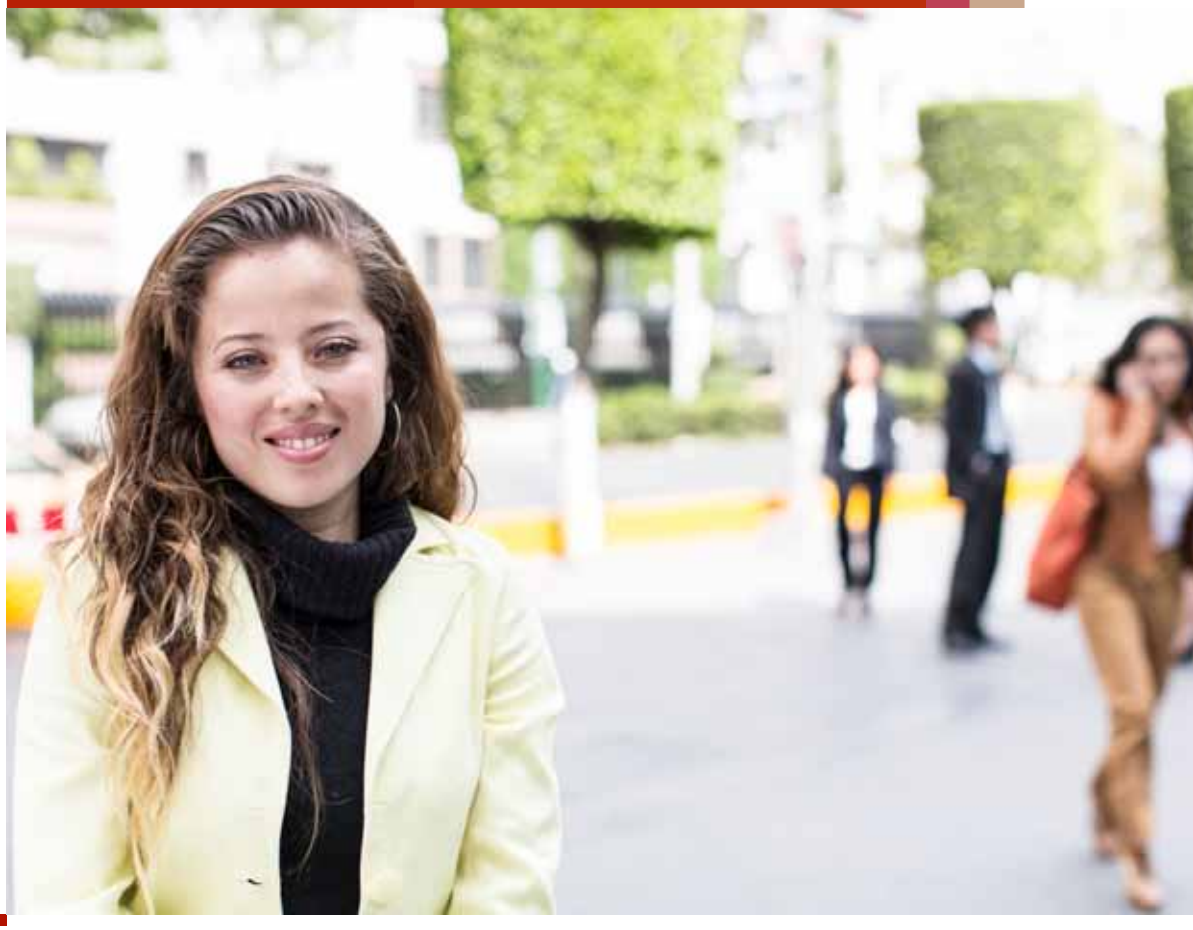
Mobile payments: Is trust the key to consumer uptake?

Banking Review

Winter 2013



pwc

The mobile landscape

Smartphones are increasingly becoming an indispensable tool in daily life. Many Canadians own smartphones and the numbers are growing exponentially. A vast majority may leave their wallets behind but can't think of going anywhere without their phones. As new services emerge, Canadians are starting to research and shop using their smartphones, with 20% of smartphone users having made a purchase on their phone.[1] In fact, smartphone market use has grown from 33% to 48% from 2011 to 2012.[2] The implication is clear: mobile will become pervasive and having a coherent strategy is critical to customer engagement.

