.	Protection of consumer assets against fraud and misuse.....	48
4.5.1.	Protection against fraud and misuse—bank-issued credit cards	49
4.5.2.	Protection against fraud and misuse—debit cards	49
4.5.3.	Assessing protection of consumer assets against fraud and misuse	49
4.6.	Complaints handling and redress	51
4.6.1.	Complaints handling and redress—bank-issued credit cards	51
4.6.2.	Complaints handling and redress—bank-issued debit cards	51
4.6.3.	Complaints handling and redress—direct-to-carrier billing.....	52
4.6.4.	Assessing protection related to complaints handling and redress.....	52
4.7.	Summary of protection of data and assets, and protection against fraud	52
5.	Conclusions	54
5.1.	Uneven protection of financial consumers.....	54
5.1.1.	Minimum standards.....	54
5.1.2.	Regulating non-bank entities.....	55
5.1.3.	Monitoring business practices.....	55
5.2.	Disclosure.....	56

5.3.	Clarifying liability against fraud and misuse	56
5.4.	Assigning responsibilities within the ecosystem	57
5.5.	Financial consumer education	57
5.5.1.	Profiling	58
5.5.2.	Malware	58
5.5.3.	Informing consumers	58
	References.....	59

Executive Summary

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 underlying 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 ecosystem. 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. The m-payments ecosystem involves 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. Since variation exists across the ecosystem, it will be important to monitor the business practices of the differing entities for the purpose of assessing the consumer protection practices of all participants. Monitoring of this type 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 ecosystem.

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 ecosystem 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.

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.

Acknowledgements

Numerous colleagues and organizations assisted with the development of this research report. The authors particularly thank the following:

- Professor Michael Deturbide of the Schulich School of Law at Dalhousie University
- William Knight of Hebb, Knight and Associates
- Professor Michael Geist of the Faculty of Law at the University of Ottawa
- Professor Teresa Scassa of the Faculty of Law at the University of Ottawa
- the Canadian Payments Association
- Industry Canada's Office of Consumer Affairs
- the Department of Finance Canada
- the Canadian Radio-television and Telecommunications Commission
- the Office of the Privacy Commissioner of Canada
- the Canadian Bankers Association
- the Bank of Canada
- PayPal Canada
- the U.S. Consumer Financial Protection Bureau;
- the Organisation for Economic Co-operation and Development
- the Consultative Group to Assist the Poor.

1. Introduction

The primary objective of this report is to identify the extent to which financial consumers in Canada are protected when making mobile payments (m-payments). Our analysis indicates that m-payment users in Canada are not protected equally. In Canada, the consumer protections applying to m-payments are dependent on two factors: the underlying source of funds and the type of entity offering the service or product. Since m-payments attract a variety of service providers, the consumer protection obligations vary across the ecosystem. Further, the emergence of this type of payment in the market introduces a number of new elements, with implications for the risks to consumers and the way the existing consumer protection framework is applied.

M-payments are evolving quickly in Canada. Many observers expect m-payments to be widely adopted in the country over the near term. The Financial Consumer Agency of Canada (FCAC) is monitoring the evolution of these payments for their potential impact on consumer protection. FCAC's interest in monitoring mobile payments is twofold. First and foremost, FCAC is responsible for supervising federally regulated financial institutions (FRFIs) and payment card network operators. The Agency seeks to ensure that these entities comply with the federal consumer protection measures to which they are subject, and the voluntary codes of conduct and public commitments into which they have entered. It is important for FCAC to keep abreast of new offerings from the financial institutions and the network operators so that it can assess the potential protection implications for financial consumers. Second, under its research mandate, FCAC is monitoring the m-payments ecosystem more broadly to support the Agency's consumer education and financial literacy objectives.

The report is organized as follows:

- Section 1 defines m-payments and describes the differences between customer-to-business (C2B) and peer-to-peer (P2P) m-payments.
- Section 2 discusses factors suggesting that Canada may be well positioned for the successful introduction of m-payments. It also presents the types of major participants and business models in Canada.
- Section 3 explores the consumer protection concerns related to m-payments and outlines a framework for analysis.
- Section 4 analyzes the current consumer protection regulatory framework and considers whether it addresses the emerging risks associated with m-payments.
- Section 5 discusses the key findings.

Where appropriate, the research draws on examples from other countries. For a more thorough account of the developments related to m-payments in other jurisdictions of relevance to Canada, consult *International Review: Mobile Payments and Consumer Protection*, a complementary research report posted on the FCAC website (fcac.gc.ca).

All monetary amounts in this report are in Canadian dollars, unless otherwise indicated.

1.1. Mobile payments: the basics

A mobile payment is a transaction for which the payer uses a mobile device instead of a more traditional payment method, such as cash, cheque, or credit or debit card (Au & Kauffman, 2008). The Organisation for Economic Co-operation and Development (OECD, 2012) defines m-payments as follows:

Mobile payments are payments for which payment data and instruction are made via mobile phones or other mobile devices. Such payments would include Internet payments using a mobile device, as well as payments made through mobile network operators (MNOs). Note that the location of the payer and supporting infrastructure is not important: the payer may be on the move (remote payments) or at a point of sale.

In addition, the OECD considers m-payments to be a subset of electronic commerce (e-commerce):

E-commerce refers to orders for goods or services which are made and confirmed electronically via the Internet (i.e. online) or via other electronic platforms (such as those operated by mobile network operators). Payments for such goods and services can be made by various means including electronically, or by cheque, cash, or phone (using a payment card or other payment means).

M-payments can be made either remotely or in person (Juniper Research, 2011). If the payer is in a different location from the payee, the transaction is a remote payment. Money transfers between individuals through text messages and payment for downloaded digital content through a telephone bill (direct-to-carrier billing) are considered remote payments. Conversely, if the payer is present in person at the same location as the payee, the transaction is an in-person or point-of-sale payment.

M-payment funds can be accessed as “proxy” or “proximity.” Proxy payments for goods and services are made using merchant-specific applications that designate the payer’s mobile device as a proxy credit card account; examples include payments of parking fees, public transportation charges and coffee shop purchases. Proximity payments are made using mobile applications that access funds directly via payers’ accounts at financial institutions and credit card companies—for example, Visa, MasterCard and Google Wallet (Dahlberg, Mallat, Ondrus, & Zmijewska, 2006; Kim, Mirusmonov, & Lee, 2010; Task Force for the Payments System Review, 2011).

M-payments are emerging worldwide. The number of global m-payment transactions was 4.6 billion in 2010 and is projected to increase to over 15 billion in 2013 (Capgemini; Royal Bank of Scotland; EFMA, 2011). Widespread adoption of m-payments requires a ubiquitous, secure ecosystem of payment technology, as well as consumers who choose to use the technology instead of other, more established forms of payment (Au & Kauffman, 2008).

1.1.1. Customer-to-business m-payment model

Figure 1, developed by Liu and Zhuo (2012), shows a simplified model¹ for customer-to-business m-payments. As depicted in the figure, mobile represents an alternative to the more well-established electronic C2B payment devices, notably payment cards and computers. Mobile devices provide greater flexibility to consumers because they enable both remote and point-of-sale payments. Depending on the nature of the transaction and the type of payment application being used, m-payment can be made through a contactless point-of-sale technology such as Near Field Communication (NFC), a cellphone number through text messaging, a mobile Web browser or other technology.

¹ This figure illustrates the C2B model. It is not intended to depict the entire range of players and technologies within the Canadian ecosystem.

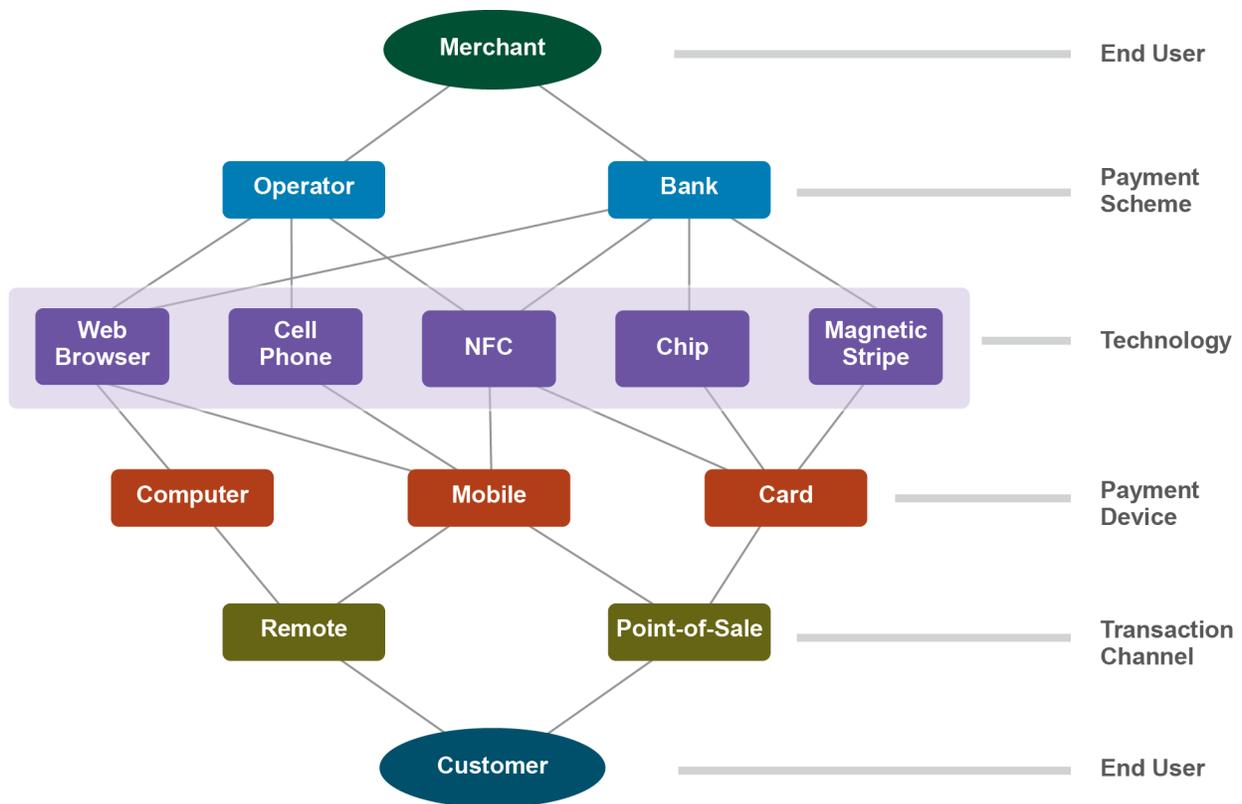


Figure 1: The C2B m-payment model (Liu & Zhuo, 2012)

The C2B model identifies the “payment scheme,”² which represents the source of funds for a given transaction. In the “operator” scenario, the consumer makes a payment via funds accessed through a third-party operator. In the “bank” scenario, a payment is made via funds accessed through a financial institution. In the operator scenario, there can be different types of payment intermediaries, including a mobile network operator such as Bell or Rogers, or a non-bank third party such as PayPal. The operator-centric payment scenario can be further subdivided into a number of payment options, such as prepaid (that is, drawing on stored value) or billing (that is, direct-to-carrier billing). It can include credit cards and other payment means. The bank-centric payment scenario is the predominant approach to m-payments in Canada at present. It includes payments made via deposit accounts held at financial institutions and payments made via credit cards issued by financial institutions (Liu & Zhuo, 2012).

² The use of the term “scheme” is generic here. It should not be confused with its other common application, which is as a synonym for “payment card network.”

Liu and Zhuo explain:

A Starbucks gift card uses a prepaid merchant-driven operator-centric payment model. Octopus Card, [used in] Hong Kong's subway system, also deploys a prepaid operator-centric payment model in which customers pre-store value in their card or mobile phone and tap the handset device when going into the subway system. An example of a [direct-to-carrier] billing system would be purchasing digital content with Rogers On Demand or subscribing to magazines with Rogers—the amount will be paid to Rogers through phone bills.

1.1.2. Peer-to-peer m-payment model

Peer-to-peer payment in Canada is used for a number of purposes: generally, for gifts, personal debt repayment, bill splitting, or remittances to friends or family. Traditionally, Canadians have relied on cash and cheques to make P2P payments, and on money services businesses such as Western Union for remittances. Online P2P payments, through services such as *Interac* e-Transfer and PayPal, are emerging as an alternative to the more traditional options. Electronic P2P payments account for less than 1 percent of payments in Canada but the proportion is growing rapidly (Canadian Payments Association, 2012).

P2P m-payments are an extension of online P2P payments. In their most basic form, they involve a text message received by a mobile device user, giving notification of an electronic transfer. As mobile device technologies evolve, more innovative approaches are emerging. These include options such as transferring funds between two mobile devices through Bluetooth technology or “tapping” two NFC-enabled mobile devices together. The transactions resulting from these options follow the same pathway shown in Figure 1 (page 3), with the exception that the merchant is replaced by another customer. Essentially, this is a mobile transaction pathway between two consumers.

P2P m-payments are only beginning to be adopted in Canada, and data specific to their use is therefore scarce. According to an estimate by MasterCard Worldwide, only 3 percent of Canadians have used P2P m-payments but 14 percent said they would be willing to use these services (MasterCard Worldwide, 2012). A report by Deloitte (2012) suggests that consumers who make domestic and international remittances are the Canadian users most likely to adopt P2P m-payments, since these services tend to be less expensive than traditional wiring options.

P2P m-payments have been most widely adopted in developing economies, where they have been a transformative technological advance for the large proportion of the population that is unbanked (Jun, 2011). In Kenya, for instance, mobile network operator Safaricom runs a service known as M-PESA; this enables consumers to deposit or withdraw cash and send money through text messages that are linked to a network of agents and automated teller machines (ATMs). M-PESA also enables consumers to buy goods and services with their mobile phones (Jun, 2011). This business model is now being adopted in a number of developing countries as a means of providing financial inclusion to the unbanked. In Canada, the model is not likely to be adopted to the same extent because the banking sector is well established and the unbanked make up a small proportion of the population.

