

RBC: MOBILE WALLET

R. Chandrasekhar wrote this case under the supervision of Professors Nicole Haggerty and Binny Samuel solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

This publication may not be transmitted, photocopied, digitized or otherwise reproduced in any form or by any means without the permission of the copyright holder. Reproduction of this material is not covered under authorization by any reproduction rights organization. To order copies or request permission to reproduce materials, contact Ivey Publishing, Ivey Business School, Western University, London, Ontario, Canada, N6G 0N1; (t) 519.661.3208; (e) cases@ivey.ca; www.iveycases.com.

Copyright © 2016, Richard Ivey School of Business Foundation

Version: 2016-06-08

It was mid-October 2012 in downtown Toronto when Linda Mantia, executive vice-president (Digital, Payments and Cards), Royal Bank of Canada (RBC), and Jeremy Bornstein, head (Emerging Payments), RBC, met with executives from one of Canada's leading telecom operators to discuss the launch of RBC's first mobile wallet.

The mobile wallet, enabled by the telecom operator's wireless network, would replace the customer's leather wallet containing individual credit and debit cards. The wallet was designed by RBC and was housed in a smartphone. As per the prevailing industry norm, the wallet relied on the subscriber identity module (SIM)¹ card, contained in a chip, issued by the telecom operator. The mobile wallet would enable customers to pay for purchases with their card of choice by simply waving the smartphone at the point of sale (POS) terminal at a checkout counter.

The imminent launch of the mobile wallet would give RBC a head start over its peers in the banking industry, which had seen Starbucks, a retailer with no legacy either in financial services or technology, gain instant traction with its mobile payments app launched in 2011.

Mantia was about to sign on the dotted line and close the deal with the telecom operator when she had second thoughts. Bornstein shared her discomfort and Mantia sensed it.

The concerns had come into sharp focus because engineers at RBC had been secretly designing, under Mantia's leadership, a cloud-based solution that could preempt the need to store the data in a SIM card. Working at an innocuous location in Toronto, dubbed among water-cooler channels at RBC as the "Shipyard" because of speculation that big things were being built there, the team was devising a product, tentatively named RBC Secure Cloud that would store customer data in the bank's own servers and route it, as required, through a cloud. The cloud-based solution would be the first of its kind and a departure from the SIM card-based solution, which was the gold standard in the payments industry.

¹ Subscriber identification module (SIM) is a card containing a unique serial number, an international mobile subscriber identity number, security authentication, information related to the local network, a list of the services the user has access to, and two passwords.

Mantia and Bornstein told their telecom counterparts at the meeting that they needed more time. As they walked away from the brink of closing the deal, they were facing a dilemma. Should RBC go forward, even if at a later stage, with a SIM card-based platform that had the support of every telecom operator and payment network but diluted user experience and carried a high cost? Or should RBC launch a cloud-based platform that would reduce costs and improve user experience but force RBC to break rank with peers in an industry that valued alliances?

PAYMENTS INDUSTRY

The annual turnover available from the global payments industry was of the order of US\$1.170 trillion.² This amount consisted of fees charged for processing electronic payments for goods and services. The industry consisted of three segments: business to business (B2B), customer to customer (C2C), and business to customer (B2C).

B2B payments were valued at US\$550 billion in revenues annually. Nearly 50 per cent of B2B payments were made by cheque, involving a two- to three-day time lag. Electronic formats like automatic clearing house (ACH), virtual cards, and payment cards (PCards) were gaining traction. They were designed to ensure not only faster turnaround for banks but lower costs for businesses. C2C payments, valued at US\$30 billion, consisted of the transfer of funds between individual consumers. While banks were the preferred medium for consumers, new technologies (like Instant ACH) and mobile apps (such as Venmo and Square Cash) were facilitating real-time transfers. The bulk of C2C payments consisted of transfer of funds from migrant workers to their families and between unbanked and under-banked individuals in different geographies.

The B2C payment market was the largest, at US\$591 billion. Its ecosystem consisted of consumers, payment networks,³ merchants,⁴ and card issuers⁵. While the payments industry in general was driven by changes in technology and regulation, the B2C segment had an additional driver: demographic composition. Changes in demography were leading to new products like mobile wallets. Millennials had different payment habits than their parents (known as boomers). Sixty per cent of millennials were regularly performing mobile financial transactions.⁶

Data security was one of the factors influencing the course of the payments industry. The course was characterized by three phases of technology — Contactless Transaction, Point to Point Encryption and Tokenization — which were often overlapping. Each phase was marked by a gradual reduction in the number of players who were part of what was known as the “circle of trust.” The wider the circle, the higher the risk of transaction security and vice versa.