Canadian banks have started going down this path and have introduced mobile banking on major smartphone platforms: BlackBerry, Apple and Android. However, adoption of mobile banking has been slow. According to a PwC survey of Canadian consumers[3], just 22% of Canadians use mobile banking applications on their smartphones. That said, online traffic has begun shifting from personal computers to mobile devices, and tablets are replacing desktops. A range of players, including PayPal, Google and Starbucks, have begun offering mobile payments and launched mobile payment platforms back in 2011.

A mobile payment transaction allows the transfer of value from one entity to another —person to person, person to a merchant or between merchants. The use of the word 'value' is deliberate – besides funds, value transfers can encompass coupons, offers and loyalty points. In the past, payments were the exclusive domain of banks. Bank-owned or bank-participated networks were the primary basis for funds transfers. With smartphone adoption, a range of new players – telephone companies, technology providers and device manufacturers – see an opportunity to provide services and secure their share of transaction rewards. This is important to banks, which have never had to trust someone else's systems to carry out their customers' payment transactions. More importantly, as a channel, mobile awards less exclusivity to banks when interacting with their customers. This is an uncomfortable position for banks to be in, but this is an issue they'll have to address head-on to succeed with mobile payments.

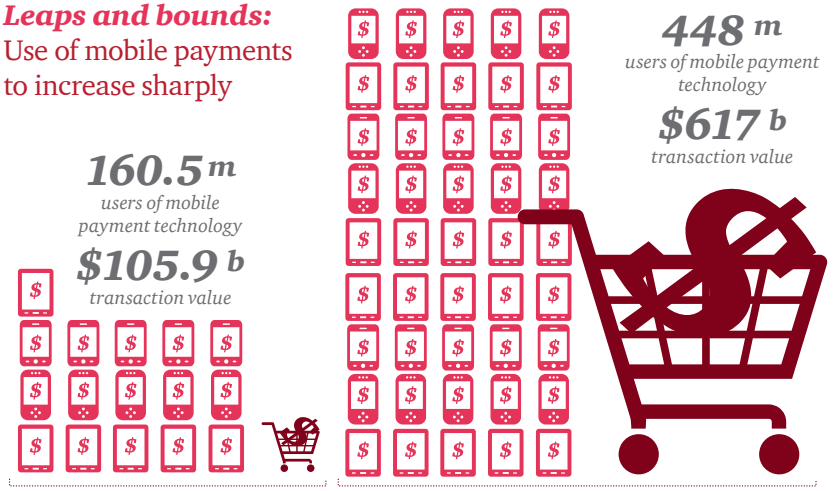
There's potential for Canadian banks to gain a competitive advantage as consumers already hold their banks to high standards of accountability, with 84% holding banks responsible for safeguarding privacy.[4] A PwC financial mobile services consumer survey also shows that 67% of those surveyed from Canada and the US would prefer that their mobile payments be enabled by their banks.[5] And 76% say that regardless of who provides the service, they want the money to come out of their bank account and go into the receiving party's bank account. They appear generally apprehensive of funds sitting in intermediate locations before being settled via the banking system – giving rise to trust and security issues.

Trust then is the key in unlocking the potential of mobile payments. With traditional boundaries being extended, participation and collaboration in an extended ecosystem—banks, mobile networks, device manufacturers, technology companies and other service providers—become critical. There are now many more touch points where a consumer's private and confidential information can be compromised. And consumers are worried.

The rise of the digital wallet: Mobile payments to surge in the next four years

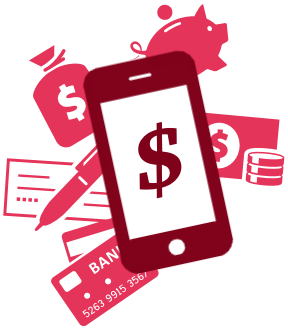
Smartphones are changing the way people make transactions in all parts of their life, rapidly becoming the Swiss Army® knife of the gadget world.