2. The Canadian landscape

Canada appears to be well positioned for successful adoption of m-payments. Mobile service is available in nearly every location in the country and most Canadians own a mobile device (Canadian Wireless Telecommunications Association, 2012). The mobile penetration rate is 100 percent among 15- to 64-year-olds³ (MasterCard Worldwide, 2012). In addition, Canadians increasingly rely on their mobile devices for daily activities, such as reading and watching the news, social networking, and using search engines (comScore, 2012).

Canada ranks close to the top (second out of 34 markets) on the MasterCard Mobile Payment Readiness Index, which assesses the readiness for m-payment adoption in international jurisdictions. Among Canada's strengths, the index identifies high Internet penetration; the quality and penetration of financial services; and the level of cooperation between banks, mobile networks and government in developing the m-payments ecosystem (MasterCard Worldwide, 2012).

Because the m-payments ecosystem is still emerging, Canadian m-payment usage statistics are scarce. However, statistics on a number of related behavioural indicators support the view that Canadian consumers are becoming increasingly ready to adopt m-payments. First, Canadians are the heaviest users of the Internet in the world, averaging over 45 hours per month online—nearly double the international average (comScore, 2012).⁴ Second, the websites most popular with Canadians are sites related to personal finance, including online banking sites. More than 6.7 million Canadians pay bills online and more than 6 million make account inquiries online (comScore, 2012).

Stratifying mobile behaviour by demographic group provides further insights into which Canadians are more likely to be early adopters of m-payments. Data from the United States indicates that young people, in particular, are early adopters of m-payments since they value speed, ease, efficiency and convenience in transactions, are very comfortable with technology, and have already demonstrated a preference for mobile donations and other mobile transactions (Barton, Fromm, & Egan, 2012). It is a reasonable assumption that Canadian youth would demonstrate many of the same characteristics as their American neighbours. Further, a recent internal FCAC study indicates that young Canadians of Chinese and South Asian backgrounds are among the heaviest users of mobile devices, with most of them downloading mobile content and using text messaging. The same study found that urban Aboriginal Canadians are also above-average users of text messaging.

³ This proportion can be compared to that of international leaders in mobile penetration: the U.K. (197 percent), Germany (192 percent), and the United States (134 percent) (MasterCard Worldwide, 2012).

⁴ The comScore data specifically refers to “fixed” Internet access, such as through a desktop or laptop computer, as opposed to accessing the Internet via a mobile device.

In addition, the attitudes of Canadians are becoming well aligned with m-payment adoption. Quorus Consulting Group Inc. conducts the annual *Cell Phone Consumer Attitude Study* on behalf of the Canadian Wireless Telecommunications Association (CWTA). The 2012 results indicate that, overall, 24 percent of mobile phone users in Canada are interested in making a point-of-sale m-payment, an increase from 18 percent in 2011 (Quorus Consulting Group Inc., 2012). When the attitudinal results are stratified, it is apparent that those with the highest level of interest in making m-payments are younger mobile users (38 percent for 18- to 34-year-olds), men (29 percent compared to 21 percent for women), those who do not have a land line but use a mobile device as their main phone (38 percent) and those who use a smartphone⁵ (38 percent, as compared to 16 percent for regular cellphone users) (Quorus Consulting Group Inc., 2012).

There is widespread optimism that the growing market adoption of e-commerce, combined with the increasing market penetration of mobile phones, will create the market conditions for mass adoption of m-payments in Canada and worldwide. Despite this, consumers in jurisdictions that are comparable to Canada have yet to adopt m-payments in significant numbers (Ondrus, Lyytinen, & Pigneur, 2009). For instance, in 2010 there were only 7.1 million m-payment users in Western Europe, compared to 62.8 million users in the Asia-Pacific region (King & Jessen, 2010). After more than a decade of trials and pilot projects, regulatory agencies in jurisdictions such as the European Union and the United States face the key question of how they can best facilitate consumer adoption of m-payments and encourage the growth of the m-payments ecosystem (Montgomery, 2012).

2.1. Lessons learned from international jurisdictions

What we see in Asia and the developing world indicates that user adoption rates have been highest in jurisdictions where m-payment technology has allowed an underserved population segment to access financial services. According to KPMG International (2007), the impetus for the development of the m-payment channel in Japan was created by an acute shortage of convenient and legal short-term credit (KPMG International, 2007). When the government recently began easing restrictions on revolving credit, new financial institutions emerged to meet demands of underbanked consumers. In South Korea, the underserved segment of the population providing the initial impetus for the surge of m-payments consisted of young people who had no access to credit cards and needed a cashless way to make payments for music and video content, computer games, applications, etc. (KPMG International, 2007).

⁵ A smartphone is “a mobile phone that is able to perform many of the functions of a computer, typically having a relatively large screen and an operating system capable of running general-purpose applications” (Oxford University Press, 2013).

Kenya's M-PESA is one of the world's most successful mobile money brands. The country's over 40 million people live primarily in rural regions and are almost entirely unbanked; only 4 percent of adults have an account at a financial institution (World Bank, 2012). However, the penetration rate of mobile devices is above 75 percent (iHub Research; Research Solutions Africa, 2012). Safaricom is Kenya's largest mobile network operator and controls 80 percent of the market (Jack & Suri, 2011). In 2007, it launched M-PESA as a method for urban Kenyans to send money home to relatives in rural areas—a form of urban-to-rural remittance that had previously been underserved (Veniard & Goss, 2012). Since financial systems are underdeveloped across much of the developing world, the M-PESA approach is widely viewed as a model to be emulated in other developing economies (Jack & Suri, 2011; Lachal & Zhang, 2012).⁶

While markets in Canada differ from those in these Asian and African examples, a service provider could acquire a significant market share in Canada by providing services to an underserved segment of the population. As we will discuss, the collaborative business models involving banks, mobile network operators and credit card networks give those institutions the potential to be the initial leaders in the m-payments ecosystem in Canada. It is possible that the majority of m-payment services will be extensions of current banking services to current customers. It may well be that non-bank service providers are better positioned to identify a financial services gap among underserved Canadians.

⁶ For a more complete discussion of m-payments in these international jurisdictions, see the research paper *International Review: Mobile Payments and Consumer Protection* on the FCAC website.

Based on the factors that have led to adoption in these international jurisdictions, financially underserved consumers could be among the early adopters in Canada. For example, young Canadians under the age of 18 cannot access their own credit cards, which may limit their abilities to make remote m-payment purchases. Precisely this youth demographic in South Korea was first to adopt remote m-payments using direct-to-carrier billing, which did not require issuing credit to minors (KPMG International, 2007). Credit card access is also disproportionately lower among the lowest-income households (70 percent) than among Canadian households overall (89 percent) (Robson, 2011). Generally, the proportion of Canadians who are “banked” is quite high. Approximately 96 percent of Canadian adults are estimated to have a bank account (Demirguc-Kunt & Klapper, 2012). However, rates are disproportionately lower among the lowest-income Canadians (91 percent) (Demirguc-Kunt & Klapper, 2012). Another recent study estimates that the rate of unbanked Canadian adults is as low as 1 percent (Arrowsmith & Pignal, 2010) but is disproportionately higher among Aboriginal Canadians, refugees and low-income individuals (Robson, 2011). It is noteworthy that there is considerable overlap between these underserved groups and groups that are more comfortable with technology and self-identify as likely early adopters of m-payments. As a result, youth, urban Aboriginal Canadians and young Asian Canadians are among the population segments that might be more likely to be early adopters of m-payments in Canada.

2.2. Ecosystem cooperation

One of Canada’s identified strengths is the cooperation between key players in the Canadian m-payments ecosystem. For example, many Canadian financial institutions worked together to develop the *Canadian NFC Mobile Payments Reference Model*, which is a set of voluntary guidelines aimed at ensuring a safe, secure and easy-to-use network for consumers and merchants (Canadian Bankers Association, 2012 a). Established to follow up on a recommendation of the Canadian Task Force for the Payments System, the Reference Model found a consensus on Near Field Communication as the technology of choice for point-of-sale m-payments in Canada.⁷

⁷ This is not intended to suggest that all m-payment offerings in Canada will be based on NFC. The technology is currently used for contactless debit and credit card transactions, and is the basis for many of the bank-led initial point-of-sale m-payment services in Canada. However, it remains to be seen what the dominant technology will be in Canada over the long term.

For m-payment use, NFC technology requires integration of hardware and software on the mobile device. To make a point-of-sale proximity payment, a consumer needs to have an NFC-enabled smartphone. At present, there are only a few NFC-enabled smartphones available to Canadian consumers, but it is estimated that 80 percent of smartphones in Canada will be NFC-enabled by 2016 (Technology Strategies International, 2012). To date, nearly half (48 percent) of Canadian mobile users are already using smartphones rather than regular mobile phones. Smartphone adoption is particularly high among 18- to 34-year-olds (69 percent) (Quorus Consulting Group Inc., 2012). Approximately 200,000 merchants are estimated to accept NFC technology across Canada (EnStream, 2012). They include some of Canada's most successful retailers: Tim Hortons, Loblaws, Shoppers Drug Mart and many more.

2.3. Key industry participants

Much of the m-payment infrastructure development in Canada can be attributed to the leadership and collaboration shown by three major industries: banks, mobile network operators and the credit card network operators. The m-payment business model best positioned for success is a collaborative model, involving point-of-sale m-payment ventures formed between companies from these three industries (OECD, 2012). In 2012, Rogers and the Canadian Imperial Bank of Commerce (CIBC) launched an m-payment application that enables point-of-sale payments via a CIBC credit card. The thinking behind this approach is expressed in a recent Deutsche Bank report: "Successful business models will rest on strategic alliances ... this is because one company alone will not be in the position to serve the complete value chain as technology is too complex and knowledge about particular market segments is essential" (Dapp, Stobbe, & Wruuck, 2012). An interesting element of this type of collaborative approach is that each "service provider has an interest in earning revenue from its relationship with the end-user" (Infineon, 2012).

Following is an overview of the three primary industries currently involved in the m-payments ecosystem in Canada: banks, mobile network operators and credit card network operators.

2.3.1. Banks

Banks play a number of roles in the m-payment supply chain. They facilitate account withdrawals and transactions by credit card and prepaid card. In the near term, most m-payments will be funded through banks or bank-issued cards. Canadians are quickly adopting mobile banking applications, which banks began offering in 2010 (Canadian Bankers Association, 2012 b). Banks are now collaborating with partners from complementary industries to develop point-of-sale m-payment offerings (e.g., mobile applications, mobile wallets) that are either on the market or are expected to be in the near term. To date, there have been a number of active banks in the mobile ecosystem in Canada.⁸

2.3.2. Mobile network operators

Mobile network operators include Bell, TELUS, Rogers and others. They supply and activate consumers' hardware, such as mobile phones and SIM (subscriber identity module) cards; and they operate the wireless networks through which transaction communications flow (Budnitz, 2012). The operators have broad customer bases that stretch across the country, as well as a wealth of experience in providing subscriber acquisition and authentication, customer support, and value-added services (Contini, Crowe, Merritt, Oliver, & Mott, 2011). In the experience of countries that are further advanced in m-payment evolution than Canada (particularly Japan, South Korea and Kenya), mobile network operators have been the primary enablers of m-payments. In Canada, MNOs tend to partner with financial institutions and others to develop m-payment solutions that draw funds from existing payment mechanisms, such as credit or debit cards. Some MNOs have sought a stronger footing in the m-payments ecosystem. Rogers, for example, has applied for a Canadian banking licence.

Mobile network operators have also increased their direct-to-carrier billing services. In this form of remote m-payment, consumers purchase and download content for their mobile devices (for example, "apps" and ringtones) and are billed on their monthly MNO bill. As MNOs increase their direct-to-carrier billing services, there are major international companies in the background that enable direct-to-carrier transactions. One international industry leader is Bango. In 2012, Bango reported that it provided access to direct billing to more than 900 million customers worldwide through more than 90 mobile operators, including Canadian MNOs Bell, Rogers, TELUS and Virgin Mobile (Bango, 2012).

⁸ For example, CIBC was the first federally regulated financial institution to launch a mobile banking application, in 2010. It was the first to launch an NFC point-of-sale m-payment application, in November 2012. In 2013, Royal Bank of Canada announced that it was launching a cloud-based mobile wallet service.

2.3.3. Credit card network operators

The credit card network operators (such as Visa and MasterCard) are active developers of m-payment products and services, and are promoting their adoption in Canada and around the world. In 2011, the 74.5 million Visa and MasterCard credit cards in circulation in Canada accounted for over \$300 billion in retail purchases (Canadian Bankers Association, 2012 c). Visa and MasterCard have both recently adopted NFC technology in their contactless card payment products. A study by MasterCard indicates that its credit card users increase spending on their MasterCard by 30 percent per month when they adopt contactless payments (MasterCard Advisors, 2012). These card networks have also continued to promote the adoption of NFC technology for point-of-sale m-payments, and current Canadian NFC point-of-sale m-payment applications are available on both Visa and MasterCard credit cards. In contrast, American Express is focusing on technologies that are not NFC-based. In 2011, the company purchased a technology that relies on cellphone numbers for making point-of-sale m-payments, and in 2012 it launched Amex Sync, which allows users to make payments on Twitter and Facebook (American Express, 2013).

Credit card networks are also developing online and mobile wallet solutions that will enable their customers to access multiple, competing credit, debit and other payment options in one virtual location.

2.4. Auxiliary participants

The model of collaboration between banks, mobile network operators and card networks described in Section 2.3 is well positioned for success. However, it is not the only model emerging in Canada's m-payments ecosystem. This section describes the non-bank prepaid issuers and mobile payment application issuers that have the potential to be active in the m-payments ecosystem in Canada.

