Have Money, Will Travel:
A Brief Survey of the Mobile Payments Landscape

Carlisle Adams[1]

June 2013

Disclaimer: The opinions expressed in this report are those of the author and do not necessarily reflect those of the Office of the Privacy Commissioner of Canada.

[1] Carlisle Adams is a Professor in the School of Electrical Engineering and Computer Science at University of Ottawa. This report, in its entirety, was completed while he was on sabbatical leave at the Office of the Privacy Commissioner of Canada (OPC) from January – June, 2013. He very gratefully acknowledges the discussions, suggestions, and valuable feedback from a number of OPC staff members, which greatly improved the quality of this report. However, all recommendations and opinions (and any remaining errors!) contained in the report are those of the author.

Abstract

The world of mobile payments is approaching very rapidly and, in some specific environments and use cases, is already here. This report's purpose is to do a focused examination of mobile payments technology through the lens of security and privacy. The goal is to think about potential security or privacy risks and to consider ways in which these risks can be mitigated, if possible.

This report is divided into three pieces: Context; Analysis; and Recommendations. The first piece looks at the motivations for mobile payments, describes some of the important payment models that have been proposed, introduces the major actors in the mobile payments ecosystem, and traces – at a high level – the flow of money in some of those models.

The second piece looks at the security and privacy risks of some specific payment models. In particular, this part of the report examines the mobile Point-of-Sale (mPOS) model of mobile payments that uses near-field communications (NFC), and also briefly considers the current mobile Commerce (mCommerce) model (as a transition phase toward true mobile payments) and some subcategories of the mobile peer-to-peer (mP2P) and mobile acceptance (mAccept) models.

The third piece looks at how the security and privacy risks of various payment models discussed in Part 2 can be minimized. It includes some recommendations from other sources that are applicable to mobile devices and mobile payments, and proposes some recommendations that arise from the analysis in Part 2 of specific payment models. It also gives recommendations that are relevant generally to all electronic payment models. This latter group of recommendations is categorized according to specific audiences: device and OS manufacturers, mobile network operators, wallet/app developers, standards bodies, merchants, and end users.

Executive Summary

This report examines the mobile payments landscape from the perspective of security and privacy. The first part of the report is intended to set the stage for the two parts that follow; its purpose is to help paint the “big picture”. In particular, it looks briefly at the history of mobile payments and some of the motivations for moving to this technology. It also categorizes mobile payments into four different types: mobile commerce (mCommerce); mobile Point-of-Sale (mPOS); mobile peer-to-peer (mP2P); and mobile payment acceptance (mAccept). Ten different categories of actors in the mobile payments ecosystem are introduced: banks / financial institutions; payment brands; wallet providers; end users; mobile device manufacturers; POS terminal manufacturers; Trusted Service Managers; Mobile Network Operators; Merchants; and Payment Network Operators. Finally, in order to make some of the concepts a bit more concrete, the flow of money is traced in some specific payment models.

Part 2 of the report provides a technical analysis of some mobile payment models. The specific models and technologies examined include online banking / shopping using a mobile browser, mobile carrier billing, near-field communications (NFC), M-Pesa (money transfer using text messaging), MintChip, and Square. This part of the report also provides an analysis of risks and concerns in electronic payments generally (that is, concerns that are applicable to all / many mobile payment models simultaneously). Concerns with respect to security and privacy are presented both in terms of specific technologies and in terms of general electronic transactions. For example, with NFC technology, discussion is presented regarding the possibility of corrupt or malicious readers (skimming attacks), malicious parties on the NFC channel (eavesdropping, relay attacks), and compromised mobile devices (hardware, software, and configuration attacks). Some of the concerns that are common to all / many payment models and technologies may be grouped according to Fair Information Principles:

- Safeguards
  - Lack of security implementation (the possibility that not all companies implement available security mechanisms)
  - Malicious employees at a payment app company (the need for audit controls, logs, and other technological and procedural mechanisms to control employee access to customer personally-identifiable information)
  - Recoverable data after loss or theft (the existence of attacks that can bypass encryption, and the ineffectiveness of some remote wipe mechanisms)
  - Natural or man-made disasters (the risk that there may be no non-electronic or alternative storage for backup in the case of an event that disables electronic memory)
- Consent
  - Small screens (the difficulty in presenting policies to, and obtaining meaningful consent from, users)
- Accuracy
  - Proprietary payment protocols (the risk that such protocols may not be designed or reviewed by security and privacy experts)
  - Buggy implementations (the risk that errors may occur in transactions or in stored data)
- Individual access
  - Natural or man-made disasters (the risk that users may be unable to access their data, accounts, money, and transaction history following a disastrous event)

The third part of the report provides recommendations that arise from the analysis in Part 2. These recommendations are presented in three sections:

- Relevant recommendations from other sources (including the Federal Trade Commission and the Payment Card Industry)
- Recommendations regarding specific payment technologies (e.g., NFC)
- Recommendations that apply to all / many electronic payment models simultaneously. These are divided into sets that are targeted to specific audiences:
    - Device / OS manufacturers
    - Mobile Network Operators
    - Wallet / payment app developers
    - Standards bodies
    - Merchants
    - End users

It is hoped that this report will be useful to the Office of the Privacy Commissioner of Canada, and to any others that may read it. The purpose of the report is to raise awareness and understanding of a variety of concerns in the mobile payments area so that, over time, they may be addressed by those involved in the creation and use of this technology. The ultimate goal is for all payment systems to be as secure and as privacy-friendly as possible; hopefully this report will make some contribution to concrete progress in that direction.

The recommendations presented are those of the author and are intended to contribute to the privacy and security research of the Office of the Privacy Commissioner of Canada and other interested parties; as such, they should be viewed as input for consideration as the OPC and others formulate their own policies and guidelines in the area of mobile payments.

Table of Contents

Abstract...2

Executive Summary...3

Part 1: Setting the Context...9

1. Introduction...9

2. History and Motivation...10

3. Types of Mobile Payments...11

4. The Mobile Payments Ecosystem for the mPOS Model...13

4.1 Ten Categories of Actors...13

4.2 Provisioning / Initialization of the Mobile Payment App and Data...18

5. Other Payment Models...19

5.1 mP2P (Transactions between Individuals)...19

5.1.1 PayPal...19

5.1.2 M-Pesa...20

5.1.3 MintChip...20

5.2 mAccept...22

6. Tracing the Flow of Money...22

7. Conclusion...24

Part 2: Analysis of Some Payment Models...25

1. Introduction...25

2. The Transition Phase: Two mCommerce Payment Models...25

2.1 Online Banking / Shopping using a Mobile Browser to a Website...26

2.2 Mobile Carrier Payments...26

3. The NFC-Enabled mPOS Payment Model...27

3.1 Corrupted POS Terminal...28

3.2 Corrupted Channel between Mobile Device and POS Terminal...30

3.3 Corrupted Mobile Device...32

3.3.1 NFC Architecture of the Mobile Device...32

3.3.2 Security and Privacy Risks on the Device...38

3.4 Summary...42

4. Some mP2P Payment Models...42

4.1 M-Pesa...42

4.2 MintChip 44
5. The mAccept Payment Model 45
6. General Technological Risks of Electronic Financial Transactions 47
6.1 Payment Tracking 48
6.2 Small Screens on Mobile Devices 48
6.3 Employees of the Payment Instrument Company 49
6.4 Natural or Man-made Disaster 49
6.5 Lack of Security Implementation 51
6.6 Buggy Implementations 52
6.7 Dispute Resolution Inconsistency 53
6.8 Proprietary Payment Protocols 54
6.9 Confiscation of Money, Blocked Transactions 54
6.10 Theft of Device 55
6.11 Burdensome Notification Process after Loss or Theft 55
6.12 Uncertainties Regarding “Remote Wipe” 56
6.13 Increasing Hacker Attention on Mobile Devices 57
7. Conclusion 57
Part 3: Recommendations 59
1. Introduction 59
2. Relevant Recommendations from Other Sources 59
2.1 FTC 59
2.2 LAP and M^{3}AAWG 60
2.3 OPC 60
2.4 PCI 61
3. Recommendations Arising from this Report (Specific Mobile Payment Models) 61
3.1 Online Banking / Shopping using a Mobile Browser 61
3.2 Mobile Carrier Billing 62
3.3 NFC-Enabled mPOS 62
3.4 mP2P 64
3.5 Electronic Cash Systems 65
3.6 mAccept 65
4. Recommendations Arising from this Report (All Electronic Payment Models) 66
4.1 For the Device / OS Manufacturer 66
4.1.1 Small Screens 66