² James Schneider et al, “The Future of Finance: Redefining the Way We Pay in the Next Decade,” Goldman Sachs Equity Research, March 10, 2015. All currency in Canadian dollars unless specified otherwise.

³ Visa and MasterCard are examples of payment networks.

⁴ Merchants are the sellers of goods and services who have POS terminals.

⁵ Issuers provide the cards to consumers. They are responsible for front-end processing (routing the electronic transaction from POS to the network) and back-end processing (handling the information flow needed to convert the electronic record created at POS into cash for the merchant).

⁶ David Berman, “TD, BMO Unveil New Mobile Banking Features, Courting Tech-Savvy Clients,” *Globe and Mail*, March 17, 2015, accessed March 18, 2015, www.theglobeandmail.com/report-on-business/td-bmo-unveil-new-mobile-banking-features-courting-tech-savvy-clients/article23512204/.

Contactless Transaction

To help consumers migrate from cash to card, the payment industry added the contactless feature to make it easier and quicker to pay than with swiping and signing. The feature used the medium of radio-frequency identification to transmit the data stored in the magnetic stripe of a credit card. Early adopters were high-volume and low-ticket transaction businesses (like gas stations and convenience stores). No signature or personal identification number verification was required. The flipside of the convenience was that there was a limit to the number of transactions and their individual value. Data theft was also an area of concern for consumers. The circle of trust was the widest (see Exhibit 1); it included in its sphere every player beyond the customer.

Point to Point Encryption

Merchants keen on protecting their clients' data asked the card-issuing bank to set up a system wherein payment data was encrypted the moment it hit the POS terminal. The system used an algorithmic calculation to encrypt the customer information stored in the magnetic strip using indecipherable codes. The codes were sent to the payment gateway for decryption and then passed to the bank for authorization. The bank approved or declined the transaction, depending upon the cardholder's balance. The loop was completed when the merchant at the POS was notified of acceptance or rejection. The process lasted less than a second. The circle of trust excluded the merchant but included everyone else beyond the customer (see Exhibit 2).⁷

Tokenization

Created by EMVCo (a consortium of Euro-Pay International, MasterCard International and Visa International), this marked a further step towards data security. Its principal vehicle was referred to as a token. Once the cardholder data was verified, a token was automatically generated and sent to a centralized secure server for storage. Simultaneously, a random unique number was generated and returned to the POS terminal for use in place of the cardholder data. The server maintained a reference database that allowed the token number to be exchanged for the real cardholder data if it was required again for something like a chargeback. The token number could not be monetized but could be used in a number of business applications as a reliable substitute for the real card data. The circle of trust was limited to the card issuer, token service provider, and the network (see Exhibit 2).

The payments industry consisted of both innovators (delivering value-added services within existing systems) and disruptors (replacing existing systems). Innovators (e.g., PayPal and Amazon) brought in new capabilities, including big-data analytics, to increase the number of electronic transactions. Disruptors (e.g., Bitcoin) eliminated the need for traditional credit/debit card networks. Merchant Customer Exchange threatened to be a major disruptor. It was a joint venture of more than 70 retailers, including Walmart, Target, Best Buy, and CVS together accounting for an estimated US\$1 trillion of annual purchase volume. Formed in 2012, it had a singular mandate of reducing processing fees.

⁷ Acquirer signs up merchants to accept payment cards for the network and arranges processing services for merchants. Examples of acquirers include Global Payments, Chase Payments Tech, and Moneris.

Mobile Payments

Mobile payments were payments made with a smartphone at a POS. The term excluded e-commerce and in-commerce transactions even when they were made with a mobile phone because they were made remotely and not at the POS.

The key tool for mobile payments was the mobile wallet. A mobile wallet let a consumer choose among credit cards, debit cards and account balances to make a payment through a single access point. It had four core capabilities: it was linked to multiple payment sources; it held currency; it operated in both physical (offline) and virtual (online) environments; and it worked with multiple devices.