2.4.1. Non-bank prepaid issuers

Non-bank issuers provide gift cards, stored-value online accounts and other prepaid products. Prepaid accounts and cards can be used for various purposes, including payroll disbursement, tourism and travel (replacing travellers cheques), gifts, distribution of government benefits, micropayments (for example, mass transit or parking payments) and money transfers (The Wolfsberg Group, 2011). The value associated with a prepaid account or card can be recorded remotely and linked to a virtual account, as in the case of PayPal; or the value can be stored on a physical card, such as a prepaid coffee card not bearing a holder's name (The Wolfsberg Group, 2011). Prepaid offerings can further be classified based on whether they are "closed-loop" (for use only at a specific merchant) or "open-loop" (usable at multiple merchants), and whether or not they are reloadable.

Prepaid payment products that are issued by non-banks are projected to fund a relatively small proportion of m-payments in the near term, compared with bank accounts and credit cards (Budnitz, 2012). However, according to the Canadian Payments Association, the market for prepaid products is growing rapidly in Canada (Canadian Payments Association, 2012).

Since they are competing with financial institutions, non-bank prepaid issuers tend to seek innovative solutions that may rely on technologies other than those favoured by the partnerships between banks and mobile network operators. For instance, PayPal and other payment providers have opened their systems to outside software developers to promote the development of innovative payment solutions (Budnitz, 2012; Deloitte, 2012).

2.4.2. Mobile wallet issuers

Many technology-based entities are developing and providing online and mobile wallet applications. Prominent examples of these offerings are Google Wallet, Amazon Payments, PayPal and Square Wallet. For the most part, these companies provide user interfaces for accessing payment information for credit cards, debit cards, prepaid cards, membership programs, etc. Similar to the examples cited in the previous section, mobile wallet issuers tend to favour cloud-based,⁹ innovative technological approaches rather than relying on NFC (Crowe & Tavilla, 2012). In the cloud-based wallet model, “data and software are retrieved from remote servers using web-based tools and applications” (Crowe & Tavilla, 2012). The wallets are not dependent on a particular technology since the payment credentials are not stored on a mobile device (Crowe & Tavilla, 2012). This is a potential benefit to consumers because it allows for payments to be made from multiple devices and allows consumers to easily switch mobile phones or mobile network operators (Pernet-Lubrano, 2010). Since the ecosystem remains in a state of development, there is still the potential for cloud-based services, or something else, to become the dominant technology.

For example, the Square Wallet app in the United States identifies when a consumer carrying a smartphone loaded with the app enters a participating merchant’s location. The consumer’s name and picture appear on the merchant’s terminal and the consumer is given the option of making a hands-free payment that does not require use of the mobile device to complete the transaction (Crowe & Tavilla, 2012). PayPal has announced that its Beacon point-of-sale service, which employs Bluetooth technology to check customers in at a merchant location, will be available in Canada in the near term. In the United States, PayPal In-Store Checkout allows consumers to make a purchase at participating merchants simply by providing a mobile phone number and entering a personal identification number (PIN) (Crowe & Tavilla, 2012).

⁹ The cloud is a remote server where payment credentials are stored, instead of being stored on the mobile device itself.

It has been suggested that related business models might be able to monetize consumer data—a major driver for many e-commerce participants. According to this business model, mobile wallet issuers could sell user information to third-party marketers, who target advertising based on demographic, behavioural and geographic data (Grami & Schell, 2004). The targeting makes use of profiling, a marketing technique that involves aggregating large amounts of consumer data and mining it to identify previously unknown correlations with desired outcomes (Hildebrandt, 2008). From the data, consumer profiles are then generated based on a combination of demographic, behavioural and geographic characteristics that are associated with a probability of carrying out a desired outcome.

3. Framework for analysis

In this section, we first describe the principles of financial consumer protection and then consider the implications of introducing m-payments into Canada’s financial marketplace. Specifically, we consider the elements that are unique to m-payments and how these interact with Canada’s existing financial consumer protection framework.

3.1. Financial consumer protection principles

Financial consumer protection is intended to promote consumer confidence by reducing imbalances between financial institutions and consumers (Melecky & Rutledge, 2011). In 1998, the Task Force on the Future of the Canadian Financial Services Sector recommended the establishment of the Financial Consumer Agency of Canada based on evidence that “consumers and financial institutions do not have the same information, understanding or bargaining power, ... [and that] it is critical that consumers be treated fairly in their dealings with financial institutions” (Department of Finance, Canada, 1999). FCAC was established in 2001 to strengthen oversight of consumer protection measures and expand consumer education in the financial sector in Canada. In 2011, the Organisation for Economic Co-operation and Development developed a set of common, high-level principles on financial consumer protection, which were endorsed by the G20 finance ministers and central bank governors. These principles share common language and ideologies with the consumer protection principles upon which FCAC was established (Department of Finance, Canada, 1999).

The OECD document *G20 High-level Principles on Financial Consumer Protection* describes the principles that apply to our analysis of m-payments in Canada.¹⁰ Taken together, the OECD principles serve as a functional definition of financial consumer protection (OECD, 2011).¹¹

- **Disclosure and Transparency**—Financial services providers and authorized agents should provide consumers with key information that informs the consumer of the fundamental benefits, risks and terms of the product.

¹⁰ Principles have been taken verbatim from the OECD document. Much of the content has been omitted for the sake of conciseness. The order of the principles has also been adjusted.

¹¹ Four of the principles have been omitted since they fall outside the scope of this analysis: “Equitable and Fair Treatment of Consumers” is an overarching statement that is reflected throughout the other principles. “Legal, Regulatory and Supervisory Framework” positions financial consumer protection as an integral part of the regulatory framework. “Role of Oversight Bodies” outlines the responsibilities for oversight. “Competition” describes the importance of competition in enhancing innovation and maintaining high standards in the marketplace. For more information, refer to *G20 High-level Principles on Financial Consumer Protection*.

- **Protection of Consumer Data and Privacy**—Consumers’ financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should define the purposes for which the data may be collected, processed, held, used and disclosed (especially to third parties).
- **Protection of Consumer Assets against Fraud and Misuse**—Relevant information, control and protection mechanisms should appropriately and with a high degree of certainty protect consumers’ deposits, savings, and other similar financial assets, including against fraud, misappropriation or other misuses.
- **Complaints Handling and Redress**—Jurisdictions should ensure that consumers have access to adequate complaints handling and redress mechanisms that are accessible, affordable, independent, fair, accountable, timely and efficient.

Two other principles should be mentioned: responsible business practices and financial education. These are considered to be key elements of a financial consumer protection framework. While a comprehensive analysis of the business conduct of service providers is beyond the scope of this research, we are mindful of its importance in the ecosystem. Where appropriate, we refer to these two principles throughout the report:

- **Responsible Business Conduct of Financial Services Providers and Authorized Agents**—Financial services providers and authorized agents should have as an objective to work in the best interest of their customers and be responsible for upholding financial consumer protection. Financial services providers should also be responsible and accountable for the actions of their authorized agents.
- **Financial Education and Awareness**—Financial education and awareness should be promoted by all relevant stakeholders and clear information on consumer protection, rights and responsibilities should be easily accessible by consumers.

3.2. Applying protection principles to m-payments

The following sections discuss the principles of consumer protection as they relate to m-payments in Canada. We also identify consumer protection risks that emerge as a result of the introduction of m-payments.

3.2.1. Disclosure and transparency

The provision of an m-payment service (whether the payment originates from a bank, stored value or a credit card account) is typically governed by an agreement between the consumer and the service provider. The agreement includes both express terms (specifically set out in the agreement) and terms imposed by statute or common law. As in many standard form contracts, the terms of the agreement have the potential to favour the service provider at the expense of the consumer. Disclosure is the most important method of offsetting the asymmetry between financial institutions and financial consumers (OECD, 2010). Consistent and simple disclosure benefits consumers: it ensures that they are treated fairly by the service provider; it allows them to verify any fees charged or restrictions imposed by the service provider; and it enables them to compare prices and practices among competitors. When disclosure statements are consistent from one m-payment service provider to another, consumers are able to compare and choose the option that best fits their needs.

Disclosure of complex information on small screens. A potential risk to consumers relates to m-payment disclosure statements presented on mobile devices (OECD, 2008). The m-payments ecosystem is likely to require the disclosure of information that is relatively complex compared to more traditional payment products as a result of the multi-party, collaborative business models. In a statement before the U.S. House of Representatives Financial Services Subcommittee on Financial Institutions and Consumer Credit, Marla Blow of the Consumer Financial Protection Bureau indicated that consumers have become generally desensitized to electronic disclosure statements after years of bypassing them online with a single, uninformed click (Blow, 2012). She further explained that this phenomenon is likely only to be exacerbated by the limited capacity of a mobile device's relatively small screen.

As the OECD has stated, disclosure is an important method of offsetting the asymmetry between financial institutions and financial consumers. However, evaluations in various countries indicate that disclosure statements may have limited effectiveness when consumers do not read or understand them entirely (OECD, 2010). Disclosure statements could lose effectiveness as a result of the simultaneous increase in information complexity and the decrease in readability with the introduction of mobile devices.

The associated consumer risks include a decrease in consumers' knowledge and understanding of their rights and responsibilities in the event of a fraudulent charge, loss or theft of a device, or an error. This may expose consumers to losses of money, time and confidence in the m-payment system. Similarly, a consumer who does not fully read or understand the disclosure statement would be less likely to be knowledgeable about the fees to be charged and the restrictions to be imposed by the service provider, and that lack of knowledge could lead to patterns of use resulting in large, unexpected charges or other unforeseen outcomes (OECD, 2008).

3.2.2. Protection of consumer privacy

As noted in Section 2.4.2, 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 (Grami & Schell, 2004). Known as profiling, this technique involves aggregating large amounts of consumer data and mining it to identify previously unknown correlations with desired outcomes (Hildebrandt, 2008). From the data, consumer profiles are then generated that are associated with a probability of achieving a desired outcome.

Segmented advertising is not new in marketing, but profiling accesses very large amounts of data and enables companies to market directly to an individual consumer's mobile phone based on the applicable profiles. Mobile advertising is already a substantial source of revenue for technology companies. For instance, it is estimated that Google generated nearly US\$1.5 billion in U.S. mobile advertising revenues in 2012 (eMarketer, 2012). Figures for Canada are not readily available but, according to projections, the overall U.S. mobile advertising market will generate around US\$6.6 billion in 2014.

One of the primary ways in which m-payment profiling differs from more established online profiling techniques is in the mobile nature of the devices being used. For geo-targeted marketing to be effective, the consumer's movements must be tracked in real time (King & Jessen, 2010). The results of a survey of American consumers by Urban et al. (2012) indicate that consumers are generally not comfortable with receiving location-based advertising. More than 90 percent of respondents indicated that they either "definitely" or "probably" would not allow a provider to use their current location to tailor ads to them (Urban, Hoofnagle, & Li, 2012).

Risks of identity theft. Identity theft is a potential risk to consumers, associated with profiling and tracking. Identity theft involves the use of someone's personal information to commit fraud or other crimes (Government Accountability Office, 2012 a). Generally speaking, profiling is based on aggregates of consumer data that has been de-identified—that is, stripped of information allowing the identification of any one person who was a source (Scassa & Deturbide, 2012). However, fragments of de-identified data can be combined, making it possible to identify an individual (Scassa & Deturbide, 2012). The possibility of identifying an individual increases when profiles are combined with location tracking data and personal data stored on a mobile device, such as photos and contacts. Identity theft can lead to serious financial hardship for consumers. In a recent report on the economic impact of identity theft, the Royal Canadian Mounted Police (2013) cited research indicating that the incidence of identity crimes is increasing rapidly in Canada and internationally. According to an estimate based on 2007 data, 6.5 percent of Canadian adults were victims of identity fraud in that year and the victims spent more than \$150 million to resolve these issues (Sproule & Archer, 2008).

Risks associated with lack of transparency. A further risk to m-payment users relates to the potential for profiling to reinforce the uneven playing field between corporations and consumers (Hildebrandt, 2008). Consumers are typically unaware of the profiles to which they belong in marketers' databases; they are therefore unaware of the marketing strategies being implemented (King & Jessen, 2010). The resulting lack of transparency may lead consumers to act in ways that would not be normal for them if they possessed the same knowledge as the marketers. For example, profiling could be used to target vulnerable populations with promotions for unhealthy food, medications or high-interest consumer loans (King & Jessen, 2010).

Risks to children. The exploitation of this asymmetry can lead to significant consumer protection concerns when harmful products are marketed to vulnerable consumers, including children (King & Jessen, 2010). The OECD (2008) states that children are particularly vulnerable to marketing on mobile devices since they may not understand the marketing information presented to them. Marketing to children has been addressed in many jurisdictions in connection with e-commerce,¹² but not specifically in connection with mobile devices. According to the OECD, one exception is the U.K., which has banned the marketing of junk food via mobile devices to children (OECD, 2008).

Risks associated with a lack of privacy disclosure. Mobile devices generate a wealth of data. King and Jessen (2010) explain that this includes behavioural trails such as detailed histories of past calls, text messages and browsing, as well as mobile network operators' subscription data. Mobile devices store highly personal data, such as photos, contact lists, personal documents and payment credentials. The devices also generate geographic location data, from which it is possible to make inferences about and track a consumer's current location (King & Jessen, 2010). From a consumer perspective, mobile device users typically consider data generated and stored on mobile devices to be private information (Kamleitner, Dickert, Falahrastegar, & Haddadi, 2013; Urban, Hoofnagle, & Li, 2012).

Risks associated with privacy disclosure also have to do with the consumer's awareness of, and consent to, the practices of collection, use and storage of private information by a particular service provider. The U.S. Federal Trade Commission (FTC) reports a need for improved privacy disclosure statements because consumers are often unaware of which information is being collected via their mobile devices, and how that information is being used (Federal Trade Commission, 2013 a). Since consumers often are unaware of these practices, they tend not to look for opportunities to opt out of, or otherwise control their involvement in, the practices (Federal Trade Commission, 2013 a).

¹² The *Canadian Code of Practice for Consumer Protection in Electronic Commerce* establishes merchant benchmarks for good business practice related to disclosure of information, contract formation and fulfillment, online privacy, security of payment and personal information, redress, unsolicited emails, and communications with children (Working Group on Electronic Commerce and Consumers, 2004). This is a voluntary code of conduct.