4.1.2 Buggy Implementations........ 66
4.1.3 Loss or Theft of Device 66
4.1.4 Failure of Protection Mechanisms........ 67
4.1.5 Remote Wipe........ 67
4.1.6 Increasing Hacker Attention 67
4.2 For the MNO 67
4.2.1 Loss or Theft of Device 67
4.2.2 Remote Wipe........ 68
4.2.3 Increasing Hacker Attention........ 68
4.3 For the Wallet / App Developer........ 68
4.3.1 Payment Tracking 68
4.3.2 Small Screens........ 68
4.3.3 Malicious Employees 68
4.3.4 Natural or Man-made Disasters 69
4.3.5 Lack of Security Implementation........ 69
4.3.6 Proprietary Payment Protocols 69
4.3.7 Dispute Resolution 69
4.3.8 Confiscation of Money, Blocked Transactions 69
4.3.9 Loss or Theft of Device 70
4.3.10 Increasing Hacker Attention........ 70
4.4 For the Standards Bodies........ 70
4.4.1 Default Credentials........ 70
4.4.2 Disabled Mobile Service 70
4.5 For the Merchant........ 71
4.5.1 Natural or Man-made Disasters 71
4.5.2 Buggy Implementation of Human Processes 71
4.5.3 Dispute Resolution 71
4.5.4 Increasing Hacker Attention........ 71
4.6 For the End User 71
4.6.1 Small Screens........ 72
4.6.2 Buggy Implementations of Human Processes........ 72
4.6.3 Dispute Resolution 72
4.6.4 Confiscation of Money, Blocked Transactions 72
4.6.5 Loss or Theft of Device 72

4.6.6 Remote Wipe ... 73

4.6.7 Increasing Hacker Attention ... 73

5. Conclusion ... 73

References ... 74

Appendix: Remote Wiping on Mobile Devices ... 80

List of Acronyms ... 81

Glossary ... 83

Have Money, Will Travel:
A Brief Survey of the Mobile Payments Landscape

Part 1 – Setting the Context

Abstract

This first of three parts examines the context for mobile payments, including the various models, actors involved, and money flow in some payment transactions. The overall report focuses on mobile point-of-sale (POS) payments using devices enabled with near-field communications (NFC), although other payment models and technologies are briefly discussed as well.

1. Introduction

The world of mobile payments is approaching very rapidly and, in some specific environments and use cases, is already here. This report's purpose is to do a focused examination of mobile payments technology through the lens of security and privacy. Thus, there is no explicit goal to dissect legal, policy, usability, governance, business, or even technological feasibility issues, although some of these will inevitably make an appearance in the overall discussion. Rather, the goal is to think about potential security or privacy risks and to consider ways in which these risks can be mitigated, if possible.

This report is divided into three pieces: Context; Analysis; and Recommendations. This first piece looks at the motivations for mobile payments, describes some of the important payment models that have been proposed, introduces the major actors in the mobile payments ecosystem, and traces – at a high level – the flow of money in some of those models. It explores how a transaction starts and ends, and what happens in between, illustrating money flows via use cases with concrete examples.

It is important to begin by noting that "mobile payments" is a large and complex topic; therefore, some limitation of scope is essential. For the purposes of this report, a mobile payment is a monetary transaction involving a mobile device (typically a smart phone) that has an individual user as the initiator or the termination point (or both) of the money flow. As a result, business-to-business (B2B), business-to-government (B2G), and government-to-government (G2G, such as federal-to-provincial transfer payments) transactions are outside this report's scope. Furthermore, the mobile device must be an essential ingredient in initiating, terminating, or facilitating the payment, and so simply using a browser on a mobile phone to do online banking (paying bills or transferring money from one account to another), or online shopping, is not considered to be a mobile payment (since these transactions can identically be performed using a browser on a PC). Such transactions are therefore not the focus of this report, although they do form an important transition phase toward mobile payments and will be considered briefly in this light.

2. History and Motivation

According to the Task Force for the Payments System Review[2], Canadians currently produce/consume over one billion cheques annually. Large corporations, small and medium enterprises (SMEs), and governments account for approximately 60% of this total, while individuals account for the remaining 40%. Estimated costs per cheque (including invoicing, accounts receivable, accounts payable, cheque processing, postage, handling, and branch/teller costs) range from $1 to $30 depending on the industry segment[3].

Ultimately, the cost associated with paper cheques is a primary motivator for digital payment transactions. Potential annual savings by 2020 resulting from replacing a portion of this paper cheque volume with digital payments are estimated between $3B to $7B, or roughly 0.1% to 0.3% of Canada's GDP[4]. Along with this is the promise of greater convenience and tremendous efficiency increases given that transactions could occur immediately or nearly instantaneously, compared with the several days that it might take a paper cheque to reach its destination via traditional mail.

Another claimed motivator is the perception that Canada lags other countries in moving to digital payments. By some measures (e.g., number of B2B electronic transactions), Canada is seen as trailing (in a few cases, seriously) South Korea, the United States, China, Denmark, Finland, Norway, Sweden, the United Kingdom, Australia, Germany, Spain, Italy, Brazil, and Japan[5]. This is viewed by various Canadian entities as an embarrassment that needs to be rectified as soon as possible. By other measures, however (e.g., percentage of electronic consumer point-of-sale (POS) transactions), Canada is among global leaders[6]. Clearly, mobile payments are a subset of digital payments and, as noted above, this report is concerned only with mobile payments that directly involve the end user (consumer). Thus, Canada's perceived low place in the "world rankings" cannot be seen in this report as a strong motivating reason for the move to mobile payments (certainly not as strong as the convenience and efficiency arguments). In fact, a recent report by MasterCard[7] shows that Canada ranks second in the world in the Mobile Payments Readiness Index (MPRI), a scorecard that looks at a variety of factors including consumer readiness, environment, financial services, infrastructure, mobile commerce clusters, and regulation[8].

[2] Task Force for the Payments System Review, "Going Digital: Transitioning to Digital Payments", Report issued to the Minister of Finance, 2011. See http://paymentsystemreview.ca/wp-content/themes/psr-esp-hub/documents/r03_eng.pdf (last accessed February 13, 2013).

[3] Ibid, p. 60.

[4] Ibid, p. 17.

[5] Ibid, p. 18.

[6] Ibid, p. 18.

[7] MasterCard Mobile Payments Readiness Index (MPRI). See http://mobilereadiness.mastercard.com/the-index/ (last accessed March 13, 2013).

[8] Fuentes, R., "Canadian Mobile Payments Adoption Ranks Second in the World", TechVibes, May 10, 2013. See http://www.techvibes.com/blog/canadian-mobile-payments-adoption-ranks-second-in-the-world-2012-05-10 (last accessed March 13, 2013).

Finally, it is also worth noting that the value of mobile payments today is estimated at $13B in the U.S. alone (approximately $10B was estimated in Canada for 2011[9]). The increasing availability of tablets and smart phones across all segments of society is expected by many to increase this value, perhaps to as high as $90B by 2017[10]. This clearly holds promise for great profits for all participants in the mobile payment industry.

3. Types of Mobile Payments

According to a 2010 article by CNET[11], there are at least four distinguishable types of mobile payments: mobile peer-to-peer (mP2P); mobile Point-of-Sale (mPOS); mobile commerce (mCommerce); and mobile payment acceptance (mAccept). Several of these use (or can use) Near-Field Communications (NFC) as an underlying technology; consequently, NFC-enabled payments will form a focus of this report. NFC is a set of standards for smart phones and similar devices to establish wireless communication with each other by touching them together or bringing them into close proximity (a few centimeters or less)[12]. A description of each payment type follows below.