Leaps and bounds: Use of mobile payments to increase sharply



each smartphone represents 5 million mobile payment users
Source: Gartner

Money on the move: The five applications of mobile payments



1. **The mobile wallet**
   Payment using a smartphone equipped with a near field communication (NFC) chip or a "tap-and-go" app to allow users to make small-ticket purchases
   Examples: CIBC & Rogers, Google wallet, Mastercard Paypass
2. **Every smartphone is a cash register**
   A merchant using a mobile device through location proximity servers to process credit card transactions.
   Example: Square
3. **The everything else mobile payment**
   Catch-all category for products that let consumers send money to merchants or even to each other, using mobile devices. This could be at the point of sale, email or via text message.
   Example: PayPal
4. **Telling digital merchants to "put it on my bill"**
   Also known as direct carrier billing, it involves consumers buying digital content, such as ringtones or games, and having it charged directly to their cell phone bills.
   Example: Bango, Zong (a PayPal service)
5. **The return of the store credit card**
   Some companies are building their own mobile platforms. It's equivalent to having a store credit card, only mobile.
   Example: Starbucks

Source: moblepaymentstoday.com and Acquity Group

1. Google. *Our Mobile Planet: Canada, Understanding the Mobile Consumer*. May 2012. Retrieved from http://services.google.com/fh/files/blogs/our_mobile_planet_canada_en.pdf.
2. Quorus Consulting Group. *2012 Cell Phone Consumer Attitudes Study*. April 23, 2012.
3. PwC. Canadian consumer survey 2012.
4. PwC. *Citizen Compass: Next generation of eservices*. 2012.
5. PwC. Financial mobile services consumer survey 2011.

The challenge

Our survey of Canadian consumers also reveals that security risk and fraud is a top concern for 78% of respondents when it comes to mobile payments, while 69% are worried about the privacy of their data.[6] Besides the banks, participants were also asked if there were any others in the extended ecosystem that they trusted with their financial data – the overwhelming response was "no".

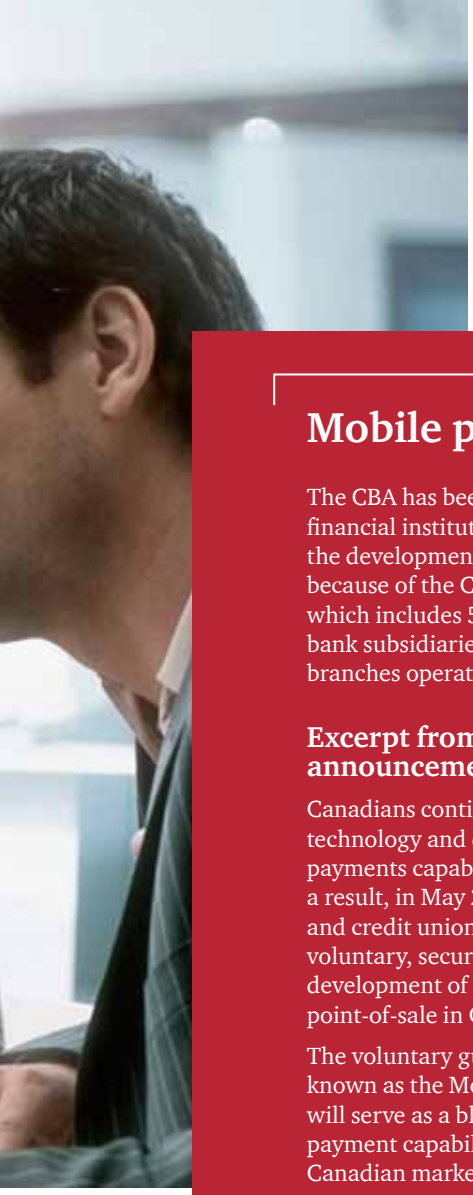
These responses are not surprising and hold the key to how financial institutions, or for that matter service providers, should move forward to ensure their place in the mobile payments ecosystem. Canadian banks start from a position of strength: they've proven they can safeguard their customers' financial data and in turn have secured their trust.

But can this trust be maintained? Until recently, payments have been managed within tight boundaries, where banks could exercise influence. With mobile payments, the ecosystem is extended. No single organization will be able to control all forms of value transfers from an end-to-end perspective, single handedly guarantee the security of the transaction, and in turn seek the associated rewards.