One approach that the FTC promotes to mitigate the privacy disclosure risk related to m-payments is the adoption of “just-in-time” disclosures, whereby service providers inform consumers and obtain express consent (that is, consent given explicitly, either orally or in writing) at the “time when it matters to consumers, just prior to the collection” of private information (Federal Trade Commission, 2013 a). The FTC also promotes the use of “dashboards” so that consumers can regularly revisit the disclosure statements and easily see which applications have access to private information. In addition, the FTC promotes the use of icons that signal to consumers when an application is actively accessing information (Federal Trade Commission, 2013 a).

3.2.3. Protection of consumer data

The electronic nature of mobile phones exposes consumers to further risks of identity theft and fraud from malware and other forms of malicious software that breach security without the user’s knowledge or consent (Chari, Kermani, Smith, & Tassiulas, 2000). Malware is a broad term for malicious software applications that can be installed on mobile devices by third parties to steal data, damage the device or use it for unauthorized purposes. The value of data stored on and generated through mobile devices can be seen by the amount of new malware that specifically targets those devices. From 2010 to 2011, there was an increase of nearly 1,000 percent in the incidence of new malware strains targeting mobile devices (G Data SecurityLabs, 2011). In continuation of past trends, malware directed at mobile devices is expected to keep focusing mainly on mobile banking information (F-Secure, 2013).¹³

As the most popular operating system for mobile phones, Google’s Android has proven to be the most common target for malware. A recent study estimates Android’s share of mobile malware to be approximately 79 percent (F-Secure, 2013). One study of limited scope managed to collect 1,200 samples of Android malware between August 2010 and October 2011. Perhaps the most disturbing finding from this study was the relative ineffectiveness of malware detection software: the best mobile security software found only 79.6 percent of malware, while the worst caught a mere 20.2 percent (Zhou & Jiang, 2012).

¹³ Common forms of banking malware trick users into divulging their bank account number and login information, as well as a mobile phone number, on a malicious website. The malware then intercepts temporary passwords that are sent by banks via text messages.

A 2012 report by the U.S. Government Accountability Office (GAO) indicates that a number of key security controls¹⁴ can be implemented on mobile devices to combat common threats and vulnerabilities, but many of these depend on the active participation of users. While mobile device security is a major concern for consumers, they are generally uninformed when it comes to actively securing their own devices, with the result that security measures are inconsistently implemented (Government Accountability Office, 2012 b). The GAO also reports that, according to a recent survey of American consumers, more than half of respondents believed they required more information before they could implement security measures on their mobile devices. The report concludes that, for mitigating security risks, education is critical to raise awareness among consumers who use mobile devices (Government Accountability Office, 2012 b).

3.2.4. Protection of consumer assets against fraud and misuse

The electronic nature of point-of-sale m-payments gives rise to other risks of fraud and misuse of assets. However, the perception of these risks may tend to be greater than the reality.

NFC-based mobile wallet fraud risks. For the present and near future, most point-of-sale m-payments in Canada are likely to employ NFC as a result of the industry's commitment to that technology. Since the recent transition to chip-and-PIN technology, Canada has seen a decrease in the incidence of credit and debit card fraud, as well as the associated losses (Canadian Bankers Association, 2012 d; King D. , 2012). NFC point-of-sale m-payments are estimated to be as secure as chip-and-PIN card transactions (Smart Card Alliance, 2011). NFC point-of-sale m-payment platforms make use of an encrypted chip called a Secure Element. This is a tamper-resistant chip that stores the user's information (e.g., PIN, card and account credentials, transaction histories). The Secure Element is separate from the mobile device's operating system, hardware and memory, and is designed to permit only trusted payment applications, running on the same mobile device, to access the user's information (Ghag & Hegde, 2012). In Canada, industry partners have collaborated on a uniform approach to securing consumer credentials. EnStream, a joint venture between the largest mobile network operators (Bell, Rogers and TELUS), has selected BlackBerry Limited to provide a Secure Element manager for NFC-enabled smartphones in Canada.

¹⁴ The key controls include: enabling user authentication; enabling two-factor authentication for sensitive transactions; verifying the authenticity of downloaded applications; installing anti-malware; installing a firewall; receiving prompt security updates; enabling remote disabling of lost or stolen devices; enabling encryption for data stored on devices or memory cards; and enabling whitelisting. For definitions of each of these terms and a more detailed discussion, see the GAO report entitled *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged*.

The risks are relatively minor that consumers will be subjected to fraud as a result of the use of NFC technology. A potential risk to consumers involves the NFC antenna; this appears to be a point of entry for “proximity attacks,” in which hackers seek to gain access to mobile devices through the peer-to-peer NFC interface. There have been cases of such attacks seeking to take the mobile phone user’s browsing history, files and documents (Miller, 2012). However, NFC technology has a number of security features that protect consumers’ data. For instance, for data to be transmitted, the NFC short-range technology requires a mobile device to be within a few centimetres of a terminal or other NFC-enabled device (Canadian Bankers Association, 2012 e). Also, NFC technology safeguards data transmitted during payment transmission (Crowe & Tavilla, 2012). When data is transmitted, it is encrypted with a unique code that expires once the transaction is completed (Crowe & Tavilla, 2012). In the case of a credit card transaction, the user’s name and the three-digit security code on the back of the credit card are not transmitted; as a result, any information that might be fraudulently accessed probably could not be used to make future transactions without the card itself. That being said, while there has been a downward trend in fraudulent credit card activity, the exception has been “card-not-present” transactions, for which fraudulent activity continues to rise. In some instances, e-commerce sites have accepted such fraudulent transactions without requiring the three-digit security codes (Hough, 2012). These examples suggest that consumers in fact face new fraud risks as a result of m-payments, although the technological safeguards appear to limit consumer vulnerabilities.

Direct-to-carrier billing fraud risk. A risk for consumers is that fraudulent charges will be placed on their mobile phone bills by third-party billers—a practice known as “cramming.” According to industry experts who participated in the U.S. Federal Trade Commission’s Mobile Cramming Roundtable in May 2013, this fraudulent practice is quickly becoming a significant problem in many jurisdictions around the world, including Canada (Federal Trade Commission, 2013 b). This form of fraudulent activity has emerged at the same time as direct-to-carrier billing practices themselves. Observers indicate that perpetrators of this type of fraud count on consumers not to read their mobile bills, or at least not to read them closely (Federal Trade Commission, 2013 b). The charges are often reported on bills in a vague and deceptive manner (Federal Trade Commission, 2013 b). While cramming is not unique to m-payments, it represents a fraud risk to m-payment users. Further, cramming represents a threat to the perception of direct-to-carrier billing as a legitimate and trusted payment option (Federal Trade Commission, 2013 c). The risk to consumers, it seems, is exacerbated because many are unaware that a third party is allowed to place charges on their mobile bill (Federal Trade Commission, 2013 c).

The FTC outlines three basic protections that can address the risks posed by cramming to consumers: (1) the ability for a consumer to block all third-party charges; (2) the clear disclosure to consumers that third-party charges may appear on a bill and what the process is for blocking such charges; and (3) the establishment of clear and consistent processes for complaints handling and redress (Federal Trade Commission, 2013 c).

3.2.5. Complaints handling and redress

Sound consumer protection regimes include effective business practices for handling complaints and redress for consumers who believe they are victims of misleading or unfair treatment by financial institutions (OECD, 2010). A risk to consumers has been noted in other jurisdictions concerning the lack of clarity around complaints handling and redress. In any m-payment, multiple service providers may be involved, including banks, credit card network operators, mobile network operators and mobile wallet issuers. This may make it difficult for consumers to know which consumer protections apply to their situation (Jun, 2011; OECD, 2012). In the event of an error or unfair treatment, a consumer may be unsure how or where to file a complaint and obtain redress.

Risks associated with lack of clear procedures and responsibilities. Observers in the United States have commented that consumers in that country are essentially on their own when it comes to determining the source of a problem and following up with the company concerned (Budnitz, 2012). If there are varying consumer protection obligations applicable to different players in the ecosystem, the consumer may have very different outcomes depending on which company is ultimately responsible. It is also quite possible that none of the companies would be willing to take responsibility for addressing a complaint or rectifying the situation.

The approach to addressing this consumer risk generally involves cooperation among stakeholders in the ecosystem, coupled with clear communication to consumers. For instance, under South Korea's *Electronic Financial Transaction Act*, regulated financial institutions have clear responsibility for addressing consumers' m-payment problems. In the event of an error, the financial institution is held responsible for problems that occur downstream. This approach is beneficial since consumers are often at a disadvantage when they have to find their own way to settle a dispute, especially within the multi-party business models prevalent in the m-payments ecosystem. An added strength in South Korea is that if the business partnership does not include a financial institution, the legislation assigns responsibility for the erroneous transaction to a subsequent party, such as a mobile network operator. The legislation places the onus on industry stakeholders to maintain open communication with one another. It also empowers consumers. In the U.K., industry best practices encourage the identification of a single point of contact so that it is clear to consumers whom they should contact to report a lost or stolen mobile device and have it disabled.

4. Analysis of consumer protection and m-payments in Canada

The introduction of m-payments brings together participants from industries that are subject to a range of regulations and accountable to various jurisdictions. In the international m-payment literature, one approach to analyzing the regulatory framework has been to assess the particular consumer protection obligations applicable to the underlying source of funds used to make a payment—for example, bank or non-bank, debit or credit card, or prepaid funds (Crowe, Kepler, & Merritt, 2012; Jun, 2011; OECD, 2012).

While analyzing the obligations that apply to the underlying sources of m-payment transactions provides a good starting point, it is apparent that that is not enough. M-payments introduce new players, business models, intermediaries and risks to the marketplace, and these may alter the application of certain obligations within the framework (Crowe, Kepler, & Merritt, 2012). For instance, new laws have the potential to reinforce the current framework. An example is Canada's new anti-spam legislation; when it comes into force, it will address matters related to security and privacy. In other instances, ambiguity could arise about the application of existing legislation and obligations in light of practices and risks that are introduced via m-payments. In some of these cases, the application of existing laws will be clarified through mechanisms such as guidance and policy position statements by supervisory authorities or through other legal means, such as court decisions.

The framework for our analysis is based on the consumer protection principles and emerging consumer protection risks that are detailed in Section 3. For each of the identified principles of consumer protection, we assess (1) the obligations that apply to the underlying sources of m-payments (bank-issued credit cards, debit cards, etc.) and (2) whether obligations exist to address the emerging consumer protection risks associated with the introduction of m-payments. We also identify proposed legislation and other legislative changes that are potentially relevant to the m-payment ecosystem.

4.1. Consumer protection framework

When an m-payment service (such as a mobile wallet) or payment source (such as a debit or credit card) is issued by a bank (i.e., a federally regulated financial institution), obligations associated with the *Bank Act* apply. Banks in Canada are also obligated to comply with a number of consumer-focused voluntary codes of conduct and public commitments. In addition, their corporate policies and business practices influence the protections extended to the consumer.

Non-FRFIs may be subject to federal and provincial legislation, may endorse voluntary industry codes of conduct, and may adhere to corporate policies that protect consumers in one way or another. In terms of the analysis of m-payment consumer protection, we sought to identify whether there are specific consumer protection obligations that are applicable to non-FRFIs providing m-payment products, services and sources of funds. In cases where specific obligations do not exist, we sought to identify whether there is more generic legislation (either federal or provincial) that might address the consumer protection principles of interest.

Each province and territory has consumer protection legislation. There may be similarities between jurisdictions on matters relating to consumer protection. For instance, most provinces have enacted legislation dealing with gift cards and functional equivalency rules for electronic signatures and contracts. Most provinces have also enacted Internet agreement (or remote agreement) legislation for the purpose of protecting consumers online; this legislation may apply to remote m-payments.¹⁵ A comprehensive analysis of provincial/territorial consumer protection legislation is beyond the scope of this report, but we have made an attempt to identify the extent to which the consumer protection principles of interest are addressed.

4.2. Disclosure and transparency obligations

It appears that all m-payment sources are subject to some form of disclosure obligation. Banks that issue debit cards and credit cards are bound by well-defined obligations relative to disclosure through provisions associated with the *Bank Act*, its associated regulations, codes of conduct and public commitments. Non-FRFIs that issue debit and credit cards are responsible for disclosing much of the same information. Other entities, such as mobile wallet providers, are at a minimum required to provide a contract under provincial/territorial consumer protection laws.

4.2.1. Disclosure—bank-issued credit cards

The *Cost of Borrowing (Banks) Regulations* set out the disclosure requirements that apply to banks when entering into a credit agreement for a credit card,¹⁶ as well as the requirements for supplementary disclosure statements. Among other information, the supplementary statements must include an itemized statement of account describing each transaction.

¹⁵ The development of these laws has been guided by the Internet Sales Contract Harmonization Template, a common template endorsed in 2001 by the federal, provincial and territorial ministers responsible for consumer affairs. The template identified commonly agreed-upon principles for contract formation, cancellation rights, credit card chargebacks and information provision in online commerce.

¹⁶ The *Cost of Borrowing (Banks) Regulations* also apply to bank lines of credit and other bank loans.

The Regulations prescribe the disclosure of information, including the initial credit limit, the nature and amounts of any non-interest charges, and the manner in which interest is calculated (Cost of Borrowing (Banks) Regulations (SOR/2001-101)). Key information (such as principal amount, annual interest rate, etc.) must be presented in an information box at the beginning of the agreement or application form in compliance with specific requirements that are intended to ensure legibility (e.g., font size and style, spacing, etc.). The *Cost of Borrowing Regulations* do not explicitly address disclosure requirements on a mobile device. However, to be consistent with the Regulations, an information box would need to appear at the beginning of a disclosure statement presented on a mobile device. While the information boxes were not designed with mobile devices in mind, they may effectively convey critical information to the consumer. An evaluation of their effectiveness would assist in determining the potential benefit from further optimizing the information boxes for mobile device users.