Mobile payments were in the early stage of development in 2012 and did not match the rigour of traditional payment methods. They were being developed by non-banking start-ups rather than banking incumbents. One of the high-profile start-ups was Softcard, a joint venture set up in 2010 by three U.S. telecom carriers, Verizon, AT&T and T-Mobile. Their aim was to block Google, the only company with a mobile app at the time, from controlling the mobile payments space.

The start-ups had a higher appetite for risk and lower regulatory oversight. They were piggybacking on the payments infrastructure put in place by banks without being accountable for transactional safety and leaving banks to pay the price. They were challenging banks on their own turf.

Many of the technologies under development were not state-of-the-art. For example, Starbucks had dressed up a gift card as a mobile wallet. It used what was known as a Quick Response code to be read by 2D scanners installed at the POS of each of its stores in North America. The chain operated a closed-loop system whereby its mobile wallet could be used only in its own stores. In general, the technologies showed limited evidence of standards, protocols and liability protection. They were therefore vulnerable to security breaches.

Mobile payments were a complex eco-system in which about 40 enterprises from five different industries — financial institutions, retailers, telecom carriers, credit card service providers, and device manufacturers — were vying for place. Each was leveraging its domain expertise in developing a unique business model.

The mobile payments value chain was a picture of contrasts. Those at the front end (e.g., device manufacturers) were backward integrating while those at the back end (e.g., carriers) were forward integrating. U.S. banks were largely blocked out of the space by a consortium of the major telecom networks, while Canadian banks were readying to dive into it. Mantia said:

Banks have a natural competitive advantage in the mobile payments market. In addition to moving money (which is all the non-banking competitors can do), they store money on behalf of clients in the form of deposits and lend money to clients in the form of loans. Banks also have a higher level of public trust. They have extensive bandwidth in risk management and fraud mitigation in addition to expertise in payments processing. They have longstanding relationships with customers. They also have branch networks facilitating local deals with local merchants. Finally, their technology platforms are so enduring that mobile payments are only a feature away. A majority of their customers are also smartphone users.

RBC: COMPANY BACKGROUND

Set up in 1869 as Merchant's Bank of Halifax and named Royal Bank of Canada in 1901, RBC was Canada's largest bank as measured by assets and market capitalization in 2012. It was also the largest card issuer in Canada, with 6.5 million cards. It employed about 80,000 full- and part-time employees serving over 15 million clients in Canada, the United States, and 49 other countries. RBC was driven by a vision of "earning the right to be our clients' first choice."

The vision was being realized through three-pronged strategic goals: holding on to the leadership position in financial services in Canada; providing capital-markets and wealth-management solutions outside Canada; and offering, in targeted markets, products and services complementary to its core strengths. The bank's strategy for growth and profitability had remained consistent over the years while the structure was being fine-tuned regularly.

In October 2012, RBC had restructured its business into five segments: personal and commercial Banking (meeting the banking needs of individuals and businesses), wealth management (serving high net worth individuals); insurance (offering insurance and reinsurance products through various channels); investor and treasury services (serving the needs of institutional clients); and capital markets (comprising global wholesale banking). The business segments were supported by two streams: technology & operations (forming the technological and operational bedrock for the organization) and functions (including finance, human resources, risk management, corporate treasury, and internal audit).

Mobile Banking

RBC had been piloting several in-house projects in mobile banking. In 2000, it partnered with Fido to provide wireless transactional banking services through Fido's Access Finances feature. Potential clients could use their Fido handsets to check account balances, transfer funds and pay bills. In 2007, RBC had teamed up with Visa Canada to pilot a mobile payment service in Ontario that used cellphones, rather than traditional credit cards, for making Visa purchases.

There were three important developments in 2008 at RBC with regard to mobile banking. RBC teamed up with Research In Motion and Thomson Reuters to launch the BlackBerry Partners Fund, a venture-capital fund to invest in mobile applications and services for the BlackBerry platform and other mobile platforms. It also tested the RBC Mobex Mobile Payment Service, which allowed pilot users to send and receive money instantly through text messages on mobile phones. RBC started working with Rogers and Motorola on a specially engineered Motorola feature phone. It was keen on developing an open-loop payment system that could work globally, unlike the closed-loop payment system developed by retailers like Starbucks, which could only work in the captive environment of their own stores.