- **mP2P**: This covers transactions between individuals, such as paying the babysitter or loaning/repaying $10 to a friend. Such transactions might use PayPal, text messaging, NFC, or other technologies on each person's mobile device. In this payment type, neither participant is a registered merchant.
- **mPOS**: This encompasses more formal transactions between a person and a registered merchant, often at the checkout counter of a bricks-and-mortar store. Individuals use their mobile devices to interact with the POS terminal to purchase goods and services. Such transactions may use an NFC-enabled mobile device to communicate with the POS terminal (e.g., the recently-launched Rogers-CIBC-Blackberry initiative[13]) or may use a technology other than NFC (e.g., the Starbucks-MasterCard bar code scanning initiative[14]). Alternatively, a mobile device may interact with a non-traditional POS device (such as a tablet) to complete mPOS transactions without NFC. An interesting example is Square Wallet, which allows users to pay a merchant simply by saying their own name, if the user and the merchant both have the Square Wallet app installed and open on their devices. When the user approaches the checkout

[9] Canadian Payments Association, "Examining Canadian Payment Methods and Trends", CPA Report, October 2012. See http://www.cdnpay.ca/imis15/pdf/pdfs_publications/examining_canadian_payment_report_2012.pdf (last accessed March 13, 2013).

[10] Carrington, D., "US Mobile Payments Forecast 2013 – 2017: Mobile Payments to Reach $90B by 2017", Forrester Research, Inc., January 16, 2013. See http://blogs.forrester.com/denee_carrington/13-01-16-us_mobile_payments_forecast_2013_2017_mobile_payments_to_reach_90b_by_2017 (last accessed February 27, 2013).

[11] Dolcourt, J., "Making Sense of Mobile Payment", CNET, August 13, 2010. See http://www.cnet.com/8301-17918_1-20013480-85.html (last accessed February 14, 2013).

[12] Wikipedia, the Free Encyclopedia, "Near field communication". See http://en.wikipedia.org/wiki/Near_field_communication (last accessed March 13, 2013).

[13] Canada Newswire, "CIBC and Rogers Unveil the Future of Mobile Payments in Canada", May 15, 2012. See http://www.newswire.ca/en/story/974935/cibc-and-rogers-unveil-the-future-of-mobile-payments-in-canada (last accessed February 22, 2013).

[14] Stark, J., "Mobile Payments: Starbucks App", June 20, 2011. See http://jonathanstark.com/blog/mobile-payments-starbucks-app (last accessed February 27, 2013). [See also http://www.starbucks.ca/coffeehouse/mobile-apps/mystarbucks]

counter, the apps communicate and the user's name and picture appear on the merchant device; by confirming his/her name (and resembling the displayed picture) the user has completed the payment transaction.

- **mAccept**: This is essentially a blend of mP2P and mPOS. Two individuals are involved in the transaction, but one is a merchant. The transaction may be informal in the sense that the merchant may not be a registered, approved agent (e.g., with MasterCard or Visa). The consumer meanwhile pays with a debit or credit card, made possible by the merchant using a mobile device along with a hardware plug-in attachment that allows it to read and process a payment card. Technologies facilitating such transactions include Square[15] and PAYware Mobile[16] (Square is discussed in Section 5.2 below). Note that the Payment Card Industry (PCI) Security Standards Council has issued guidelines for the mAccept payment model; see PCISSC[17], for example.

- **mCommerce**: This involves the use of an app or the browser on a mobile device to do online shopping. It includes familiar online shopping environments such as Amazon, eBay, and iTunes. In this category, a mobile device is used but is not essential for the transaction (i.e., the same transaction could be performed on a laptop or desktop computer), and so it is considered to be outside the main focus of this report. It is important to note, however, that the idea of buying things online using a phone instead of a PC plays a role in preparing people for the concept of the phone itself as a payment device. This report, then, will look briefly at this transition phase.

In essence, excluding the mCommerce category, the remaining three mobile payment models can be viewed in the following way. Begin with a traditional physical-store purchase scenario (the customer uses a credit/debit card at a POS terminal), and replace the payer end, the payee end, or both ends with a mobile device:

- under mPOS, the payer's device replaces a credit/debit card (through the use of a payment app, for example);
- in mAccept the payee's device replaces a POS terminal (through the use of Square, for example); and
- mPSP comprises mobile devices performing both the payer and payee functions.

These scenarios do not simply bring mobile devices into the payment transaction; they can expand the transaction itself to additional actors and features. For example, replacing a traditional POS terminal with a mobile device has allowed arbitrary individuals to become merchants accepting credit/debit card payments (think of buying lemonade from the roadside stand run by a neighborhood child, or an item from a garage sale or farmer's market, using MasterCard). As another example, replacing a traditional credit/debit card with a mobile device has allowed the development of electronic wallets (such as Google Wallet) that hold multiple payment instruments, including various debit and credit cards,

[15] Dolcourt, J., "Start Your Own Business with Square for Android", CNET, May 19, 2010. See http://www.cnet.com/8301-19736_1-20005441-251.html (last accessed February 14, 2013).

[16] VeriFone, PAYware Mobile. See http://www.paywaremobile.com/ (last accessed February 14, 2013).

[17] Emerging Technologies, Payment Card Industry Security Standards Council, "PCI Mobile Payment Acceptance Security Guidelines, Version 1.0", February 2013. See https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf (last accessed March 1, 2013).

coupons, loyalty cards, and membership discount cards. Finally, replacing both credit/debit cards and POS terminals with mobile devices has not only allowed simple informal card- or bank-account-based payments between individuals (e.g., via PayPal), but has also provided the impetus for the movement toward digital cash (i.e., coins and bills in electronic form) that can be exchanged just like hard currency between various entities (see MintChip[18], for example).

As mentioned above, this report will examine the mPOS model of mobile payments (as built around the use of NFC-enabled mobile devices at the payer end), but will also look at some subcategories of the mP2P, mAccept, and mCommerce payment models.

4. The Mobile Payments Ecosystem for the mPOS model

This section gives an overview of the different actors involved in the NFC-enabled mPOS model of mobile payments. The information is based on the following sources: the 2009 white paper by the Smart Card Alliance entitled "Security of Proximity Mobile Payments"[19]; the 2012 Canadian NFC Mobile Payments Reference Model[20]; and the 2011 CNET article entitled "Who Will Profit from NFC, Mobile Payments?"[21]

4.1 Ten Categories of Actors

There are 10 categories of actors in the NFC mPOS model: four involved primarily in enabling the payment service; two involved primarily (or only) in the payment transaction itself; and the other four involved in both.
Each one is described below.

Involved in both enabling payments and in payment transactions

- **Bank / Financial Institution:** Much of their role is unchanged from traditional credit / debit card transactions, but the dawn of mobile payments provides the potential for higher revenues. For example, as with credit cards, banks can extend lines of credit to users for mobile payment use. As well, the ability to offer new payment services can boost transaction volumes, extend the bank's brand, and increase customer loyalty. Banks may also be able to persuade (through

[18] The Royal Canadian Mint, "MintChip Developer Resources". See http://developer.mintchipchallenge.com/devguide/index.php (last accessed February 14, 2013).

[19] Smart Card Alliance, "Security of Proximity Mobile Payments", A Smart Card Alliance Contactless and Mobile Payments Council White Paper, Publication CPMC-09001, May 2009. See http://collaboration/lib-bib/Library%20Document%20Collection/Security%20of%20Proximity%20Mobile%20Payments.pdf (last accessed February 14, 2013).

[20] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed February 14, 2013).

[21] Dolcourt, J., "Who Will Profit from NFC, Mobile Payments?", CNET, April 7, 2011. See http://www.cnet.com/8301-17918_1-20049894-85.html (last accessed February 14, 2013).

convenience and efficiency arguments) merchants who currently use cash and cheques to convert to mobile payment acceptance.

Interestingly, the promise of mobile payments has also enticed non-traditional players to consider acting as banks to increase their profits. One prominent Canadian example is Rogers Communications, Inc., who filed papers in 2011 with the federal government to start a bank ("Rogers Bank / Banque Rogers")[22].