Banks are also required to disclose that if a lost or stolen credit card is used without authorization, the borrower's maximum liability is \$50 or the maximum set by the credit agreement, whichever is less; that if the borrower's PIN is used without authorization to make a transaction at an ATM, the liability incurred by the transaction is the maximum liability set by the credit card agreement; and that if the borrower has reported a lost or stolen credit card to the financial institution either orally or in writing, the borrower has no liability to pay for any transaction entered into through the use of the card after the receipt of the report (Cost of Borrowing (Banks) Regulations (SOR/2001-101)). This provision does not directly address some disclosure-related consumer risks associated with a lost or stolen mobile device. For instance, since the wording of the provision is centred on the card itself, there may be room for differing interpretations between issuers and consumers on the liability that results from loss or theft of a mobile device. Consumers may not be aware of the need to contact their bank when a mobile device that is used for making m-payments is lost or stolen.

4.2.2. Disclosure—bank-issued debit cards

The *Disclosure of Charges (Banks) Regulations* require banks to disclose in writing to their customers and the public all charges applicable to personal deposit accounts. Banks must also maintain a list of all applicable charges and the usual amount to be charged. Copies of these written statements and the list of charges must be made available in each of the bank's branches, at each point of service and on all websites. New or increased charges must be disclosed to customers at least 30 days prior to the effective date (Disclosure of Charges (Banks) Regulations (SOR/92-324)).

Under the Regulations, a bank charging fees to its customers for m-payment transactions, products or services associated with a personal deposit account would be required to disclose the information in a manner that is compliant with the Regulations. The *Disclosure of Charges Regulations* specify that the list of charges must be made available on all websites, but it does not specify the requirement for legibility on a particular device. Since m-payments will enable consumers to make decisions quickly and on the go, consumers might be disadvantaged if the list of charges is not easy to read on a mobile device. This could leave the mobile consumer with less information about fees upon which to base decisions. Consumers may benefit from the requirement to optimize fee information for mobile (or other) devices.

The *Canadian Code of Practice for Consumer Debit Card Services* requires the use of plain language in debit cardholder agreements to disclose information about dispute resolution, liability, lost or stolen cards, PIN confidentiality, service charges, and how to terminate an agreement. The Debit Card Code also requires that card issuers provide consumers with transaction records, as well as periodic statements containing sufficient information for cardholders to be able to check account entries. The Debit Card Code applies to the members of organizations that endorse it.¹⁷ Of relevance to this report, the Debit Card Code applies to debit cards issued by members of the Canadian Bankers Association, the Credit Union Central of Canada and the Fédération des caisses Desjardins du Québec.

4.2.3. Disclosure—new bank product or service

The *Negative Option Billing Regulations* require banks to obtain express consent (either orally or in writing) before they provide a new product or service. The Regulations are technology-neutral, and section 2 of the Regulations states that they apply to “an institution’s products or services for non-business purposes.” Accordingly, the Regulations apply to banks that offer new or optional mobile wallets, or other forms of related m-payment products or services.

Under the Regulations, before a consumer provides express consent to receive a new optional product or service from an institution, the institution must provide:

- a description of the product or service;
- the term of the agreement;
- the charges for the product or service or the method for determining the charges and an example to illustrate the method;
- the conditions under which the person may cancel the product or service;

¹⁷ The following organizations endorse the Debit Card Code: the Canadian Bankers Association, the Canadian Federation of Independent Business, the Credit Union Central of Canada, the Consumers’ Association of Canada, the Fédération des caisses Desjardins du Québec and the Retail Council of Canada.

- the date from which the product or service is available for use and, if different, from which charges apply; and
- the steps required to use the product or service.

In addition:

- all of this information must be disclosed in language that is clear, simple and not misleading;
- any subsequent changes to the terms and conditions must be disclosed to all subscribers to the product or service at least 30 days before the change takes effect; and
- banks must, without delay, refund or credit a customer who cancels an optional product or service. (Negative Option Billing Regulations (SOR/2012-23))

Debit Card Code extended to online transactions

The *Canadian Code of Practice for Consumer Debit Card Services* has been extended to online transactions through the Canadian Bankers Association's customer commitment concerning online payments. Under this public commitment, Association members undertake to apply the principles and provisions of the Debit Card Code to online payments associated with customer deposit accounts. Another related commitment is the *Interac Online Customer Commitment*. At present, four federally regulated financial institutions offer online debit payment services via *Interac Online*. The four have committed to providing customers with appropriate disclosures related to any fees associated with *Interac Online* services; the customer's responsibilities for protecting passwords and the consequences if these are violated; whom the customer should contact in the event of a problem; and the potential extent of losses resulting from unauthorized use of *Interac Online* services (Interac, 2012).

Merchants who offer *Interac Online* are required to comply with the *Canadian Code of Practice for Consumer Protection in Electronic Commerce*. The Code establishes merchant benchmarks for good business practices related to disclosure of information, contract formation and fulfillment, online privacy, security of payment and personal information, redress, unsolicited emails, and communications with children (Working Group on Electronic Commerce and Consumers, 2004).

4.2.4. Disclosure—credit cards issued by non-FRFIs

Provincial cost-of-credit disclosure legislation governs the disclosure of fees and interest rates with respect to credit account transactions facilitated by non-FRFI card issuers. While there is variation between the relevant provincial consumer protection acts, efforts have been made to harmonize credit disclosure so that users of credit cards share nearly the same rights and protections regardless of the jurisdiction of the card issuer.¹⁸ The consumer protection obligations that apply to non-FRFI issuers of credit cards are generally similar to those applicable to banks. Like banks, non-FRFI credit card issuers are required to provide initial and subsequent disclosure statements, to limit liability for unauthorized charges, and to clearly indicate contact information for handling complaints and redress. Unlike the *Cost of Borrowing Regulations*, in certain jurisdictions the definition of a credit card explicitly includes “other devices.” This definition further clarifies the application of the legislation to m-payments and reduces the risk of ambiguity relative to the interpretation of the liability provisions.

4.2.5. Disclosure—debit cards issued by non-FRFIs

Debit cards that are issued by non-FRFIs are subject to the Debit Card Code, which is endorsed by a number of organizations including the Credit Union Central of Canada and the Fédération des caisses Desjardins du Québec. Therefore, users of m-payments funded through debit cards that are issued by a credit union or a caisse populaire share with bank-issued debit card users the same consumer protections afforded by the Debit Card Code.

¹⁸ In 1998, the federal and provincial consumer affairs ministers agreed to harmonize the cost-of-credit disclosure laws in Canada in order to “reduce compliance costs and provide uniform consumer protection across Canada; to clarify and, where possible, simplify cost of credit disclosure rules; and to modernize laws to take account of developments in credit markets in recent years” (Consumer Measures Committee, 1998).

4.2.6. Disclosure—companies offering direct-to-carrier billing

Direct-to-carrier billing is an increasingly prevalent option for remote m-payments and potentially for point-of-sale m-payments being offered by mobile network operators and online service providers (for instance, Facebook or Skype). In May 2013, the Canadian Radio-television and Telecommunications Commission (CRTC) announced a Wireless Code that is intended to better inform wireless consumers of the rights and obligations contained in their contracts. The Wireless Code applies to all “wireless services” (i.e., mobile network operators) but does not apply to other entities offering direct-to-carrier billing services. The Wireless Code will apply to new contracts starting on December 2, 2013. It requires service providers to give the customer a permanent copy of the contract and related documents that set out key terms and conditions, such as those related to services included in the contract, minimum monthly charges, privacy policy, the fee to unlock the device, etc. (CRTC, 2013). For consumers with postpaid contracts,¹⁹ a “Critical Information Summary” must also accompany the permanent copy of the contract to briefly explain its most important elements.

The Wireless Code addresses a number of items that are relevant to direct-to-carrier billing. For instance, contracts must state the rates for optional services that are selected by the customer at the time of the contract, and must indicate where customers can find information about rates for optional and pay-per-use services. The Wireless Code also states that a “service provider must not charge for any device or service that a customer has not expressly purchased.” Also relevant to the risks associated with fraudulent direct-to-carrier billing, the Code requires the service provider to give the customer information on how to unsubscribe from premium services.

¹⁹ Postpaid services are wireless services that are paid for after use, usually upon receipt of a monthly bill.

Non-bank payment service providers. The consumer protection obligations of non-bank entities that provide mobile wallets and other payment services are not explicitly stated. Some such providers that offer peer-to-peer m-payments and mobile remittance services are registered as money services businesses, while others are not. For example, PayPal issues online prepaid accounts and offers point-of-sale m-payment services. PayPal Canada is not considered a financial institution, nor is it registered as a money services business in Canada. Consequently, it is not regulated under the *Bank Act* and its practices are not monitored by an oversight agency in Canada. If a consumer seeks specific information or has a problem with a service, the consumer would be protected by provincial consumer protection laws and would have access to the protection provided under the policies and business practices of the company. In the case of PayPal Canada, many of its corporate policies are developed to comply with regulations in other jurisdictions. Since PayPal is regulated under *Electronic Fund Transfers Act* (Regulation E) in the United States, a number of its consumer protection policies and business practices are aligned with the requirements of this regulation. Similarly, PayPal's user protection practices are aligned with the European Union Data Privacy Directive.

Non-bank prepaid issuers. Since the mid-2000s, most provinces have brought into force gift card legislation that prohibits expiry dates, places limits on the type and timing of fees, and requires the disclosure via gift card agreements of all fees, all restrictions, limitations and conditions that are placed on a gift card. Use of gift cards is subject to the policy and terms and conditions of any agreement with the relevant company.

4.2.7. Summary of disclosure obligations

With regard to disclosure obligations, credit and debit card issuers in Canada are required to disclose agreements to terms, all fees and charges, information about liability against loss, statements of accounts, transaction records, and contact information for the purpose of filing a complaint or obtaining redress (Table 1). Banks and other organizations that collect, use or disclose personal information in the course of commercial activity, including those involved in m-payments, are required to disclose their information management and privacy practices and to obtain meaningful consent from the consumer (that is, consent given by an individual who has understood how the information will be used).

Issuers of other sources of m-payment funds may share some but not all of the same disclosure obligations. In the case of direct-to-carrier billing, the Wireless Code will require mobile network operators to provide contracts that clearly spell out fees, contact information and privacy disclosure, among other details. The Wireless Code does not require the operators to disclose a limit to the consumer's liability against loss. Of course, the Wireless Code applies only to wireless service providers, and any other entities providing direct-to-carrier billing would not be subject to these requirements.

It appears that all issuers of sources of funds analyzed are required to provide a form of contract or agreement to terms. Since the provincial/territorial rules are jurisdiction-specific, the nature and content of the contracts may vary. Most provincial/territorial gift card legislation requires issuers to disclose all fees and contact information for the purpose of accessing balances or filing a complaint. However, gift card issuers are not required to disclose practices related to liability against loss, or to provide regular statements of account or transaction records. Issuers of online prepaid accounts appear not to have disclosure obligations beyond the general requirement to provide a contract or an agreement to terms and, if appropriate, the requirement to disclose privacy practices under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) or a provincial equivalent.

Table 1: Disclosure obligations, by source of funds

Source of funds	Contract	Fees & charges	Liability against loss	Statement of account	Contact info	Privacy disclosure**
Bank-issued credit cards	Yes	Yes	Yes	Yes	Yes	Yes
Bank-issued debit cards	Yes	Yes	Yes	Yes	Yes	Yes
Non-FRFI credit cards	Yes	Yes	Yes	Yes	Yes	Yes
Non-FRFI debit cards	Yes	Yes	Yes	Yes	Yes	Yes
Direct-to-carrier*	Yes	Yes	No	Yes	Yes	Yes
Gift cards	Yes	Yes	No	No	Yes	Yes
Online prepaid	Yes	No	No	No	No	Yes

Yes: the issuer of a source of m-payment is bound by an obligation to provide a specified form of disclosure.

No: the issuer of a source of m-payment is not bound by an obligation to provide disclosure.

* The Wireless Code applies to wireless providers but not to other entities offering direct-to-carrier billing. The Wireless Code will apply to new contracts starting from December 2, 2013.

** The *Personal Information Protection and Electronic Documents Act* requires organizations to disclose their practices and obtain meaningful consent from the consumer.

4.3. Protection of consumer privacy

The *Personal Information Protection and Electronic Documents Act* applies to organizations that collect, use or disclose individuals' personal information in the course of commercial activity. It does not apply to organizations in provinces deemed to have substantially similar private-sector privacy legislation—that is, as of the date of this report, British Columbia, Alberta and Quebec.²⁰ PIPEDA continues to apply in cases of cross-border data flows. It also applies to federal works, undertakings, or businesses across Canada—including telecommunications companies as well as banks listed in schedules I and II of the *Bank Act*—where it covers both customer and employee personal information.²¹

PIPEDA applies to the collection, use or disclosure of “personal information.” This term is broadly defined as “information about an identifiable individual,” excluding “the name, title or business address or telephone number of an employee of an organization.” Information is also “about” a person if it relates to or concerns that individual. An individual is “identifiable” if there is a serious possibility that he or she could be identified through the use of that information, alone or in combination with other available information. According to Scassa & Deturbide (2012), “Personal information has been found to include medical or biological data, biometric data, the sound of one’s voice, and photographic or video images, to give just a few examples.”

4.3.1. Addressing risks associated with privacy disclosure

As stated in Section 3.2.2, when privacy practices are not clearly communicated, consumers are at risk from a lack of awareness of who has access to their data and how it is being stored or used. PIPEDA provides a foundation for requiring organizations to disclose privacy practices. The Act requires individuals' knowledge and consent for every collection, use and disclosure of personal information unless an exception applies. The Act states that an organization must identify and document the purposes for which it seeks to collect personal information at or before the time of collection.

An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before it is used or disclosed. An example would be a case in which an organization wants to use information for a purpose not previously identified.

²⁰ Ontario, New Brunswick, and Newfoundland and Labrador also have substantially similar legislation, but with a focus limited to the personal health information management practices of health custodians in their respective jurisdictions.

²¹ Schedule I of the *Bank Act* lists banks that are not subsidiaries of foreign banks. Schedule II lists banks that are subsidiaries of foreign banks. PIPEDA does not apply to banks listed in Schedule III of the Act, that is, branches of foreign banks authorized to carry on business in Canada.