By 2009, RBC had completed development on its first mobile wallet. Cardholders could tap their phones against merchants' Visa payWave-compatible POS terminals to pay. The challenge was that there were few Visa payWave-compliant terminals in Canada. No one was purchasing feature phones anymore because they did not have options like touch display, multi-tasking, and integrated applications. The world had moved to smartphones, which provided those options and more. By 2010, however, RBC was the first Canadian bank to launch fully integrated mobile-banking applications for select smartphones.

By mid-October 2012, RBC had completed development on the traditional SIM solution for Visa credit cards. It was then that Mantia and Bornstein were meeting with their counterparts at a telecom company but had walked away from signing the deal with it for launching the solution.

RBC Secure Cloud

The RBC Secure Cloud was an in-house initiative for which its two inventors were soon to apply for a patent. Its development was being funded by a budget of \$10 million. It differed from the SIM card-based model in the sense that the payment data would be stored in a private cloud but was similar to this model in the sense that the customer would need a smartphone and an SIM card. A seven kilobyte Java applet would connect the payment data with the near-field communication (NFC) antenna on an NFC-enabled phone. The applet would communicate with the mobile banking app and become whatever type of payment the consumer wanted.

The bank would verify the client's credentials and pre-issue an electronic token that would authorize any purchase up to \$100. To make a purchase, clients would select the desired debit, credit or loyalty card on the phone and enter a passcode. Then, they would wave the smartphone close to the POS terminal to send the token. The smartphone would pull down a new token from the cloud. Tokens were preloaded in case wireless connectivity was not available; soon after connectivity was restored, the tokens would be refreshed, readying the phone to make another payment.

The payment data would be stored at the bank's own data centre instead of on the smartphone and would be transmitted in an encrypted form to the device, one payment token at a time, on demand. The data would be decoded by the applet, and then transmitted to the NFC antenna and into the merchant's POS device.

The circle of trust with RBC Secure Cloud would be limited to the issuer and the token service provider, which were the same entity, RBC (see Exhibit 2). Bornstein said:

There are five prerequisites for a mobile wallet to gain traction. They also distinguish the winners from the losers. First, the mobile wallet must have acceptance at merchant locations. The greater its endorsement by merchants, the firmer would be its hold on the market. Second, it should have interoperability. The more compatible a mobile wallet is with the systems of telecom operators and device manufacturers, the higher would be its penetration. Third, it should be secure. The fear of security breach is the number one barrier to mobile payments adoption. Fourth, it should fit seamlessly with related pieces. It should be able to link the core payment program with loyalty, reward, and incentive plans. Finally, it should provide a platform for marketing data integration. This is particularly relevant at a time now when big data holds promise for all stakeholders in the payments industry.

ISSUES FOR MANTIA AND BORNSTEIN TO CONSIDER

The primary issue was whether to run with the herd or break rank. The former meant playing it safe; the latter meant facing the risks of the unknown. In choosing between the SIM card-based mobile wallet and the cloud-based mobile wallet, Mantia and Bornstein had to weigh five areas of contrast between them.

First, the SIM card had become the industry standard. The cloud was untested in the payments industry although it was becoming popular across industries as a way to store data.

Second, the telecom operator would have free access to customer credentials stored in the SIM card. The free access would turn RBC into a commodity provider of credit. The cloud would not require RBC to share customer data with either the wireless provider or the retailers and device manufacturers.

Third, the SIM card had limited storage, for which other banks would also be competing for space in it. The SIM card inserted into each device was owned by the telecom operator, which, in turn, would be renting out spots to competing banks. The overall space itself was finite. The telecom operators were guarded about sharing information with card issuers on the installed capacity of a SIM card. Although no individual bank knew which banks it was competing with for space, each bank had to have enough space in the SIM card to load the client's credit cards, debit cards, and co-branded cards. A typical RBC customer held an average of 2.1 cards. But customers would be inclined, given the option, to load their SIM card with personal data like their driver's licence, passport, health card and others. Storage capacity was not an issue with RBC Secure Cloud. The space in the cloud was potentially infinite.

Fourth, there was the matter of rack rent. RBC had 6.5 million cardholders. The telecom operator charged \$3.50 per spot (of 55 kilobytes) per annum to RBC, as the card issuer, for the space it provided on the SIM card. Known as rack rent, the tariff was set by Enstream, the Canadian telecom consortium. Assuming 10 per cent of RBC's card holders were to migrate to the digital wallet, the rack rent would be, at a minimum, \$2,275,000 per annum for the SIM card-based mobile wallet. For the RBC Secure Cloud, the cost would also be \$2,275,000 (since the rent still had to be paid to the telecom operator) but it would be a one-time, rather than recurring, payment. There was a major saving with RBC Secure Cloud.