- **Payment Brand:** The payment brand (e.g., Visa, MasterCard, American Express), which would typically also play the role of the payment application owner/provider, is responsible for the safety and security of payment credentials. The growing success and acceptance of contactless (i.e., chip-enabled tap-and-pay) credit / debit cards suggests that the transition to NFC-enabled mobile devices may be relatively smooth and painless. Payment brand organizations have the opportunity to appear innovative and attractive to consumers and, like the banks, may benefit financially from persuading merchants to convert to mobile payment acceptance.

  In addition, the possibility exists to expand the variety and number of payment brands available to the user. This includes issuers of coupons, loyalty cards, and membership discount cards. Since such items can be used to make a payment, or to reduce the price of an item at the time of purchase, the number of players in the payment brand space becomes virtually limitless: any merchant can easily send a coupon to its list of customers, any group can send a discount card to its list of members, and so on. The disadvantage is that this may significantly raise the level of complexity in securing the payment process (for example, how can the merchant ensure the validity of a coupon it didn't issue?).

- **Electronic Wallet Provider:** The possibility of multiple payment brands being available to the user has naturally given rise to the concept of an electronic wallet (as an app on the device or as a service on a remote server). If users have credit cards, debit cards, various membership cards, and coupons from different issuers, all on their mobile devices, an application is needed to manage and secure these instruments. The wallet provider supplies an app or service (i.e., the wallet), which is what manages these instruments and interfaces with the payer. Providers of such wallets include Google, Isis[23], Visa, MasterCard, financial institutions, and other third parties. Although wallets are usually free for consumers, wallet providers may charge merchants a flat fee or a percentage for every successful purchase made through the wallet[24].

- **End User:** The end user is the consumer of mobile payment and mobile connectivity services. While clearly a critical part of the payment transaction, the end user is also involved in enabling the payment service in the following ways: it requests specific payment brands (although some may come preinstalled on the device) and will initiate requests for the issuance of payment

[22] Evans, P., "Rogers Wants to Start a Bank", CBC News, September 6, 2011. See http://www.cbc.ca/news/business/story/2011/09/06/rogers-bank.html (last accessed February 22, 2013).

[23] Isis Mobile Wallet (Isis was founded by AT&T Mobility, T-Mobile USA, and Verizon Wireless to realize their shared vision of mobile commerce). See http://www.paywithisis.com/ (last accessed February 28, 2013).

[24] Wikipedia, the Free Encyclopedia, "Digital Wallet". See http://en.wikipedia.org/wiki/Digital_wallet (last accessed February 15, 2013). See also "A Global Overview of Digital Wallet Technologies", published by the ID Lab, University of Toronto, on May 28, 2011: http://propid.ischool.utoronto.ca/digiwallet_overview/ (last accessed February 15, 2013).

credentials (to allow payment applications to function). The user will typically also make choices regarding mobile network operator, mobile device, electronic wallet provider, financial institution, and merchant.

Involved primarily in enabling the payment service

- **Mobile Device Manufacturer:** The mobile device manufacturer (e.g., Apple, Blackberry, Nexus) can gain a competitive advantage by building devices that support mobile payments. In particular, this may mean building NFC-enabled mobile devices with a secure element (i.e., a smart card chip for secure storage) that stores the payment application and account information. The number of NFC-enabled smart phones is large and is growing at a rapid rate (see NFCWorld[25] for a current list).

  Innovative mobile applications (including payment) will allow device manufacturers to attract new customers and forge new business relationships, and so this represents a financially attractive opportunity for device manufacturers.

- **POS Terminal Manufacturer:** The point-of-sale terminal manufacturer makes the device that sits by the cash register, on the bus, at the metro stop, and so on. NFC-enabled POS terminals allow payments with a wave of the NFC-enabled mobile device, and the speed and convenience of this transaction is attracting merchants worldwide. VeriFone was an early player, but many others are now profiting from sales of NFC POS terminals.

- **Trusted Service Manager:** The Trusted Service Manager (TSM) (e.g., Vodafone, Oberthur, Gemalto, Giesecke & Devrient, Telefonica) plays a central and critical role in enabling (i.e., provisioning) mobile payments, although it plays no role at all in the actual payment transaction. In particular, as spelled out in some detail in Section 10 of the Canadian NFC Mobile Payments Reference Model[26], financial institutions, payment brands, public transit authorities, retailers, and others who wish to provide a payment, ticketing, or loyalty application to users with NFC-enabled devices, must do so through the TSM. Acting as a single point of contact and security gate controlling who can install payment instruments on the device, the TSM collects the NFC-enabled payment application and personal consumer data (such as name, credit card number, and expiry date, for example) and sends it over the air (via the Mobile Network Operator, MNO) to the secure element on the mobile device. The TSM thus provides secure download and lifecycle management services for NFC payment applications and consumer data.

  There are typically strict requirements imposed by payment brands for entities that wish to act as TSMs, including going through security audits before being authorized to process the delivery of payment card data. TSMs need to properly manage the cryptographic keys used to secure the communication between the financial institution and the user's mobile device.

[25] NFC World, "A Definitive List of NFC Phones, Last updated on 19 February 2013". See http://www.nfcworld.com/nfc-phones-list/ (last accessed February 19, 2013).

[26] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed February 14, 2013).

The TSM represents a new business opportunity in the mobile payments ecosystem[27]. Third parties (such as personalization service providers as used with traditional credit and debit payment cards) may choose to become approved as TSMs and offer their services to financial institutions and MNOs. Alternatively, financial institutions or MNOs may choose to become approved and function as TSMs themselves as a way of enlarging their service offerings and increasing revenues.

- **Mobile Network Operator:** The primary role of the MNO (e.g., Rogers) with respect to mobile payments is to provide the channel through which payment applications and consumer data from financial institutions, payment brands, etc., can be delivered to the secure element (SE) on the device. The MNO is therefore responsible for the integrity of the keys and certificates that will be used to protect communication across its network (using the TLS protocol, for example). When the secure element is owned by the MNO (in particular, when the SE is embedded on the UICC (Universal Integrated Circuit Card, commonly referred to as the Subscriber Identity Module (SIM) card) provided by the MNO to the user, the MNO must also maintain the integrity of the keys that allow access (reading, writing) to the secure element. Note that this does not give the MNO access to consumer data: the MNO uses one key to unlock the SE in order to write data to it, and uses a different key to protect the TLS communication of this data from the payment brand to the SE. The data itself is encrypted by the payment brand before transmission using another key known only to the payment brand (so that only the payment brand's own payment application can read/modify this data). As an additional role in the overall payment process, the MNO may also offer NFC-enabled devices to its customers.

  Typically, MNOs experience some churn rate in their subscriber base and consequently seek applications and services that will allow them to not only attract new customers, but also retain the customers they currently have. Mobile payments have the potential to bring economic benefits in this way, and may also realize increased revenues from new payment-related services, such as text message ads and coupons.

Involved primarily (or only) in the payment transaction itself

- **Merchant / Retailer:** NFC-enabled mobile payments are attractive to merchants because they use, without modification, the existing contactless card payment infrastructure. As a result, merchants who currently accept such payments have everything in place to immediately accept NFC mobile payments. Contactless card payments have been used worldwide for some time to increase both payment transaction speed (through faster transactions and fewer requirements to handle cash) and customer convenience. NFC-enabled mobile payments inherit these benefits, and additionally have the potential to allow merchants to establish stronger customer relationships and customer loyalty.

  NFC-enabled mobile payments also have revenue-generating possibilities that contactless cards lack. For example, merchants, like financial institutions, can offer their customers purchase-related and loyalty services, and can make these gift card and loyalty programs more effective

[27] NFC Times, "Topic: 'Trusted Service Manager'", 2013 (this is a collection of recently-signed TSM contracts). See http://nfctimes.com/tags/trusted-service-manager (last accessed February 28, 2013).