For banks to acquire and even extend their revenue potential from mobile payments, they'll have to play an active role in the enforcement of standards across the ecosystem. End-to-end security hinges on all the participants collaborating to create these standards that can evolve as technology changes and as risk and potential threats emerge. An excellent illustration of this collaboration is the near field communications (NFC) voluntary guidelines, known as the Mobile Reference Model, supported by the Canadian Bankers Association (CBA). But key questions remain:

- How will consumers be protected when fraudulent payments occur?
- Who will indemnify them?
- Up to what amount will they be indemnified?
- Will some of these costs be borne by merchants?
- How will costs be apportioned between participating ecosystem players?

6. PwC. Canadian consumer survey 2012.



Mobile payments in Canada

The CBA has been asked by the Canadian financial institutions to help coordinate the development of the mobile guidelines because of the CBA's broad membership which includes 54 domestic banks, foreign bank subsidiaries and foreign bank branches operating in Canada.

Excerpt from a CBA announcement:[7]

Canadians continue to adopt mobile technology and demand for mobile payments capability continues to grow. As a result, in May 2012 the banking industry and credit union system announced a set of voluntary, secure, open guidelines for the development of mobile payments at the point-of-sale in Canada.

The voluntary guidelines, technically known as the Mobile Reference Model, will serve as a blueprint for how mobile payment capabilities can be offered in the Canadian market.

The 133-page model begins with a set of guiding principles for mobile payments in Canada, explaining that they must be[8]:

Open

- Allow for different business models
- Foster innovation
- Ensure competition among market participants

Safe and secure

- Protect confidential personal, financial and transactional information within the mobile payments ecosystem
- Facilitate secure interactions between financial institutions and the mobile payments ecosystem

Responsive to end user and merchant needs

- Provide for ease of use, speed, availability, security, transparency, choice and consistency for users

Standards-based

- Establish clearly defined standards essential for interactions between financial institutions and the mobile payments ecosystem
- Align with the Canadian regulatory environment and avoid overlap with existing standards
- Consider and respect international standards as a means of facilitating interoperability

Sustainable

- Create a path forward for standards to support the long-term viability of mobile payments in Canada
- Encompass activities between financial institutions and the mobile payments ecosystem
- Adapt over time as technology and the ecosystem evolve
- Allow for economically viable business models that accelerate mobile payments adoption for the mobile payments ecosystem

7. Canadian Bankers Association. *Mobile Payments in Canada*. July 19, 2012. Retrieved from http://www.cba.ca/en/component/content/category/89-mobile-payments-in-canada.
8. NFC World. *Canadian banks issue landmark NFC payments guideline*. May 14, 2012. Retrieved from http://www.nfcworld.com/2012/05/14/315691/canadian-banks-issue-landmark-nfc-payments-guidelines.

What about the US?

On March 22, 2012, the Congressional subcommittee on Financial Institutions and Consumer Credit hosted a hearing titled 'The Future of Money: How Mobile Payments Could Change Financial Services.' This was one of the first meetings hosted by Congress on the topic, and expert panelists ranging from the Federal Reserve to industry participants (MasterCard, PCI Security Standards Council (PCI SSC), Smart Card Alliance) were brought in to explain the basics of mobile payments and address concerns.[9]

Chief among the concerns of many Members of Congress were questions surrounding security.

Today, according to PCI SSC, mobile payment security can be divided into two categories:[10]

- Merchant acceptance applications where phones, tablets, and other mobile devices are used by merchants as POS terminals in place of traditional hardware terminals
- Consumer facing applications where the phone is used in place of a traditional payment card by a consumer to initiate payments

Notably, the PCI SSC has only concentrated on providing requirements and guidance to the first category — securing the use of mobile devices as a point of sale acceptance tool. As for the second category of applications, there are no regulators, forums, roadmaps or industry standards that wallet providers can refer or adhere to.[11,12] This is likely to change in the coming years and represents a potential area of growth for trusted mobile security players.