Finally, there was the matter of customer experience. It would take up to 60 minutes to load a single card (known as provisioning) on to the SIM card. The rate of failure in loading the cards was high. Since the provisioning had to be done by the user, the time lag affected the user experience. Provisioning was a particular issue in lifecycle situations (such as theft, fraud, expiry, and shift from one card to another with the same bank) requiring deletion of an existing card. Because of this, very few customers were likely to load their mobile wallet with more than one card. And, if they loaded only one card, their choice at the checkout would be limited, potentially changing a merchant's payment mix and affecting the merchant's business. With RBC Secure Cloud, provisioning could be done in less than two minutes with a 99 per cent success rate, and it only had to be done once.

Mantia and Bornstein were facing dilemmas at two other levels: the ongoing consolidation among Canadian telecom carriers and the ongoing fragmentation among mobile device manufacturers.

The SIM card used the medium of a telecom operator's wireless network. The cloud would reduce the dependence on a wireless partner, limiting its involvement to an applet that was required to direct traffic. But it would also require the telecom operator to break rank with its own peers. The telecom operator also had to have a strong and growing subscriber base. Finding such a partner from among existing players in Canadian telecom would be difficult (see Exhibit 3).

The range of mobile phone devices used by Canadians was wide but limited, principally, to four operating systems: Android (developed by Google), BlackBerry (RIM), iOS (Apple), and Microsoft (see Exhibit 4). The payment system was different for each platform and each phone. The strategy was not as simple as choosing the largest-selling device because the technology was changing rapidly. Interoperability was a critical factor in the choice of a device. Mantia said:

Every one of our peers in the telecom and payments industries wants us to sign the deal for the SIM card-based model and move on. While we are on the verge of going against the tide, there are two questions for which we have to find definitive answers. Would the network providers certify RBC Secure Cloud and allow the passage of payment credentials through the RBC applet? They are bound by rules, systems and protocols and are not comfortable with disruption. Would

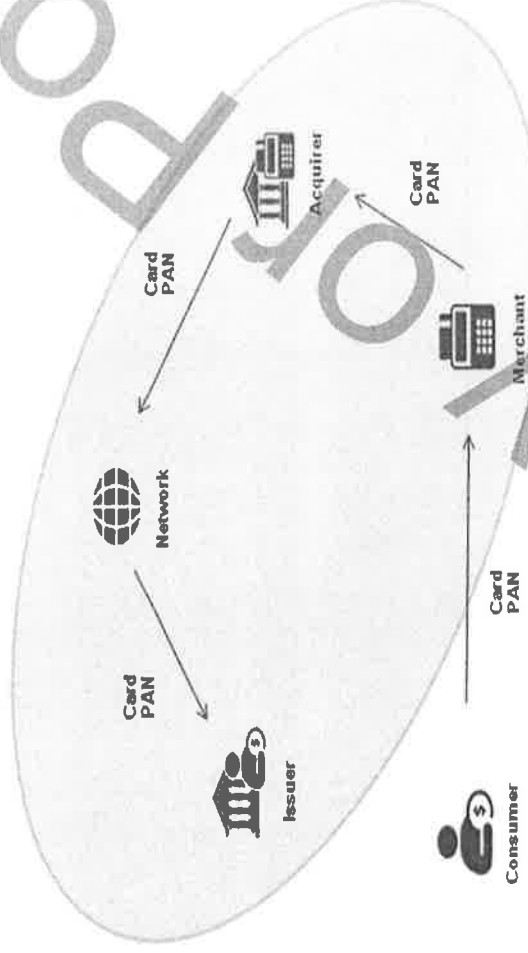
the telecom carriers agree to place an RBC applet in the SIM and also ensure that the right SIM is attached to the right phone? They value alliances and would not want to break rank.

There was also the option of not pursuing the mobile payments at all. Two factors were compelling. First, credit cards were not expected to disappear soon. Only 24 per cent of payments were predicted to be made on mobile platforms by 2020. By then, 80 per cent of the merchants would be using NFC, and 60 per cent of consumers would own a smartphone and would be using it to pay for half their purchases. Cards would continue to remain in use until mobile payments accounted for over 95 per cent of payments. That would give RBC a big time window. Second, only eight million people in Canada owned smartphones in September 2011, representing 40 per cent of the mobile market in Canada. The market was growing at about 10 per cent per annum.