To our knowledge, no obligations in Canada require service providers to optimize privacy disclosures for mobile devices. As indicated by the U.S. Federal Trade Commission, mobile devices are well equipped to provide consumers with “just-in-time” privacy disclosures so that consumers can give meaningful consent at the time when the data is being collected, as opposed to the time that an app is installed. The FTC also promotes the use of “dashboards” that enable consumers to review privacy disclosures and adjust privacy settings as they like. Also, it is not required that icons be used to bring to the consumer’s attention an instance when personal information (such as geo-tracking) is being transmitted.

Non-Canadian entities. Many of the major technology companies that are involved in providing mobile wallets and mobile payment applications, and that therefore are involved in collecting personal data of Canadian m-payment users, are based in the United States and other jurisdictions. Generally speaking, when an entity (organization or individual) carries out business within a jurisdiction and profits from the people who live there, it has indicated that it accepts that jurisdiction’s authority (Scassa & Deturbide, 2012). The *Personal Information Protection and Electronic Documents Act* applies to organizations that operate outside Canada if there is a real and substantial connection between the subject matter of a complaint and Canada. Consumers have the right to file a complaint with the Privacy Commissioner of Canada against any organization that contravenes the terms of the Act. The Privacy Commissioner has established precedents for investigating foreign companies accused of breaching the terms of PIPEDA. As a result of these investigations, companies have generally cooperated with the Office of the Privacy Commissioner and sought to resolve the concerns (Scassa & Deturbide, 2012). In other cases where companies have refused to cooperate, the Privacy Commissioner’s investigation enables a complainant to seek damages from the Federal Court, and the court’s decision is enforceable in another jurisdiction (Scassa & Deturbide, 2012).

PIPEDA requires personal information that is stored outside Canada to be adequately safeguarded. However, since foreign companies must adhere to the laws of the jurisdictions in which they operate, the personal information of Canadians may be subject to lawful access by foreign authorities (Scassa & Deturbide, 2012). For instance, any personal information that is stored in the United States is subject to the *Patriot Act*, which “facilitates access by US authorities to all personal data in the hands of US-based private sector companies for a range of law enforcement and national security purposes” (Scassa & Deturbide, 2012).

4.3.2. Addressing privacy risks

The consumer risks associated with privacy are related to identity theft, lack of awareness of profiling and the exploitation of the vulnerability of children. PIPEDA appears to provide a good foundation for addressing these risks.

Safeguarding personal information against loss or theft is a requirement under PIPEDA. Specifically, it is required that the security used to safeguard information be appropriate to the sensitivity of the information. The methods of protection include (1) physical measures (e.g., locked cabinets and restricted access to offices); (2) organizational measures (e.g., security clearances and access on a need-to-know basis; and (3) technological measures (e.g., passwords and encryption). The Act also stipulates that care be used in the disposal or destruction of personal information to prevent unauthorized access to it (Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)).

In June 2012, the Office of the Privacy Commissioner of Canada released a general guidance and a complementary policy position statement to clarify the intended application of PIPEDA to profiling practices and online behavioural advertising (Office of the Privacy Commissioner of Canada, 2012a; Office of the Privacy Commissioner, 2012b). While the guidance and statement do not directly address mobile devices and m-payments, they establish a precedent of interpretation for data profiling practices in Canada. The high-level position adopted by the Office is that “online behavioural advertising may be considered reasonable ... provided it is carried out under certain parameters, and is not made a condition of service for accessing and using the Internet, generally” (Office of the Privacy Commissioner of Canada, 2012a).

The Office acknowledges that the information involved in online tracking and targeting for the purpose of directing behaviourally targeted advertising to individuals will generally constitute personal information. Online behavioural advertising is considered appropriate if it meets the following conditions: it is not considered a term or condition for individuals to use the Internet generally; meaningful consent is obtained; and limitations are placed on the types of information collected and used for profiling. The Office further states, “Safeguarding the information is also vital, as is limiting the retention of the data to the least amount of time possible.”

In term of prohibitions, the Office of the Privacy Commissioner provides guidance restricting tracking and targeting if the user is not able to decline participation or if declining renders the service unusable. Organizations should also avoid tracking of children as well as any tracking practices on websites aimed at children, since it is difficult to ensure meaningful consent from children.

4.3.3. Summary of privacy protection

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*. The Act appears to address the consumer risks associated with privacy disclosure, identity theft and, to a certain extent, profiling. As mentioned, the Office of the Privacy Commissioner's guidance on targeted behavioural advertising does not explicitly address the use of behavioural marketing on a mobile device. It therefore remains to be seen how PIPEDA will be interpreted in connection with profiling based on consumers' use of mobile devices, including geo-tracking.

4.4. Protection of consumer data from malware

The consumer risks of identity theft and fraud that are presented by malware and other forms of malicious software are addressed via legislation including the *Criminal Code* and the *Competition Act*. The *Criminal Code* has a number of provisions that prohibit fraudulently obtaining or using computers, computer systems²² and data (Criminal Code (R.S.C., 1985, c. C-46)). These include fraudulently using a computer system (or causing one to be used) with intent to commit an offence, as well as fraudulently intercepting any function of the computer system. It is a criminal offence under the *Competition Act* to make false or misleading representations similar to those that would be related to tricking a consumer into installing malware on a mobile device (Competition Act (R.S.C., 1985, c. C-34)).

Canada's Competition Bureau published Enforcement Guidelines in 2009 to clarify the application of the *Competition Act* with regard to representations on the Internet. The guidelines state, "Canadian law governing jurisdiction on-line is evolving with the growth in electronic commerce. It is therefore difficult to predict how the courts or the Competition Tribunal will interpret jurisdictional questions in respect of liability for false or misleading representations and deceptive marketing practices carried out in whole or in part over the Internet" (Competition Bureau of Canada, 2009). The Bureau also states that it will "assert Canadian jurisdiction over foreign entities to the fullest extent authorized by law ... [and] will also actively seek the assistance and co-operation of foreign agencies to address false or misleading representations and deceptive marketing practices having an effect on the Canadian market" (Competition Act (R.S.C., 1985, c. C-34)).

²² The term "computer system" is defined in the *Criminal Code* in a manner that applies to mobile devices: "a device that, or a group of interconnected or related devices one or more of which, (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other function."

If a person outside Canada makes a false or misleading representation—for example, by attaching malware to a mobile application—the *Competition Act* deems that the responsibility lies with the person who imports the false or misleading representation into Canada. Since this technology is in its infancy, there are few precedents to shed light on how the *Competition Act* will be interpreted and applied. According to Scassa & Deturbide (2012), “It is unclear whether intermediaries such as service providers and Web hosts who have a role in the dissemination of advertising can also be found guilty of contravening the *Competition Act*. Presumably in most cases, service providers would be considered distributors who have no control over content, but that is not necessarily true of other intermediaries.”

4.4.1. Pending anti-spam legislation

Legislation continues to evolve to address risks associated with m-payments and other related technological advances. Pending anti-spam legislation and accompanying regulations will further address matters related to security and privacy of m-payments in Canada by extending provisions of the *Competition Act* concerning false and misleading marketing to electronic messages. The new federal legislation (Bill C-28) was passed on December 15, 2010. When it comes into force, it will prohibit the following:

 sending of commercial electronic messages without the recipient’s consent, including messages to email addresses and social networking accounts, and text messages sent to a cell phone; alteration of transmission data in an electronic message which results in the message being delivered to a different destination without express consent; installation of computer programs without the express consent of the owner of the computer system or its agent, such as an authorized employee; use of false or misleading representations online in the promotion of products or services; collection of personal information through accessing a computer system in violation of federal law (e.g. the *Criminal Code of Canada*); and collection of electronic addresses by the use of computer programs or the use of such addresses, without permission (address harvesting). (Government of Canada, 2011)

Within the anti-spam legislation, perhaps the most explicit application to malware is the prohibition on installation of computer programs on any other person’s computer system in the course of commercial activity unless express consent has been obtained or the person is acting in accordance with a court order. According to this section of the legislation, a person is in contravention if the computer system is located in Canada. The implication is that the anti-spam legislation will apply to parties outside Canada who install malware on a mobile device.

The anti-spam legislation will give the Canadian Radio-television and Telecommunications Commission the authority to regulate certain forms of electronic contact in the course of commercial activity. The *Electronic Commerce Protection Regulations (CRTC)*, which will come into force on the same day as the anti-spam law, will require consumer consent prior to sending commercial electronic messages, altering transmission data in electronic messages or installing computer programs on another person's computer system (CRTC, 2012). The Regulations require specific information to be included in commercial electronic messages, including the name and contact information of the person or business sending the message and a clear mechanism for unsubscribing. The Regulations also provide direction about the information to be included in a request for consent.

The *Electronic Commerce Protection Regulations* are intended to provide clarity and legal certainty regarding key terms in Canada's Anti-spam Legislation. Among other clarifications, the Regulations define exceptions to the legislation, such as family and personal relationships; excluded commercial electronic messages, such as those sent by an employee to another employee or the first contact as the result of a referral from someone with an existing relationship; computer programs that are installed on behalf of a telecommunications service provider to upgrade a network; and non-profit clubs and associations. Public comment on the Regulations has closed but as of the writing of this report the Regulations have not been finalized.

4.4.2. Summary of protection against malware threats

Consumer protections against malware threats are not comprehensive in Canada at present. The anti-spam legislation has not yet come into force. This legislation was developed to explicitly address the sending of spam, as well as the undesired installation of malware, and also to extend the provisions of the *Competition Act* concerning false and misleading marketing through electronic messages. Since the legislation has not yet come into force, we consider that explicit consumer protections do not yet exist in Canada relative to protections against malware.

4.5. Protection of consumer assets against fraud and misuse

The *Criminal Code* has provisions for mitigating the risks of fraud and misuse of consumer credit card assets. Under these provisions, it is an indictable offence to steal, forge or falsify a credit card. It is also an indictable offence to possess use, traffic or permit another person to use fraudulent credit card data (Criminal Code (R.S.C., 1985, c. C-46)).

4.5.1. Protection against fraud and misuse—bank-issued credit cards

As discussed in Section 4.2.1, the *Cost of Borrowing (Banks) Regulations* specify that a bank entering into a credit agreement for a credit card must provide the borrower with an initial disclosure including a statement that if a lost or stolen card is used without authorization, the borrower's maximum liability is \$50 or the maximum set by the credit agreement, whichever is less. Visa, MasterCard and American Express have made formal public commitments to protect consumers from unauthorized credit card use. If the borrower has reported a lost or stolen credit card to the bank either orally or in writing, the borrower has zero liability to pay for any transaction entered into through the use of the card after the receipt of the report.

4.5.2. Protection against fraud and misuse—debit cards

The Debit Card Code clearly sets out the liability for loss for unauthorized debit card transactions. Cardholders are not liable for losses resulting from circumstances beyond their control, such as technical problems, card issuer errors and other system malfunctions. The Debit Card Code defines unauthorized use of a card and the circumstances in which a cardholder may be deemed to have contributed to the unauthorized use—for example, by voluntarily disclosing a PIN or failing to notify the issuer when the card is lost or stolen. The Code indicates that a cardholder deemed to have contributed to an unauthorized use is liable for losses.

4.5.3. Assessing protection of consumer assets against fraud and misuse

Responsibilities and liabilities. What is unclear about the application of the zero liability provisions is how the responsibilities and liabilities will be affected in the m-payments ecosystem. For instance, it is not clear whether a credit card issuer will necessarily take on the liability for losses when a mobile device is lost, stolen or otherwise compromised. It is also not clear to what extent a cardholder is responsible in an environment where a PIN is not necessary to authenticate a debit payment. For instance, contactless payments generally do not require a PIN for any value of less than \$50, and many mobile wallets do not require the use of PINs. In this regard, a precedent has been set through the Canadian Payments Association's Rule E4,²³ which assigns liability for unauthorized PIN-less transactions to the "payer" financial institution. This rule's scope includes "payment applications embedded in a device (such as a debit card, key fob, or cellular phone)." Clarification is likely to be required to determine how other existing obligations will be applied to m-payments. For instance, it may be that consumers could be required to lock a mobile device to avoid being deemed to have contributed to the unauthorized use of a credit card if the mobile device is lost or stolen.

²³ For more information, see the Canadian Payments Association's *Rule E4—Exchange of PINless Point-of-Service Debit Payment Items for the Purpose of Clearing and Settlement*.

Fraud risks associated with NFC-based mobile wallets. There may be a gap in the framework relative to risks associated with NFC-based mobile wallets. As discussed in Section 3.2.4, the risks of fraud that are directly related to technology breaches appear to be quite minor. However, security is a major concern for consumers and so it is worth noting that m-payment providers are not required to follow specific obligations relative to NFC technology.

The *Canadian NFC Mobile Payments Reference Model* provides a level of security to m-payments that employ NFC technology. The Reference Model was developed through an initiative of the Canadian financial industry, with the participation of banks and credit unions.²⁴ It describes guidelines related to the design of m-payment applications, the installation of these applications on mobile devices, the collection and storage of data, and the execution of mobile payments themselves.

The guiding principle related to data collection is that each ecosystem participant should have access to only the minimum amount of information required to perform its primary function. The model provides guidance about which members of the m-payments ecosystem can have access to different forms of data, such as credentials, payment information and wallet data. The Reference Model also encourages all participants to put processes in place to track, monitor and mitigate fraud and security concerns, including malware, hacking and theft of mobile devices. The Reference Model is intended to guide all participants in the NFC ecosystem; however, it applies only to financial institutions that participated in its development, along with their partners. The Reference Model may provide additional security to some m-payment users, but compliance with the Reference Model is voluntary and is not enforced by an oversight agency. For this reason, we acknowledge its presence in the marketplace but exclude it from our analysis.