This is an excerpt from *Opportunity calls: An update on the evolution of mobile payments.*

To read the rest of this publication please go to:

www.pwc.com/us/en/banking-capital-markets/publications/evolution-mobile-payments-update.jhtml

9. United States Congress Committee on Financial Services. Hearing entitled "*The Future of Money: How Mobile Payments Could Change Financial Services*." March 22, 2012. Retrieved from http://financialservices.house.gov/Calendar/EventSingle.aspx?EventID=284912.
10. Troy Leach, PCI Security Standards Council. Prepared Remarks for "*The Future of Money: How Mobile Payments Could Change Financial Services*." March 22, 2012. Retrieved from http://financialservices.house.gov/UploadedFiles/HHRG-112-BA-WState-TLeach-20120322.pdf.
11. Darin Contini, Marianne Crowe, Cynthia Merritt, and Richard Oliver, Federal Reserve. *Mobile Payments in the United States: Mapping Out the Road Ahead*. March 25, 2011. Retrieved from http://www.bostonfed.org/bankinfo/payment-strategies/publications/2011/mobile-payments-mapping.htm.
12. Richard Oliver. Prepared Remarks for "*The Future of Money: How Mobile Payments Could Change Financial Services*." March 22, 2012. Retrieved from http://financialservices.house.gov/uploadedfiles/hhrg-112-ba-wstate-roliver-20120322.pdf.

Keeping consumer data secure

Within many banks, operations, risk and technology are still worlds apart, making it very difficult to generate integrated information and insights. Why is this?

Banks need to extend their frameworks for managing security and privacy to their partners and third parties to deliver the same degree of assurance to customers as provided by Canadian banks. This is by no means a small task and banks will be increasingly under pressure to play the role of the gate keeper in keeping their customers' data secure – even when customers use third-party services.

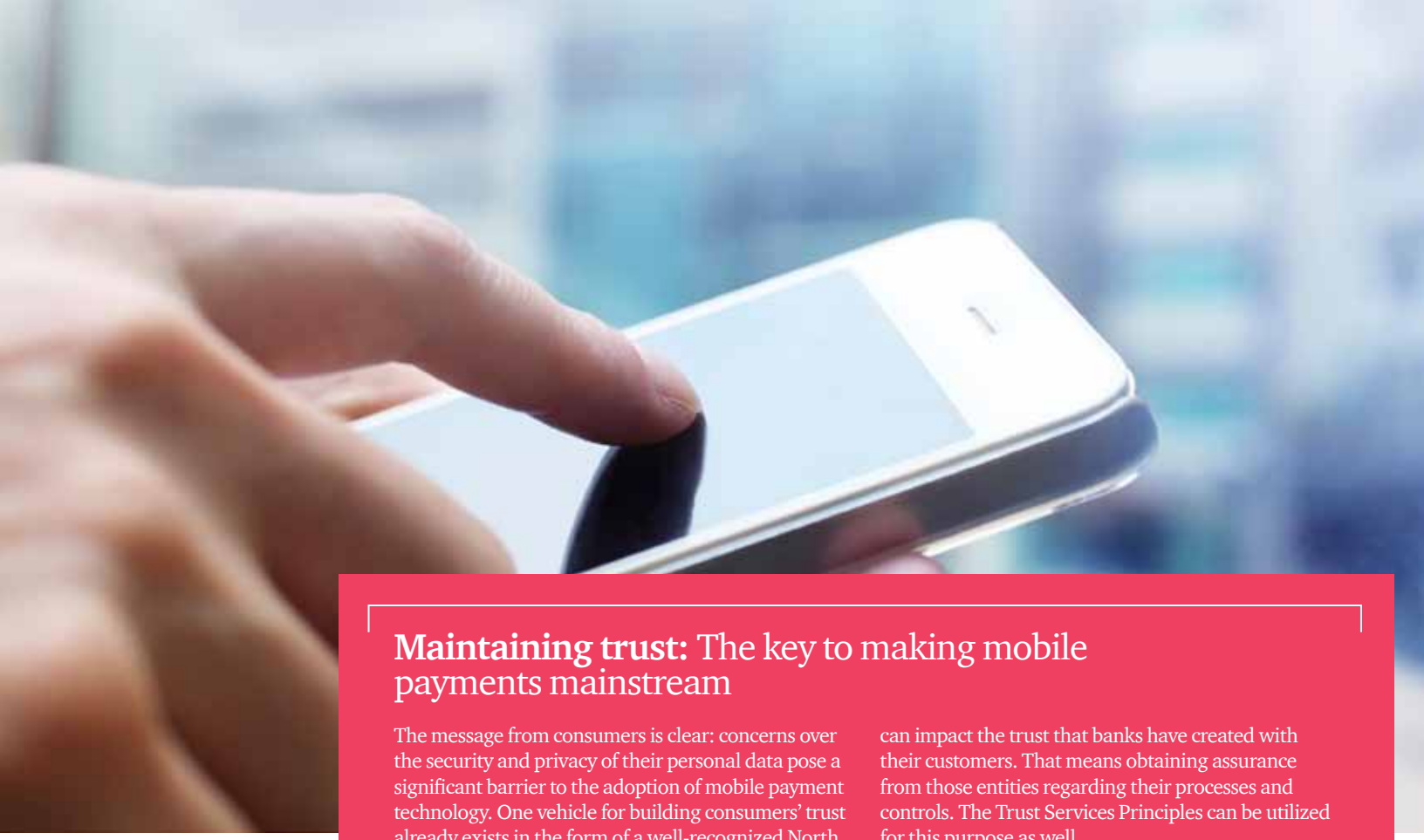
What can banks do? The first step is to help establish and propagate a set of standards that is both robust and widely accepted by the expanded ecosystem—banks, cell phone makers, mobile networks, technology companies—and to constantly evolve those standards. Security threats constantly evolve and all participants will need to embrace a coordinated approach when dealing with new fraud and security threats.