(since a customer's "payment cards" will always be available in his/her mobile device). Furthermore, paperless receipts (e-receipts, sent to the customer via NFC, e-mail, or SMS) will also always be available on the device, simplifying returns or exchanges. Finally, advanced mobile marketing and promotion programs can deliver context- and location-sensitive messages to customers, influencing their purchase behaviour both inside and outside the store, in hopes of leading to more sales and improved customer loyalty.

- **Payment Network Operator:** Authorization and settlement of mobile payment transactions occurs through the existing financial networks, and payment network operators (such as Interac) play the same role they currently play in traditional credit/debit card transactions. The move to mobile payments does nothing to change the function or operation of these back-end payment-processing networks.

Note that **an 11th category of actors can also be mentioned**, even though it is not involved in the actual payment process: **advertising networks.** These actors send ads to users' mobile devices enticing them to make purchases ("there is a Starbucks two blocks from you"; "Häagen Dazs ice cream is on sale this week"; "customers who have purchased this book often purchase that book"). Such location- and context-based advertising can be the impetus to a purchase, both triggering impulse buying and serving to remind users of a previous buying decision.
In the context of this report, this category is intended to encompass 3rd-party advertisers (who deliver advertising to a large set of people as the primary source of their revenue), as opposed to the merchants/retailers who send ads or recommendation information directly, and perhaps exclusively, to their own customers. The relevance of this category to the report is that some payment models may be "free" for use by the end user, and the wallet or payment credential provider may profit from selling information to 3rd-party advertisers, thus raising potential privacy concerns.

Some of the actors in the payment system ecosystem are shown in the following figure (taken from Figure 1 of the Smart Card Alliance white paper[28]):

[28] Smart Card Alliance, "Security of Proximity Mobile Payments", A Smart Card Alliance Contactless and Mobile Payments Council White Paper, Publication CPMC-09001, May 2009. See http://collaboration/lib-bib/Library%20Document%20Collection/Security%20of%20Proximity%20Mobile%20Payments.pdf (last accessed February 14, 2013).

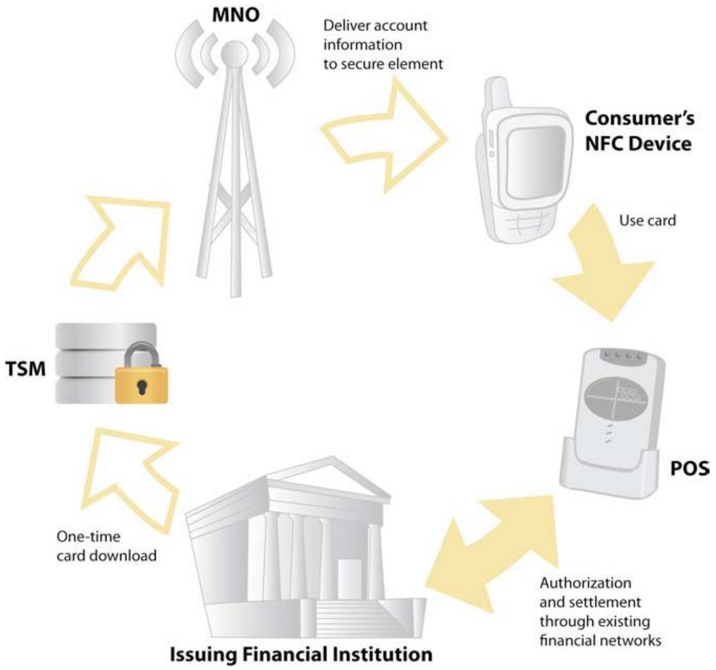
MNO
Deliver account information to secure element
Consumer's NFC Device
Use card
TSM
POS
One-time card download
Authorization and settlement through existing financial networks
Issuing Financial Institution

Figure 1. Some of the actors in the mPOS payment system ecosystem

Not surprisingly, the mPOS mobile payment ecosystem is similar to any other financial ecosystem: everyone wants a "piece of the pie"; everyone wants to make some money (or save some, in the case of the user) in the payment transaction. At one end are users, who have a maximum amount that they are willing to pay for an item (e.g., $3). At the other end are merchants, who have a minimum amount that they must receive in order to cover costs and make a profit (e.g., $2.50). The difference between these two price points is the money that will be split among all the actors in the ecosystem (for example, if the difference is $0.50, perhaps five cents will go to the user (the item is sold for $2.95), 5 cents will go to the merchant (the merchant retains $2.55), and 40 cents will go to the remaining actors).

4.2 Provisioning / Initialization of the Mobile Payment App and Data

In order to perform NFC-enabled mPOS payments, the user must have an NFC-enabled mobile device, a payment application and payment credentials. According to the Canadian Reference Model[29], p. 27, the payment application is similar to the application installed in a contactless card (e.g., Visa PayWave and MasterCard PayPass), and the payment credential is the personalized information within this application that is unique to a specific payment product (including the pass code). Typically, the user software would also include an electronic wallet to manage, and provide an interface for, multiple payment applications. Information associated with the payment credential that is viewable by a wallet or other application is the name of the payment network, the card artwork (i.e., logo), the type of payment product (e.g., debit or credit), and a small portion (e.g., the final 3-4 digits) of the credit/debit card account number: making these viewable allows the consumer to identify and select a payment credential at the time of the payment transaction.

[29] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed February 14, 2013).

Enabling of the payment application and payment credential is initiated by the financial institution, but only after the consumer is ready to begin the process on the mobile device (which might involve the consumer entering a bank-supplied activation code into the handset to initiate the enabling process). As described in the Canadian Reference Model, Section 10, the financial institution provides the app and data to the TSM, which installs the app and data on the secure element on the device (via the wallet, if present, which has access only to the viewable information while all other information is stored solely within the secure element). After this enabling process, the consumer is able to make mobile payment transactions.

5. Other Payment Models

In addition to the model presented above, two other mobile payment models will be briefly discussed in the following sections (and in Part 2 of this report): the mP2P and mAccept models. While these do not currently seem to be as important or prevalent as the NFC mPOS model in Canada, they are examined here because they either have strong proponents or are prevalent in other parts of the world.

5.1 mP2P (Transactions between Individuals)

Peer-to-peer (also known as person-to-person although some have made a distinction; see Charrat[30], for example) payment transactions using mobile devices can be realized using many different underlying technologies. Those that have achieved some prominence include PayPal (using Bump or NFC) and M-Pesa (using SMS text messages); another technology on the horizon is MintChip (using digital cash).

5.1.1 Paypal

PayPal has been operating as a processor for e-commerce payments and money transfers since March 2000[31]. By 2004, PayPal began exploring the use of mobile devices for money transfer (PayPal Mobile) through text messages on cell phones[32]. By 2010 they had extended their technology to the use of Bump (Bump was subsequently dropped from PayPal, although it is still used by ING and elsewhere), and by late 2011 an Android app was launched that used NFC to transfer money.

Although it looks very much like an NFC transaction, Bump does not use NFC technology. The Bump Pay app recognizes tapping motions and maps them. When a “bump” is recognized, a signal is sent to cloud servers that match it with another “bump” that occurred at the exact same place and time. It decides that those two “bumps” are a match and exchanges information between them[33]. To use the app, Alice connects to her PayPal account, types in the amount she wants to pay, bumps her phone against Bob’s

[30] Charrat, B., “Debunking NFC Peer-to-Peer Myths”, Inside Secure, February 2012. See http://insidesecure.com/eng/Media/White-papers (last accessed February 20, 2013).

[31] Wikipedia, the Free Encyclopedia, “PayPal”. See http://en.wikipedia.org/wiki/PayPal (last accessed February 20, 2013).

[32] PayPal, “Texting with PayPal – easy as lifting a finger”. See https://personal.paypal.com/ca/cgi-bin/?cmd=_render-content&content_ID=marketing_ca/mobile_text (last accessed February 20, 2013).

[33] Kessler, S., “Bank Lets Customers Pay Friends By Bumping iPhones”, April 29, 2011. See http://mashable.com/2011/04/29/ing-direct-customers-bump/ (last accessed February 20, 2013).

phone, and then confirms the payment. Bob must also have Bump Pay installed in order to receive the payment. If both PayPal accounts are associated with checking accounts, there is no fee for the transfer; otherwise, a few percent will be charged if only a credit card is associated[34].