The risk in not pursuing mobile payments was that disruptive solutions could disintermediate RBC from moving money altogether. If RBC misses the opportunity to keep up with services demanded from customers with respect to mobile payments, there was an inevitable likelihood that their core service of storing and lending money could be replaced by disruptive solutions as well.

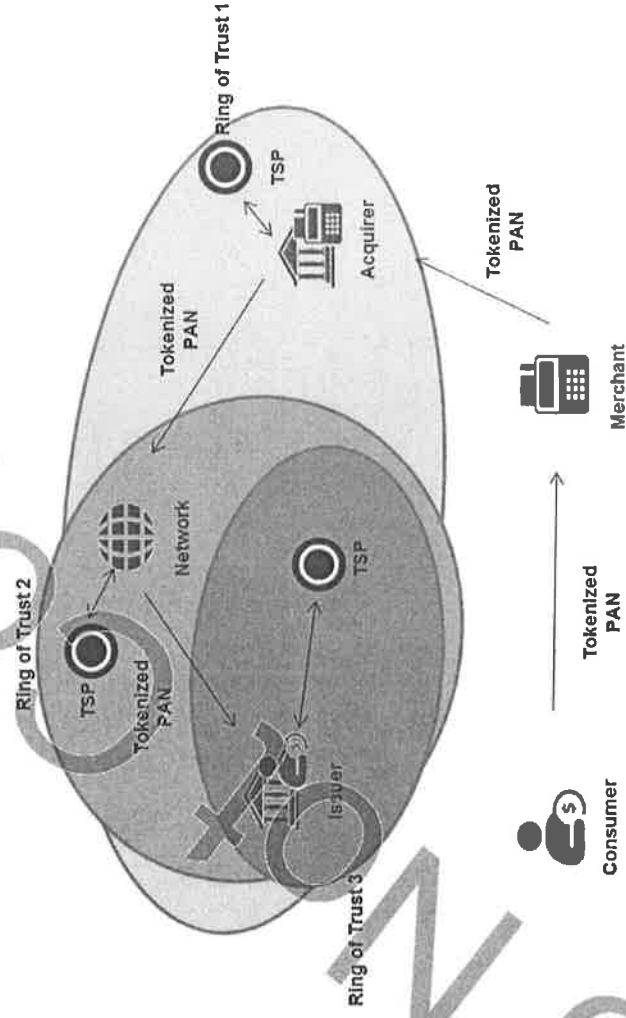
The Ivey Business School gratefully acknowledges the generous support of Pierre Lapointe, MBA '83, in the development of this case.

EXHIBIT 1: CONTACTLESS TRANSACTION



Source: Company files.

EXHIBIT 2: SUBSEQUENT DEVELOPMENTS



Ring of Trust 1: For Acquirer P2P Encryption
 Ring of Trust 2: For EMVCO Tokenization
 Ring of Trust 3: For RBC Secure Cloud

Source: Company files.

EXHIBIT 3: CANADIAN TELECOM OPERATORS

	Q3 2012	Number of Subscribers		
		2011	2010	2009
Bell Wireless	7,576,027	7,427,482	7,242,048	6,833,174
MTS mobility	494,564	496,432	483,754	458,478
Rogers Wireless	9,432,000	9,335,000	8,977,000	8,494,000
SaskTel Mobility	594,405	594,405	569,904	541,105
TELUS Mobility	7,558,000	7,340,000	6,971,000	6,524,000
Wind Mobile	510,484	403,000	232,641	-
Videotron	378,300	287,500	92,600	-
Total Subscribers	26,543,780	25,883,819	24,568,947	22,850,757

Source: Case authors.

EXHIBIT 4: CANADIAN MOBILE DEVICES MARKET

Top Mobile Original Equipment Manufacturers (September 2011)		Top Smartphone Platforms (September 2011)	
Device Manufacturer	Share of mobile subscribers (%)	Operating System manufacturer	Share of smartphone subscribers (%)
Samsung	25.2	RIM	35.8
LG	20.0	Apple	30.1
RIM	14.3	Google	25.0
Apple	12.0	Symbian	4.2
Nokia	10.1	Microsoft	3.2

Source: Case authors.