The next step is to ensure standards are enforced and compliance demonstrated. This will go a long way in building trust with consumers. Some banks are considering third-party assurance to critique standards and review how banks and their partners will jointly deliver these standards. This third-party assurance seal can serve two purposes:

(i) Provide executive management consolation that the bank's risk assessment and control procedures align with those of the service providers

(ii) Together, the bank and its partners will provide business processes that deliver the required degree of security and trust

Such assurance may also be critical from a regulatory perspective and may provide a competitive differentiation for banks in the short term.



Maintaining trust: The key to making mobile payments mainstream

The message from consumers is clear: concerns over the security and privacy of their personal data pose a significant barrier to the adoption of mobile payment technology. One vehicle for building consumers' trust already exists in the form of a well-recognized North American framework —the Trust Services Principles. This framework can be leveraged through assurance reporting on existing governance structures, processes and controls to provide an independent assessment of banks' mobile payment operations. As the use of technology and the number of players delivering ecommerce increases, trust reporting and independent assurance around non-financial risk is becoming increasingly important to all stakeholders and will likely become standard operating procedure in the near future.To use the Trust Services Principles, you should first identify the five criteria to report to your stakeholders about:

1. privacy
2. confidentiality
3. processing integrity
4. availability
5. security

Different stakeholders will have different concerns. For example, a merchant would be most concerned that the system is available for operation and use, while an individual will want to be reassured that their privacy and data is protected. Banks can then tailor their reports to satisfy the needs of each category of client and build the confidence necessary to encourage adoption.

The mobile payments ecosystem has grown to include new players including mobile networks, and banks should ensure that new entrants are equally stable, secure and controlled as the banks to maintain the same level of trust. The mobile payments process will only be as strong as each individual player. Banks must have confidence in each of those players as they can impact the trust that banks have created with their customers. That means obtaining assurance from those entities regarding their processes and controls. The Trust Services Principles can be utilized for this purpose as well.

The Trust Services Principles also provide the opportunity for banks and their business partners to obtain third party trust services seals (WebTrust™ and SysTrust℠) to demonstrate to end users that their systems and processes are reliable and comply with ecommerce standards. The seals can be placed on their websites to give a visual representation that there's been an independent evaluation. By clicking on the seal, stakeholders will have access to the report and the measures put in place to protect their data.