Direct-to-carrier billing fraud risk. The introduction of the Wireless Code (see Section 4.2.6) will further clarify the responsibilities for service providers and consumers relative to direct-to-carrier billing practices. It should be noted that when the Wireless Code comes into force in December 2013, it will address two of the three “basic protections” identified by the U.S. Federal Trade Commission that protect consumers against cramming (fraudulent charges on mobile phone bills). Through the Wireless Code, Canadian consumers have been ensured clear disclosure of third-party charges on a bill along with the process for blocking such charges, as well as access to a clear and consistent process for complaints handling and redress. The protection that is recommended by the FTC but has not been extended via the Wireless Code is the ability to block all third-party charges.

²⁴ The participants in the initiative are the Bank of Montreal, the National Bank of Canada, the Canadian Imperial Bank of Commerce, the Credit Union Central of Canada, Desjardins Financial Group, the Royal Bank of Canada, the Bank of Nova Scotia and the Toronto Dominion Bank.

The legal framework may soon have relevant precedents as well. In September 2012, the Competition Bureau began legal proceedings against Bell, Rogers, TELUS and the Canadian Wireless Telecommunications Association based on evidence that they had facilitated the sale of premium-rate digital content (e.g., trivia questions, ringtones) for fees that were not adequately disclosed (Competition Bureau, 2012).

4.6. Complaints handling and redress

The *Bank Act* and the Debit Card Code require banks to ensure that they have complaints handling and redress mechanisms. The Wireless Code requires mobile network operators to provide customers with information on how to contact the Commissioner for Complaints for Telecommunications Services to seek assistance in resolving complaints.

4.6.1. Complaints handling and redress—bank-issued credit cards

Under the *Bank Act*, banks must establish procedures for dealing with complaints, must designate an officer or employee to be responsible for implementing the procedures, and must designate one or more officers or employees to receive and deal with any complaints (Bank Act S.C. 1991, c. 46). All of this information must be made publicly available, whether through branches, on websites or in written format. Customers must also be made aware of how to contact the Financial Consumer Agency of Canada if they have a complaint related to a consumer provision under the *Bank Act* (Bank Act S.C. 1991, c. 46).²⁵

4.6.2. Complaints handling and redress—bank-issued debit cards

The Debit Card Code sets out procedures for addressing unauthorized transactions and other transaction problems. Under these procedures, the consumer must contact the PIN issuer to file a report. The PIN issuer then undertakes to respond to the consumer as soon as possible and no later than 10 days after the consumer makes the report. In the case of an unauthorized transaction that is not fully reimbursed, the PIN issuer is responsible for demonstrating how the consumer contributed to the unauthorized use of the card. When a debit cardholder's problem cannot be resolved by the PIN issuer, the consumer will be advised which party to contact regarding the dispute and will not be unreasonably restricted from using funds that are subject to the dispute.

²⁵ New *Complaints (Banks, Authorized Foreign Banks and External Bodies) Regulations* (SOR/2013-48) came into force on September 2, 2013, requiring banks to belong to a designated external complaint body.

4.6.3. Complaints handling and redress—direct-to-carrier billing

With regard to complaints handling and redress, the Wireless Code requires the clear disclosure of how to contact the service provider's customer service department and how to file a complaint, along with the contact information for the Commissioner for Complaints for Telecommunications Services and the Wireless Code itself (CRTC, 2013). The Wireless Code applies to all wireless services.

4.6.4. Assessing protection related to complaints handling and redress

The debit and credit card issuers and the mobile network operators have clear redress mechanisms in place, but the mechanisms may be inadequate in an m-payments ecosystem in which multi-party business models exist. The Wireless Code states that consumers are to contact their MNO to report a lost or stolen mobile device. Similarly, credit and debit card issuers require consumers to report their cards as lost or stolen. If there is an intermediary involved, such as a third-party mobile wallet issuer (e.g., Google Wallet or Square Wallet), it is likely that corporate policies will require the consumer to contact the issuer as well.

Ultimately, a gap may exist in Canada since there is no legislation that assigns responsibility within the ecosystem for communicating procedures to the consumer and ensuring that appropriate redress is obtained. There is also no clarity in terms of which service provider should be contacted in the event of a problem, such as loss or theft of a mobile device.

4.7. Summary of protection of data and assets, and protection against fraud

There is inconsistency across the ecosystem with regard to the principles of protection of consumer data and privacy; protection of consumer assets against fraud and misuse; and complaints handling and redress. Credit and debit card issuers are required to comply with provisions that protect consumers to some degree under each of these principles (Table 2). There is, however, an ecosystem-wide gap related to the protection of data against malware; this is likely to be addressed when the federal anti-spam legislation comes into force.

Other m-payment sources have varying obligations under the consumer protection principles. Mobile network operators offering direct-to-carrier billing are not bound by an obligation to provide a zero-liability policy. Other entities offering direct-to-carrier billing (e.g., technology companies) are not subject to the Wireless Code and therefore also do not have specific obligations related to complaints handling and redress. Gift card issuers and online prepaid account issuers do not have specific obligations related to the principle of protection of consumer assets against fraud and misuse, or the principle of complaints handling and redress. It is possible that some of these gaps are addressed by corporate policies, voluntary codes of conduct and other mechanisms that are not legislated and are not under the oversight of a supervisory agency. From the perspective of regulatory obligations, these are identified as gaps in the consumer protection framework.

Table 2: Consumer protection obligations, by source of funds

Source of funds	Protection of privacy	Protection of data against malware**	Protection against fraud & misuse	Complaints handling & redress
Bank-issued credit cards	Yes	No	Yes	Yes
Bank-issued debit cards	Yes	No	Yes	Yes
Non-FRFI credit cards	Yes	No	Yes	Yes
Non-FRFI debit cards	Yes	No	Yes	Yes
Direct-to-carrier*	Yes	No	No	Yes
Gift cards	Yes	No	No	No
Online prepaid accounts	Yes	No	No	No

Yes: the issuers of a certain source of m-payment are **bound** by a specific obligation.

No: indicates that the issuers of a certain source of m-payment are **not bound** by a specific obligation.

* The Wireless Code applies to wireless providers but not to other entities offering direct-to-carrier billing. The Wireless Code will apply to new contracts starting on December 2, 2013.

** The anti-spam legislation will provide protections against malware. At the time of publication, the date on which the legislation will come into force had not been set.

5. Conclusions

We conclude that users of m-payments in Canada are not all protected equally. The consumer protections that apply to m-payments are dependent on the underlying source of funds and the entity providing the service, such as a bank or mobile network operator. Since m-payments attract a wide variety of service providers, the consumer protection obligations vary across the ecosystem. The emergence of m-payments in the market also introduces a number of new elements that have an impact on the risks to consumers and potentially on the application of the existing consumer protection framework.

The following sections outline the major gaps that were identified and potential solutions to address these gaps.

5.1. Uneven protection of financial consumers

The m-payments ecosystem involves 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. For instance, the obligations of a bank that offers its customers a mobile wallet are considerably greater than those of a money services business or technology company offering a comparable mobile wallet. A consumer using a mobile wallet issued by a bank would be entitled to clear disclosure of information related to fees, complaint and redress mechanisms, etc. However, the same consumer using an identical mobile wallet issued by a technology company would not necessarily be entitled to these disclosures. Further, in the event of an error or complaint, the bank issuer will be required to follow clear procedures, whereas the technology company may not. The technology company may well follow practices very similar to those required of the bank. However, the consumer protection provisions are not embedded in the legislation that governs the activities of that industry.

5.1.1. Minimum standards

In certain OECD member countries, there has been a call for minimum consumer protection standards to apply to all m-payment sources (OECD, 2012). It would be beneficial for policy makers to further consider the value to Canadian consumers of minimum consumer protection standards that would apply uniformly across the m-payments ecosystem. Each payment source presents a different level of risk to consumers, and it is appropriate to consider whether the current consumer protections are proportionate to the risks of the associated underlying payment sources. If minimum standards are deemed to be beneficial for Canadian consumers, an analysis of payment risk is most likely necessary to determine the levels at which minimum standards should be set.

5.1.2. Regulating non-bank entities

Given the potential importance of non-bank service providers in the m-payments market, it is important to consider the manner in which non-bank entities have been regulated in other jurisdictions. In a number of jurisdictions, for instance, legislation has been written that applies to financial institutions and “other entities”; the result is that all providers are subject to the same obligations. In the United States, the *Electronic Fund Transfers Act* (Regulation E) defines a financial institution as “a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services.” South Korea’s *Electronic Financial Transaction Act* applies to financial institutions as well as to “electronic financial business operators”—a catch-all reference to non-financial institutions. 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. More analysis and evidence may be required prior to implementing such a policy reform.

5.1.3. Monitoring business practices

As the m-payments market develops, it will be important to monitor the business practices of the differing entities for the purpose of assessing the consumer protection practices of all participants. It will also be important to monitor consumer complaints and other relevant data about bank and non-FRFI issuers of m-payment products and services; this will provide indicators of the effects of inconsistent consumer protection obligations across the ecosystem. Monitoring of this type will provide evidence about whether the gaps in the Canadian consumer protection framework are problematic for consumers and whether they need to be addressed.

5.2. Disclosure

As mobile banking and m-payments become more common, there may be an increased demand for disclosure statements to be made available on mobile devices. Since mobile devices have limitations as a result of their relatively small screen size, it may be necessary to update disclosure requirements to stipulate that these should also be prepared in a manner that is conducive to viewing on mobile device screens so that they can be fully read and comprehended. Our analysis indicates that while all entities involved in providing m-payments are responsible for providing a contract or agreement to terms or more comprehensive disclosure, none is required to provide disclosure statements that are optimized for mobile devices. Beyond optimizing general disclosure statements, Canadian obligations do not also require the optimization of privacy disclosure for mobile devices through such means as just-in-time disclosures, dashboards and geo-tracking icons. We are not aware of any such provisions that exist in other jurisdictions either. Since the technology is still in its infancy, this is not surprising. Evidence from experts in other jurisdictions suggests that the optimization of disclosure statements on mobile devices would be beneficial to consumers. Canadian policy makers are invited to consider whether it is appropriate for service providers to be required to disclose terms of agreement and privacy disclosure in a manner that is optimized for a mobile device.

5.3. Clarifying liability against fraud and misuse

The introduction of m-payments could create ambiguity in the financial consumer protection framework. For instance, it is unclear how the consumer protection provisions related to liability against loss will be interpreted when a mobile wallet is introduced. The Debit Card Code clearly defines the criteria for determining whether a customer has contributed to the unauthorized use of a debit card. These criteria are not specific to m-payments. Therefore, in a situation where the loss or theft of a mobile device leads to an unauthorized payment, it is unclear whether the customer will be held liable. The *Bank Act* provisions related to credit card issuers raise similar questions about who will be liable when an unauthorized transaction takes place via a mobile device. The *Bank Act* obligations clearly provide a good foundation; but in the m-payments context, some modifications or further commitments may be required to ensure that the obligations remain technologically relevant and appropriate given the introduction of new intermediaries. Further analysis is likely to be required to identify appropriate modifications that would address potential ambiguities, such as those related to liability for loss.

5.4. Assigning responsibilities within the ecosystem

It is important for consumers to have access to mechanisms by which they can submit complaints and receive redress. Our analysis indicates that this consumer protection principle is inconsistently applied across the m-payments ecosystem in Canada. From experiences in other countries, it appears that consumers may benefit from having a more level playing field so that they will not be at a disadvantage when attempting to settle a dispute. This is especially pertinent in the type of multi-party business models prevalent in the m-payments ecosystem.

With the goal of a more level playing field in mind, it may be necessary to set obligations applicable to all players in the m-payments ecosystem and to assign clear responsibility for handling complaints. For instance, South Korean legislation assigns ultimate responsibility to the financial institutions for handling complaints and redress, regardless of which service partner was responsible for the error that occurred. The development of the NFC Reference Model demonstrates the effectiveness of industry collaboration. Similar mechanisms may be appropriate for developing industry consensus on matters related to assigning responsibilities for complaints handling, redress and other matters that require coordination. Policy makers should consider which service providers are best positioned to assume this role in Canada.

Consumers would also be likely to benefit from the disclosure of information related to complaints handling and redress. They are concerned about having their mobile devices lost, stolen or hacked, and so it is of prime importance that consumers know how to quickly contact the service providers concerned when there is a problem with a mobile device. This is particularly important since the limitations on liability associated with many card schemes generally begin once a consumer has alerted the service provider to the problem. With disclosure of clear, cooperative complaints handling and redress processes, as well as contact information, consumers would be likely to know exactly whom to contact and how to do this as quickly as possible.

5.5. Financial consumer education

For a protection regime to be effective, consumers must be knowledgeable about their rights and responsibilities. Knowledgeable consumers are empowered and are better able to make informed decisions. Informed consumers are likely to be better prepared to seek out key information within disclosure statements, and to identify resources for assisting with comprehension of complex information. To implement effective consumer education initiatives, it will be important to determine the best messengers and key target audiences, as well as the most appropriate media for communicating messages.

5.5.1. Profiling

It is apparent that consumers are not generally aware of profiling tactics that are common in the m-payments ecosystem. While evidence suggests that consumers are becomingly increasingly comfortable with profiling in e-commerce, there is contradictory evidence when it comes to profiling based on consumers' use of mobile devices, including geo-tracking. Generally, consumers are not comfortable with these practices at present. A first step may be to inform consumers of mobile profiling in order to increase the general level of transparency of the practice. A second step may be to inform consumers of their rights related to profiling and how to go about changing the preferences on their mobile devices.

5.5.2. Malware

In the near term, there is a consumer protection gap with regard to threats from malware, which can place consumers at risk of identity theft and fraud. When it comes into force, the anti-spam legislation could provide a solid foundation for addressing these threats. In the meantime, a good approach to mitigating the risks may be to increase consumer awareness of malware threats. Consumers are very concerned about the security of their information on mobile devices, but it appears that their general level of knowledge about malware threats is quite limited. Since many of the controls that can be implemented to protect against malware require users' active participation, it is essential to increase awareness of the threats. It is also essential to put in place processes to inform consumers of what these controls are and how best to implement them.