For NFC, PayPal has an app that allows money transfers using a very simple interface. Alice and Bob each need to have an NFC-enabled Android phone and the PayPal app with the Request Money functionality installed. To request money, Alice enters an amount and taps her phone with Bob's phone. Once Bob receives the request, he enters his password to send money[35]. Interestingly, PayPal has recently turned away from NFC, claiming that it is "technology for technology's sake" and that it doesn't "address true customer pain points [irritants]"[36], although mobile payments via NFC-enabled devices (using underlying payment channels other than PayPal, such as "Osaifu-Keitai" (mobile wallet) by DoCoMo) have been widespread for many years in some countries such as Japan and China.

5.1.2 M-Pesa

M-Pesa (mobile money) was launched in Kenya in 2007 and is now used by well over half the Kenyan population to pay bills, wages, and taxis, to shop, and to send money directly to another person's mobile phone. In Kenya a large percentage of the population does not have access to banking facilities and M-Pesa allows money transfers to take place quickly and easily in this environment. There are approximately 50,000 M-Pesa agents around the country, typically located in small grocery stores and gas stations. Customers go to one of these agents and register with Safaricom, the mobile phone operator. When registered, they can put money onto their phone by giving cash to the agent. The agent holds onto the cash and the money is virtually transferred to the phone. The customer can then, for example, send money to another person using an SMS message; the recipient takes the message to the nearest agent and is given the cash by that agent[37].

M-Pesa (or a very similar service) is also used in other African countries, including Ivory Coast, Senegal, and Mali, as well as other countries such as Afghanistan[38]. Mobile payment using SMS is also popular in several European countries, many Latin American countries, the United Kingdom, India, and Australia.

5.1.3 MintChip

[Please note that the Royal Canadian Mint has not launched MintChip. This subsection has been developed by reviewing the information published on the Royal Canadian Mint's MintChip website[39].]

[34] Constine, J., "Bump Pay Lets You PayPal Someone With A Tap, But Only In-Person", TechCrunch Hot Topics, March 29, 2012. See http://techcrunch.com/2012/03/29/bump-pay/ (last accessed February 20, 2013).

[35] Samuel, S., "New in the Android Market: Updated PayPal Mobile App Featuring P2P NFC Capabilities", The PayPal Blog, November 8, 2011. See https://www.thepaypalblog.com/2011/11/new-in-the-android-market-updated-paypal-mobile-app-featuring-p2p-nfc-capabilities-2/ (last accessed February 20, 2013).

[36] Gabriel, C., "PayPal extends mobile wallet, but no NFC", Rethink Wireless, January 15, 2013. See http://www.rethink-wireless.com/2013/01/15/paypal-extends-mobile-wallet-nfc.htm (last accessed February 22, 2013).

[37] Mobile Transaction, "Growing Use of SMS Payments Around the World". See http://www.mobiletransaction.org/sms-payments/around-the-world (last accessed February 20, 2013).

[38] Ibid.

The Royal Canadian Mint, after considering the evolution of currency and payment technologies (particularly in the area of high-volume, low-value payments at the point of sale), has developed MintChip[40]. It sees MintChip as the digital equivalent of coins and bank notes and expects that it will find widespread use for micro-transactions (under $10) and nano-transactions (under $1).

The core of the system is the MintChip "chip", a secure integrated circuit smartcard which acts as a storage location for the digital cash itself. This chip can be deployed in different ways, leading to at least four different realizations of MintChip that can be available to users.

First, the chip can be implemented in a single-purpose MintChip USB device. This USB device can then be plugged into any PC or laptop to enable online or offline payment transactions. Second, the chip can be implemented in a single-purpose hardware security module (HSM). The HSM is designed for large online merchants and is meant for environments with high transaction rates. Third, and most relevant to this report, the chip can be implemented in a MicroSD card (i.e., a small, portable memory card commonly used with cameras and other devices, but also available on some smart phones) which can easily be inserted into a mobile device to make it "MintChip ready", and removed at any time when this functionality is no longer required. Finally, a third-party service provider may host a farm of MintChips in the cloud on behalf of its users. Users would need to be authenticated by the service provider before being given access to their MintChips. This architecture enables users to participate in MintChip transactions with a device that does not accommodate a MicroSD card or USB stick, such as an Apple iPhone.

The MintChip ecosystem is intended to emulate the existing coin distribution model: MintChip is created by the Royal Canadian Mint, distributed by a Trusted Broker (see below), and used by consumers and merchants. Consumers buy MintChip value from the Trusted Broker and then transact with merchants or other consumers who use the tool to purchase goods or services, or simply perform money transfers. The MintChip acceptors redeem value at the Trusted Broker, and the Broker will typically also interact with a financial institution to acquire and deposit hard currency, as required.

For the mP2P model, two individuals are involved, each with a MintChip chip on a MicroSD card in their phone (the USB and HSM form factors do not involve a mobile device, and although a mobile device can be used to access a Mintchip in the cloud, it is not essential; these three form factors are thus outside the scope of this report). The devices exchange "request" and "value" messages; this exchange can take place using SMS, e-mail, or NFC communication. According to the MintChip website, once the value message is created by the sender using the MintChip app with the sender's chip, the chip's balance is decreased by the corresponding value. The sender cannot stop or cancel the transaction after the value message has been created. On receiving the value message, the receiver's app verifies the validity of the message (by checking a digital signature and an included challenge value). If the message is valid, the receiver's balance is incremented by the amount specified in the value message.

It is not yet clear who will play the role of the Trusted Broker in the MintChip ecosystem. Possible candidates include banks and Canada Post, but perhaps others will campaign to take on this task as well.

[39] The Royal Canadian Mint, "MintChip Developer Resources". See http://developer.mintchipchallenge.com/devguide/index.php (last accessed February 14, 2013).

[40] Ibid.

Also unclear is how anyone will make money from this payment model. One can guess that the Royal Canadian Mint could conceivably make a profit by selling MintChip value to the Trusted Broker at a premium (e.g., $1.00 of value for a price of $1.02). Further, it seems likely that the Trusted Broker could make a profit by treating MintChip as a different currency and charging exchange rates ("today's rate: we sell $1.00 of MintChip value for $1.05; we buy $1.00 of MintChip value for $0.97"). However, what will be the eventual monetization of the transactions when the system is actually deployed, and who will be the full set of entities that make money, is still up in the air.

5.2 mAccept

The mAccept payment model replaces the POS terminal at the merchant end of a transaction with a mobile device (while the payer uses a traditional credit card). A small piece of hardware attaches to the mobile device, allowing it to physically accept swipes of a credit card so that independent merchants can process credit card payments anytime and anywhere. One of a handful of technologies that enable this payment model is Square[41]. A white plastic square (more like a cube) plugs into the headphone jack of an Android or Apple phone. This square has a thin slit running through it, which is where the credit card is swiped. Along with the plastic square is the Square app that runs on the phone to process payments. The merchant may swipe the card, take a picture of the merchandise as a reminder (to both parties) of what was sold, and attach the merchant's own photo/logo/etc. to remind the payer of who the payee was. The Square app hides the card details so that the payee never sees the credit card number or security code, and e-mails or texts a digital receipt to the payer.

According to the Square website[42], Square charges the merchant 2.75 percent of the total for every card swipe, and 3.5 percent plus 15 cents for transactions made with a manually-entered card number. This is similar to PayPal's pricing strategy (1.9 – 2.9 percent for each sale, plus 30 cents), and is smaller than the transaction fees charged by some banks. This pricing strategy has been highly successful for PayPal; additionally, with Square there is effectively no restriction on when and where the payment transaction can take place.

6. Tracing the Flow of Money

It may be helpful to consider the flow of money in mobile payment transactions. For illustrative purposes, three concrete examples will be described (the first two using the mPOS model and the third using an mP2P model).