When asked as part of PwC's consumer survey[13], 43% of Canadians told us that the presence of a third party certification seal has influenced their decision in trusting a website in the past. Furthermore, when asked about the websites they would trust enough to purchase from today, 62% indicated that they would only use established websites while 21% told us that they would rely on third party certificates. At first glance the level of reliance on third party certificates may appear low. But when understood in context with the ratio of online commerce concentrated between the top websites and ecommerce arms of brick and mortar retailers, the fact that 21% of consumers are willing to consider certified – but not well established – websites is a key to success of emerging retailers, or any other party involved in financial transactions, such as emerging payments providers.

Implementing a trust services framework will give early adopters a competitive advantage by providing a means to enhance trust and transparency — a critical success factor in allaying consumer concerns around mobile payments.

13. PwC. Canadian consumer survey 2012

Conclusion

Payment transactions constitute an important source of revenue for banks worldwide. For Canadian banks, this opportunity is even more pronounced given the degree of trust established with their customers.

While standards continue to evolve and expand beyond NFC, two dimensional (2D) code and cloud processing technologies, banks can adopt several key practices to ensure they acquire their fair share of revenues generated within the mobile ecosystem:

- **Know your risks:** Focus on new points in the transaction life cycle where customer data can be compromised. Some of these break points will be outside the domain of the banks.
- **Develop a collaboration model to interact with ecosystem participants, both known and emerging:** Clarify how trust will be managed, what controls will be deployed, what assurance can be obtained that such controls are functioning and effective and how risks will be shared. Embrace a formal due diligence model to certify third-party service providers.
- **Educate consumers:** The risks associated with the use of wallets and other services, such as couponing, offers, loyalty points and in general sharing of personal information, need to be clarified together with liability disclosures. Mobile payments allow for the collection of a significant volume of information, and not all customers may want this information used or shared inappropriately.
- **Be technology agnostic:** Mobile technologies are still in their infancy and will mature over time. With new tools come new risks of inadvertent disclosures and opportunities for deliberate intrusions. Validate new technologies critically with a focus on customer ease-of-use, financial integrity, information risk and privacy.

What about merchants?

Merchants will exert significant influence on the pace of adoption of mobile payments. While significantly encouraged by the potential to improve customer interaction with targeted offers, location aware services, coupons and loyalty rewards, merchants continue to be concerned about the costs associated with payment transactions.

Merchants are important banking customers and in growing their mobile portfolio, banks will have to balance the needs of the merchants and the needs of their customers. A universally beneficial approach is for banks to not only offer the merchants a new channel to distribute offers (ie. coupons, rewards, etc.), but also combine the silos of information (with the explicit permission of its customers) to enable the delivery of these targeted offers. Furthermore, banks could use their aggregated consumer behaviour data to offer value-added services such as benchmarking, trend analysis and forecasting to smaller merchants who may not be able to do so themselves on a cost effective basis.

For more information, please contact:

Balaji Jairam
Director, Consulting & Deals
416 687 8618
balaji.jairam@ca.pwc.com

George Warfel
Director, FS Banking Advisory (US)
415 498 7448
george.h.warfel@us.pwc.com

Sasan Parhizgari
Manager, Consulting & Deals
416 947 8903
sasan.parhizgari@ca.pwc.com

Recent PwC banking and capital markets publications

To view these publications, please visit our website at www.pwc.com/ca/banking and click on Publications.

Opportunity calls: An update on the evolution of mobile payments

The escalation of mobile has begun to impact financial services companies, and is changing the way we think about payments. While a dominant player has not yet emerged, and consumers have still not widely adopted mobile payments, new developments have occurred, providing a glimpse of the future.

Gaps in the apps: Why the traditional security lifecycle no longer works

As banks race to develop mobile banking apps that satisfy consumer demands, how can they guard against the security breaches that could damage their reputation and prompt customers to flee?

FS Viewpoint – Dialing up a storm: How mobile payments will create the most significant revenue opportunities of the decade for financial institutions

Mobile services have put over $20 billion in play for FS industry participants. If traditional players don't keep pace, tech innovators will prevail.

Canadian Banks 2012

In this edition of Canadian Banks we look back and examine the 2012 results for the largest six banks in Canada. Read this publication to get industry perspectives into "what's next" and how our banks may tackle the challenges and opportunities that lay ahead.