5.5.3. Informing consumers

An excellent method for informing and empowering consumers could be the development and promotion of mobile applications, enabling users to compare and contrast payment options and gain insights into other relevant m-payment information quickly and on the move. For instance, apps would be likely to benefit peer-to-peer m-payment users by enabling them to identify and compare international remittance service providers. Equally useful could be education about which foreign jurisdictions use interoperable technology and how m-payments are protected. An example of a useful tool for consumers is the mobile app recently launched by the Office of the Privacy Commissioner of Canada, with the aim of educating mobile users on how to "better protect personal information on their mobile devices" (Office of the Privacy Commissioner of Canada, 2013).

References

- American Express. (2013). *Amex Sync*. Retrieved March 13, 2013, from American Express: sync.americanexpress.com
- Arrowsmith, S., & Pignal, J. (2010). *Initial Findings from the 2009 Canadian Financial Capability Survey*. Ottawa: Canadian Task Force on Financial Literacy.
- Au, Y. A., & Kauffman, R. J. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications*, 7(2), 141-164.
- Bango. (2012). *Bango Annual Report 2012*.
- Bank Act* (S.C. 1991, c. 46). (n.d.). Retrieved March 7, 2013, from laws-lois.justice.gc.ca
- Barton, C., Fromm, J., & Egan, C. (2012). *The millennial consumer: Debunking Stereotypes*. The Boston Consulting Group Inc.
- Blow, M. (2012). *Statement for the Record of Marla Blow before the House Financial Services Subcommittee on Financial Institutions and Consumer Credit*. House Financial Services Subcommittee.
- Budnitz, M. E. (2012, January). Mobile Financial Services: The Need for a Comprehensive Consumer Protection Law. *Banking & Finance Law Review*, 27(2), 213-232.
- Canadian Bankers Association. (2012a). *Canadian NFC Mobile Payments Reference Model*.
- Canadian Bankers Association. (2012b). *How Canadians Bank*. CBA.
- Canadian Bankers Association. (2012c, February 23). Credit Card Statistics—VISA and MasterCard. Retrieved March 13, 2013, from www.cba.ca
- Canadian Bankers Association. (2012d). *Credit Card Fraud and Debit Card Fraud Statistics—Canadian Issued Cards*.
- Canadian Bankers Association. (2012e, May 24). *Contactless Payment Card Security—An FAQ*. Retrieved November 26, 2012, from Canadian Bankers Association: www.cba.ca
- Canadian Payments Association. (2012). *Examining Canadian Payment Methods and Trends*. Ottawa: CPA.
- Canadian Wireless Telecommunications Association. (2012). *Industry Facts and Figures*. Retrieved November 5, 2012, from Canadian Wireless Telecommunications Association: www.cwta.ca

- Capgemini; Royal Bank of Scotland; European Financial Management Association. (2011). *World Payments Report 2011*. Capgemini and The Royal Bank of Scotland.
- Chari, S., Kermani, P., Smith, S., & Tassioulas, L. (2000). Security Issues in M-Commerce: A Usage-Based Taxonomy. In J. Liu, & Y. Ye (Eds.), *E-Commerce Agents: Marketplace Solutions, Security Issues, and Supply and Demand* (pp. 264-282). Berlin: Springer.
- Competition Act* (R.S.C., 1985, c. C-34). (n.d.).
- Competition Bureau. (2012, September 14). *Competition Bureau Sues Bell, Rogers and Telus for Misleading Consumers: Bureau Seeks Customer Refunds and \$31 Million in Penalties*. Retrieved from Competition Bureau: <http://www.competitionbureau.gc.ca>
- Competition Bureau. (2009). *Enforcement Guidelines: Application of the Competition Act to Representations on the Internet*.
- comScore. (2012). *Canada Digital Future in Focus 2012*.
- Consumer Measures Committee. (1998). *Agreement for Harmonization of Cost of Credit Disclosure Laws in Canada: Drafting Template*.
- Contini, D., Crowe, M., Merritt, C., Oliver, R., & Mott, S. (2011). *Mobile Payments in the United States: Mapping Out the Road Ahead*. Federal Reserve Bank of Boston, Federal Reserve Bank of Atlanta.
- Cost of Borrowing (Banks) Regulations* (SOR/2001-101). (n.d.). Retrieved March 7, 2013, from laws-lois.justice.gc.ca
- Criminal Code* (R.S.C., 1985, c. C-46). (n.d.).
- Crowe, M., & Tavilla, E. (2012). *Mobile Phone Technology: "Smarter Than We Thought."* Federal Reserve Bank of Boston.
- Crowe, M., Kepler, M., & Merritt, C. (2012). *The U.S. Regulatory Landscape for Mobile Payments: Summary Report of Meeting between Mobile Payments Industry Workgroup and Federal and State Regulators*. Boston, MA: Federal Reserve Bank of Boston and Federal Reserve Bank of Atlanta. Retrieved February 11, 2013, from <http://www.bos.frb.org/>
- CRTC. (2012, March 28). *Telecom Regulatory Policy CRTC 2012-183*. Retrieved March 14, 2013, from CRTC: www.crtc.gc.ca
- CRTC. (2013, June 6). *The Wireless Code*. Retrieved June 24, 2013, from CRTC: www.crtc.gc.ca

- Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2006). Mobile Payment Market and Research—Past, Present and Future. *Proceedings of Helsinki Mobility Roundtable. 6(48)*, pp. 1-12. Helsinki: Sprouts: Working Papers on Information Systems.
- Dapp, T. F., Stobbe, A., & Wruuck, P. (2012). *The future of (mobile) payments: New (online) players competing with banks*. Deutsche Bank.
- Deloitte. (2012). *Dialing in: The future of mobile payments in Canada*. Deloitte & Touche LLP.
- Demirguc-Kunt, A., & Klapper, L. (2012). *Measuring Financial Inclusion: The Global Findex Database*. The World Bank.
- Department of Finance Canada. (1999). *Reforming Canada's Financial Services Sector: A Framework for the Future*. Ottawa.
- Disclosure of Charges (Banks) Regulations (SOR/92-324)*. (n.d.).
- eMarketer. (2012, September 6). *Twitter Tops Facebook in US Mobile Advertising Revenue*. Retrieved from eMarketer: www.emarketer.com
- EnStream. (2012). *Merchant Impact and Adoption*. Retrieved November 5, 2012, from Enstream: www.enstream.com
- Federal Trade Commission. (2013a). *Mobile Privacy Disclosures: Building Trust through Transparency*. Washington: FTC.
- Federal Trade Commission. (2013b). *Mobile Cramming Roundtable*. Washington: FTC.
- Federal Trade Commission. (2013c). *Paper, Plastic...or Mobile? An FTC Workshop on Mobile Payments*. Washington: FTC.
- F-Secure. (2013). *Mobile Threat Report, Q4 2012*. F-Secure Labs.
- G Data SecurityLabs. (2011). *Bi-annual report: July–December 2011*.
- Ghag, O., & Hegde, S. (2012). A Comprehensive Study of Google Wallet as an NFC Application. *International Journal of Computer Applications, 58(16)*, 37-42.
- Government Accountability Office. (2012a). *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy*. GAO.
- Government Accountability Office. (2012b). *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged*. GAO.

- Government of Canada. (2011, August 3). *Fast Facts*. Retrieved March 14, 2013, from Canada's Anti-Spam Legislation: fightspam.gc.ca
- Grami, A., & Schell, B. H. (2004). Future Trends in Mobile Commerce: Service offerings, technological advances and security challenges. *Proceedings of the 2nd Annual Conference on Privacy, Security and Trust*.
- Hildebrandt, M. (2008). Profiling and the rule of law. *Identity in the Information Society*, 1, 55-70.
- Hough, A. (2012, March 23). *Barclays "contactless" cards exposed to fraud*. Retrieved February 20, 2013, from *The Telegraph*: www.telegraph.co.uk
- iHub Research; Research Solutions Africa. (2012). *Mobile Phone Usage at the Kenyan Base of the Pyramid*. iHub Research; Research Solutions Africa.
- Infineon. (2012). *Security on NFC-enabled platforms: Building trust in the new mobile applications ecosystem*. Neubiberg, Germany: Infineon Technologies AG.
- Interac. (2012). *Interac Online for Customers*. Retrieved March 11, 2013, from Interac: www.interac.ca
- Jack, W., & Suri, T. (2011). *Mobile Money: The Economics of M-PESA*. The National Bureau of Economic Research.
- Jun, M. (2011). *Closing the Gap Between Mobile Payment Systems and Consumer Protections*. Consumers Union.
- Juniper Research. (2011). *Whitepaper: Mobile Money Goes Mainstream*. Hampshire, UK: Juniper Research.
- Kamleitner, B., Dickert, S., Falahrastegar, M., & Haddadi, H. (2013). Information Bazaar: a Contextual Evaluation. *HotPlanet '13*. Hong Kong.
- Kim, C., Mirusmonov, M., & Lee, I. (2010). An empirical examination of factors influencing the intention to use mobile payment. *Computers in Human Behavior*, 26, 310–322.
- King, D. (2012). *Chip-and-PIN: Success and Challenges in Reducing Fraud*. Retail Payments Risk Forum.
- King, N. J., & Jessen, P. W. (2010). Profiling the mobile customer—Privacy concerns when behavioural advertisers target mobile phones—Part 1. *Computer Law & Security Review*, 26(5), 455-478.

- KPMG International. (2007). *Mobile payments in Asia Pacific*. Hong Kong: KPMG.
- Lachaal, L., & Zhang, J. (2012, December). Mobile Money Services, Regulation and Creating an Enabling Environment in Africa. *Africa Capacity Development Brief*, 3(2).
- Liu, S., & Zhuo, Y. (2012). *The Consumer Implications of the Use of Electronic and Mobile Payment Systems*. Ottawa: Financial Consumer Agency of Canada.
- MasterCard Advisors. (2012). *MasterCard Advisors PayPass adoption study*. Press Release. Retrieved November 9, 2012, from www.mastercardadvisors.com
- MasterCard Worldwide. (2012). *Mobile Payments Readiness Index*.
- Melecky, M., & Rutledge, S. (2011). *Financial Consumer Protection and the Global Financial Crisis*. World Bank.
- Miller, C. (2012). *Exporing the NFC Attack Surface*. Denver: Accuvant Labs. Retrieved February 22, 2013, from <http://media.blackhat.com>
- Montgomery, K. C. (2012). *Statement to the Senate Hearing on Mobile Payments*. Committee on Banking, Housing, and Urban Affairs. Washington, D.C.: U.S. Senate.
- Negative Option Billing Regulations (SOR/2012-23)*. (n.d.).
- OECD. (2008). *OECD Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce*. Paris: OECD.
- OECD. (2010). *Addressing Financial Consumer Protection Deficiencies in the Post Crisis Era*. Paris: OECD.
- OECD. (2011). *G20 High-level Principles on Financial Consumer Protection*. Paris: OECD.
- OECD. (2012). *Report on Consumer Protection in Online and Mobile Payments, OECD Digital Economy Papers, No. 204*. Paris: OECD Publishing.
- Office of the Privacy Commissioner of Canada. (2012b). *Policy Position on Online Behavioural Advertising*. Ottawa: OPC.
- Office of the Privacy Commissioner of Canada. (2012a). *Guidelines: Privacy and Online Behavioural Advertising*. Ottawa: OPC.
- Office of the Privacy Commissioner of Canada. (2013, January 28). *Privacy Commissioner launches privacy mobile application*. Retrieved March 28, 2013, from Office of the Privacy Commissioner of Canada: www.priv.gc.ca

- Ondrus, J., Lyytinen, K., & Pigneur, Y. (2009). Why Mobile Payments Fail? Towards a Dynamic and Multi-perspective Explanation. *System Sciences HCISS 42nd International Conference on Computing and Processing*. Hawaii: IEEE.
- Oxford University Press. (2013). Smartphone. Retrieved March 18, 2013, from Oxford Dictionaries: oxforddictionaries.com
- Pernet-Lubrano. (2010). Mobile Payments: Moving Towards a Wallet in the Cloud? *Communications & Strategies*, 79, 63-71.
- Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5). (n.d.).
- Quorus Consulting Group Inc. (2012). *2012 Cell Phone Consumer Attitudes Study*. Canadian Wireless Telecommunications Association. Retrieved November 2, 2012, from <http://cwta.ca>
- Robson, J. (2011). *Financial Literacy in Canada: Setting a baseline*. Ottawa: Financial Consumer Agency of Canada.
- Scassa, T., & Deturbide, M. (2012). *Electronic Commerce and Internet Law in Canada* (2nd ed.). Toronto: CCH Canadian Limited.
- Smart Card Alliance. (2011). *The Mobile Payments and NFC Landscape: A US Perspective*. Smart Card Alliance.
- Sproule, S., & Archer, N. (2008). Measuring Identity Theft in Canada: 2008 Consumer Survey—Working Paper #23. McMaster University. Retrieved June 12, 2013, from <http://merc.mcmaster.ca>
- Task Force for the Payments System Review. (2011). *Going Digital: Transitioning to digital payments*.
- Technology Strategies International. (2012). *Canadian Payments Forecast—2012*. Press Release, Oakville ON. Retrieved November 9, 2012, from <http://www.tsiglobalnet.com>
- Urban, J. M., Hoofnagle, C. J., & Li, S. (2012). *Mobile Phones and Privacy*. BCLT Research Paper.
- Veniard, C., & Goss, S. (2012, January). Mobile Payments in the Philippines: Future Opportunities for Growth. *Lydian Journal*(8).
- Wolfsberg Group. (2011). *Wolfsberg Guidance on Prepaid & Stored Value Cards*. The Wolfsberg Group.

Working Group on Electronic Commerce and Consumers. (2004). *Canadian Code of Practice for Consumer Protection in Electronic Commerce*. Ottawa: Industry Canada.

World Bank. (2012). *The Little Data Book on Financial Inclusion*. Washington: World Bank.

Zhou, Y., & Jiang, X. (2012). Dissecting Android Malware: Characterization and Evolution. *2012 IEEE Symposium on Security and Privacy* (pp. 95-109). San Francisco: IEEE Computer Society. Retrieved February 23, 2013, from <http://iee-security.org>