Scenario 1: purchase at a merchant POS terminal

In this scenario, Alice wishes to purchase a coffee and muffin at a local coffee house with her NFC-enabled mobile device. After placing her order, she opens the wallet app on her phone, checks that the default payment instrument (which she has previously chosen to be a MasterCard debit card) is selected, informs the teller that she will be using a MasterCard debit card, and once prompted by the teller, puts her phone near the contactless POS terminal. Because this is deemed to be a "convenience

[41] Dolcourt, J., "Start Your Own Business with Square for Android", CNET, May 19, 2010. See http://www.cnet.com/8301-19736_1-20005441-251.html (last accessed February 14, 2013).

[42] Square pricing, as shown at https://squareup.com/ca/pricing (last accessed February 27, 2013).

transaction" (i.e., one that is performed frequently and quickly), Alice does not need to do any more than "tap-and-go"; in particular, she does not need to engage in a card verification method (such as entering a pass code). Once the transaction has been approved at the POS terminal, an electronic receipt is created and sent to Alice via e-mail, SMS, or NFC. This last option would require a second tap of the mobile phone to the terminal, but has the advantage of the receipt going directly to the mobile wallet and being stored there, which would be useful for a purchased item that might later be returned).

The convenience transaction rule (i.e., no PIN or pass code) and the electronic receipt issuance are unique to the NFC-enabled technology (see the Canadian Reference Model[43], p. 35), but otherwise the transaction is the same as payment with a contactless debit card. Specifically, the underlying flow of money is identical to what happens today.

Scenario 2: loyalty card rewards (after 10 muffin purchases you get a free muffin)

This scenario builds on scenario 1, adding a loyalty card from the coffee house into the picture. In this scenario, the coffee house loyalty card is stored in Alice's mobile wallet and is transmitted to the POS terminal along with her debit card details when she taps her phone. The merchant system checks/updates Alice's loyalty points balance and determines whether a price reduction is warranted (i.e., whether the price of the muffin should be subtracted from the total). The payment transaction proceeds as above, and the updated loyalty card is transmitted to Alice's wallet along with her electronic receipt with the second tap of her phone.

Note that the coupon/loyalty or membership card portion of mobile payments is still relatively new and therefore still somewhat in flux. Thus, there are no standards determining how such transactions will precisely operate. In particular, it is not yet clear whether Alice will need to search manually through her electronic wallet to find the relevant coffee house loyalty card, or whether the card will be found automatically once the merchant information (name, location) has been transmitted to the phone. It is also not clear whether the loyalty card will travel with the debit card details in a single NFC exchange, or whether a second tap will be required. Similarly, the updated loyalty card might travel with the electronic receipt at the conclusion of the transaction, or might require an additional tap. In the near term, it might be that different wallets and different merchants will adopt different practices until some standardized transaction flows emerge.

Scenario 3: money transfer between two friends ("Can I borrow $10?")

In this scenario Alice wishes to give Bob $10 so that he can purchase a birthday card for his brother. A number of technologies have been deployed (or proposed) for doing this, including Bump Pay (with PayPal or ING Direct, for example), SMS (with M-Pesa, for example), NFC (with PagSeguro[44] in Brazil, for example), and digital cash (MintChip, for example); some of these transaction flows have already been outlined above (see Section 5.1). At least in North America, however, none of these technologies has

[43] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed February 14, 2013).

[44] The Paypers: Insights in Payments, "Brazil: PagSeguro, Nokia to introduce NFC P2P payments", May 3, 2012. See http://www.thepaypers.com/news/mobile-payments/brazil-pagseguro-nokia-to-introduce-nfc-p2p-payments/747502-16 (last accessed February 22, 2013).

yet been very successful, and it is unclear which (if any) will dominate the mP2P payment model in the next few years.

7. Conclusion

This part of the report has looked at the context for mobile payments, including what various models exist, who the major actors in the ecosystem are, and how money flows from sender to receiver in some payment transactions. The focus is on mobile point-of-sale (mPOS) transactions that are enabled by near-field-communications (NFC) technology, although mention is made of other models and technologies as well.

Part 2 of the report will discuss the security and privacy implications of some of these mobile payment models.

Have Money, Will Travel:
A Brief Survey of the Mobile Payments Landscape
Part 2 – Analysis of Some Payment Models

Abstract

This second of three parts provides an analysis of some specific mobile payment models. The analysis focuses on mobile point-of-sale (POS) payments using devices enabled with near-field communications (NFC), although other payment models and technologies are briefly considered as well.

1. Introduction

This report on mobile payments is divided into three pieces: Context; Analysis; and Recommendations. This second piece, *Part 2 – Analysis of Some Payment Models*, looks at the security and privacy risks of some specific payment models. In particular, this part of the report examines the NFC-enabled mPOS model of mobile payments, but also briefly considers the current mCommerce model (as a transition phase toward true mobile payments) and some subcategories of the mP2P and mAccept models.

The remainder of Part 2 is structured as follows. Section 2 looks at two commonly-used mCommerce payment models (online shopping/banking and mobile carrier billing). Section 3 begins the analysis of true mobile payment models, looking in some detail at the NFC-enabled mPOS model and focusing on the three areas where security and privacy risks lie. Section 4 looks briefly at the mP2P model of money transfers, specifically mentioning M-Pesa and MintChip. Section 5 looks briefly at the mAccept model, using Square`s payment model as a case study example. Section 6 talks in general terms about the risks of financial transactions that take place exclusively in electronic form (this discussion is applicable to all mobile payment models). Finally, Section 7 provides some concluding comments.

2. The Transition Phase: Two mCommerce Payment Models

As mentioned in Part 1 of this report (see Section 3 of Part 1), online banking / shopping is out of scope for this paper because in these transactions, the mobile device is the conduit for conducting the transaction, but is not essential for the transaction. However, it represents an important transition phase in society, getting people comfortable with the idea of making a monetary transaction (i.e., paying a bill or purchasing an item) using a phone instead of a computer.

A second model also fits into the mCommerce category and is worth a brief discussion due to its growing use: mobile carrier payments. In the mobile carrier payment model, the mobile device is more essential (i.e., the user must have a mobile device in order to have a contract with the mobile carrier), but the payment transaction is non-traditional (the user “purchases” an item by requesting that the price of the item be added to the user’s next phone bill). A pre-arranged business agreement between the mobile carrier and the merchant is required for such transactions to take place.

2.1 Online Banking / Shopping using a Mobile Browser to a Website

Online banking and online shopping via a mobile browser on a smart phone or tablet is essentially identical to online banking or shopping using a browser on a laptop or desktop computer (minor modifications might include adaptation to a smaller screen or special web pages designed specifically for mobile devices). The only significant difference is that the transaction may take place anywhere and at any time (simply because the user is more likely to have the device on his/her person than a desktop or even a laptop computer). As mentioned above, however, this scenario gets people used to the idea of paying a bill or making a purchase "using a mobile device" rather than a computer (even if the mechanics of the process, such as entering a credit card number and expiration date on a website form, are the same).

Given that the transaction process is identical, it is not surprising that the security and privacy considerations would be similar: browser vulnerabilities can lead to loss or misuse of data, as well as the possibility of malicious software being downloaded to the device. One mitigating factor (compared with laptops and desktops) is that on some mobile device platforms (Android, for example) apps are partitioned so that one app is unable to see (or corrupt) the processing or data of other apps; this can potentially limit the damage that a browser vulnerability can do. On the other hand, if the downloaded malicious software allows the attacker to escalate privileges (for example, by exploiting the fact that the phone has previously been rooted/jailbroken by the legitimate user in order to remove some built-in restrictions on software download and configurability), then anything on the phone may be vulnerable to theft, modification, or destruction.

2.2 Mobile Carrier Payments

In mobile carrier payment systems, the price of a purchased item is put on the next phone bill. The MNO is thus acting like a credit agency (i.e., the MNO pays the merchant at the time of purchase and retrieves the money from the customer at the next billing cycle) and so no traditional payment instrument (such as a credit / debit card) is used by the customer for the purchase. A growing number of third parties have entered into agreements with carriers to allow this payment method (for example, Google allows Android app purchases to be charged to a customer's mobile phone bill for supported networks[45], and BlackBerry World has recently struck a similar deal[46] with Wind Mobile).