Changing the game – Key findings from The Global State of Information Security® Survey 2013

For many businesses, security has become a game that is almost impossible to win. The rules have changed, opponents are armed with expert technology skills, and the risks are greater than ever. Using the Global State of Information Security® Survey results, our industry specialists break out the most meaningful findings for the financial services sector.

Banking Banana Skins 2012

The Banking Banana Skins Survey is conducted by the Centre for the Study of Financial Innovation and sponsored by PwC. This survey of leading members of the finance industry seeks to find out their concerns about the soundness of the financial markets and puts together a league table identifying risks to banks and ranks them by severity.

PwC's 15th Annual Global CEO survey: Reigniting growth in a tough market: Key findings in the Banking and Capital Markets sector

Explores CEO confidence in prospects and, how they are building local capabilities and creating new networks for new markets. This is a summary of the findings in the banking and capital markets sector, based on interviews with 122 BCM CEOs in 42 countries.

Mobile Innovations Forecast

Where will the disruptions in mobile innovation arise over the next five years? How will they change consumer and employee behaviour? This ongoing article series looks at analyzing and understanding mobile innovation.

Technology Forecast

This quarterly journal focuses on emerging trends in technology and the strategic options that new technologies can create for the enterprise. Focusing on one main theme per issue, it offers an analysis of technology trends that are changing the way companies do business.

For more information

National Financial Services Leader
Diane Kazarian 416 365 8228

National Financial Services Consulting & Deals Leader
John MacKinlay 416 815 5117

National Financial Services Tax Leader
Emma Purdy 416 941 8433

Global and National Banking and Capital Markets Assurance Leader
Rahoul Chowdry 416 815 5059

Audit and Assurance Group

Greater Toronto Area
Leigh Chalmers 416 869 2359
Diane Kazarian 416 365 8228
Ryan Leopold 416 869 2594
Alaina Tennison 416 814 5784
Jerry Whelan 416 365 8209

Calgary
Michael Godwin 403 509 7322

Edmonton
Barry James 780 441 6838
Gordon Keiller 780 441 6840

Vancouver
Paul Challinor 604 806 7218
Ronnie De Zen 604 806 7065

Montréal
Lyne Dufresne 514 205 5298
Alain Dugal 514 205 5091
Kenneth Hotton 514 205 5292

Quebec City
Raynald Lafrance 418 691 2440

Halifax
James Nicoll 902 491 7434
Nikki Robar 902 491 7453

Tax
Michael Bondy 416 365 2724
Yves Magnan 514 205 5194
Richard Marcovitz 416 365 8821
Jillian Welch 416 869 2464

Wilson & Partners LLP
Steven Baum 416 869 2444
David Glicksman 416 947 8988
Gwen Watson 416 869 8720
James Wilson 416 869 2988

Indirect Tax
Michael Firth 416 869 8718

Transfer Pricing
Emma Purdy 416 941 8433

Consulting and Deals

Corporate Advisory and Restructuring
David Planques 416 815 5275

Dispute Analysis and Valuation
Nikki Robar 902 491 7453
Charlene Rodenhiser 902 491 7462

Corporate Finance
Julian Brown 416 687 8592

Performance Improvement and IT Effectiveness
John MacKinlay 416 815 5117
Paula Pereira 416 941 8460
George Sheen 416 815 5060
Andrew Smee 416 815 5128

Cyber Security
David Craig 416 814 5812
Adriana Gliga 416 815 5148
Salim Hasham 416 365 8860

Financial Risk Management
Jason Boggs 416 941 8311
Allen Ho 416 869 2338
Rani Turna 416 869 2911

Capital Markets
Jason Boggs 416 941 8311

Risk and Regulatory
Jason Boggs 416 941 8311
John Ingold 416 815 5095
Elisabeth Burke 416 687 8589
Allen Ho 416 869 2338
Rani Turna 416 869 2911

Controls
Usuff Currim 416 687 8129
Peter Hargitai 416 941 8464
Jennifer Johnson 416 947 8966
Tony Pedari 416 941 8226

Forensics
Peter Vakof 416 814 5841

If you would like to be added to our mailing list, please email financial.services@ca.pwc.com.

This publication can also be viewed on our website at www.pwc.com/ca/banking.