A potential privacy concern with mobile carrier payments is associated with big data and the use of analytics: the MNO will know much more about its customers than without carrier billing (e.g., detailed purchase history and merchants involved) and thus has the potential to purposefully or accidentally misuse that data in some way (such as sharing this information with others for marketing purposes).

[45] Google Play, "Purchase with carrier billing". See http://support.google.com/googleplay/bin/answer.py?hl=en&answer=167794&topic%20=1046%20718&ctx=topic (last accessed April 8, 2013).

[46] Hardy, I., "WIND Mobile goes live with BlackBerry World carrier billing", MobileSyrup, April 1, 2013. See http://mobilesyrup.com/2013/04/01/wind-mobile-goes-live-with-blackberry-world-carrier-billing/ (last accessed April 30, 2013).

Consumer issues extend beyond privacy, however. Another concern with mobile carrier payments is that (at least in the U.S.[47] and Canada[48]) there are currently no federal statutory protections regarding consumer disputes about fraudulent or unauthorized charges on mobile carrier bills. Rather, consumers must rely on the terms of their mobile carrier agreements or on the good will of the companies involved when disputes arise (see the FTC Workshop Report[49], p. 8. This has led to an escalation of the practice of "cramming" (first identified years ago with the landline billing platform[50]) whereby third parties place fraudulent charges onto consumers' mobile carrier bills in hopes that the consumers will not notice the charges and will simply pay their monthly bill. FTC Workshop Report recommendations in this area include giving consumers the ability to block all third-party charges on their mobile accounts, and establishing a clear and consistent process for consumers to dispute suspicious charges and obtain reimbursement (p. 8). Other suggestions include getting mobile carriers to "standardize and prominently highlight billing descriptions of third-party charges, in a format that makes clear why the consumer is being billed for a third-party charge, the provider or merchant that placed the charge, and the good or service being provided" (p. 9).

Cramming is a significant concern because many consumers are unaware that third parties can place charges on their mobile bills, and that the third parties can do so even if the consumer has provided no credit card or other payment information (p. 10). Furthermore, such charges may appear on the bill as "service fee", "service charge", "other fees", "voice mail", "mail server", "calling plan", or "membership" (these may be cramming if they were unauthorized or if the cost was misrepresented) and can thus go undetected indefinitely[51].

3. The NFC-Enabled mPOS Payment Model

In the NFC-enabled mPOS payment model, the user has a mobile device equipped with a near-field communications chip and one or more installed payment instruments (such as debit or credit card applications, prepaid / loyalty / discount / membership cards, and coupons). The merchant has a contactless Point-of-Sale terminal which allows users to wave or tap their NFC devices to make payment transactions.

[47] U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), "Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments", FTC Staff Report, March 2013. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed April 5, 2013).

[48] Canadian Radio-television and Telecommunications Commission (CRTC), "You have rights", Guide for understanding rights with respect to local home phone services, section on "Disputing phone charges". See http://www.bell.ca/web/common/en/all_regions/pdfs/wireline/SCR_Final.pdf (last accessed May 10, 2013).

[49] U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), "Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments", FTC Staff Report, March 2013. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed April 5, 2013).

[50] U.S. Federal Communications Commission (FCC) Infographic on Cramming. See http://www.ftc.gov/os/2011/12/111227crammingcomment.pdf (last accessed April 8, 2013).

[51] Ibid.

Three Possible Attack Locations for NFC Payment Transactions

In an NFC mobile payment there are at least three possible locations for an attack to occur. Two of these are shared with current contactless credit / debit cards: the POS terminal (more generally, the reader) may be corrupted in some way; and the channel between the mobile device and a legitimate reader (i.e., the air space) may be breached in some way. Thirdly, what is different about mobile NFC payments (compared with contactless-card-based NFC payments) is that the device itself may be attacked in multiple ways.

The following subsections will consider the security and privacy implications of each of these locations in turn.

3.1 Corrupted POS Terminal

An NFC-enabled mobile device can act in three different ways. First, it can be an active device (a reader) that sends a radio-frequency (RF) signal to supply electrical power to a passive device (i.e., one without a power source such as a battery) in order to enable that device to respond to messages. This is the mode employed when a phone is held near to an NFC tag on a poster or bulletin board in order to retrieve more information than is given in the text of the poster (such as additional description, pricing information, or a link to a web site).

Second, the mobile device can be a passive device, which receives a signal from an external active reader. This is called "card emulation mode" because the mobile device looks exactly like an ordinary contactless card to the reader (e.g., a POS terminal); this is the mode used for mobile payments.

Finally, both the mobile device and the external device can be active, sending signals to each other. This is the mode used, for example, when two phones are "tapped" to exchange business cards.

In card emulation mode, the mobile device is passive, waiting for a message from an external reader. Such a state can make the device vulnerable because the external reader may be corrupted, or even entirely fake (i.e., not a POS terminal at all, but rather some reader that an attacker has built for his/her own malicious purposes). Such "rogue" readers may send valid-looking messages to the mobile device, causing the device to think that a legitimate payment transaction is occurring and therefore transfer money from the user's account to the reader. For high-value payments ($50 and higher) an additional verification by the user may be required (even something as simple as pressing an "OK" button) and so it would be difficult for this attack to succeed, but for low-value amounts such as a payment of a few dollars, the verification step may be bypassed (particularly if a default payment credential has been enabled in the wallet).

Low-value attacks with a rogue reader (sometimes referred to as "skimming attacks" because the attacker stands near various people, say on a crowded bus or subway train, and "skims" a few dollars from each) are likely to be possible with NFC-enabled mobile devices because similar attacks (skimming card number and expiry date information) have been demonstrated multiple times for NFC-enabled (i.e., contactless) credit cards[52,53]. Skimming the credit card information from a mobile device (i.e., without

[52] Snopes.com, "Electronic Pickpocketing", October 4, 2012. See http://www.snopes.com/fraud/identity/pickpocket.asp (last accessed March 22, 2013). See also http://www.youtube.com/watch?v=EKks3vfiy6Q

completing a payment transaction) is also possible when the device is in card emulation mode and the NFC chip is turned on. (Note that card info skimming does not reveal the 3- or 4-digit number (the CVV) on the back of a credit card, which limits the number of places that the skimmed data can be used for a malicious purchase.) It is much more difficult for an attacker to corrupt the real POS terminal of an actual merchant (even if the attacker is also the merchant!) so that, for example, it displays one amount while charging a slightly higher amount, but such attacks are undoubtedly at least theoretically possible.

Metal-lined security sleeves or cases for credit / debit cards can protect against unintended exchanges with malicious readers, but similar sleeves for mobile devices are not likely to find use since they would interfere with normal phone operation. On the other hand, many NFC-enabled phones deliberately disable the NFC capability when the screen is off in order to give some protection against skimming attacks (a protection mechanism that is unavailable to contactless cards). Note, however, that this practice appears to conflict with the Canadian NFC Mobile Payment Reference Model statement that a default credential allows payments to be initiated even if the device is in standby mode (Reference Model[54], p. 26).

A topic somewhat related to the concept of a corrupt reader is that of a corrupt NFC tag. An NFC tag is a passive device that is powered and read by a mobile device running in active mode. As mentioned above, such tags may be used on posters or other public places so that phones can be tapped to obtain additional information (such as a trailer for a movie advertised on the poster). However, there has been recent interest in technology that allows users to write their own tags in order to automate specific functionality or repetitive tasks – the tag essentially contains a list of actions (a script) that will be executed one-by-one on the phone[55,56]. For example, when a typical user leaves work and gets in his/her car to go home, the user might change a number of phone settings, such as disabling Wi-Fi, enabling Bluetooth, setting the ringer type to silent, setting the screen brightness, and launching a particular application. An NFC tag can be created (requiring only a writable tag and an application such as “NFC Task Launcher”) to hold all these instructions; the user can then simply tap his/her phone against the tag and all these actions will be completed automatically[57].

Clearly, if malicious readers can exist then malicious tags can also exist: an attacker can create an NFC tag that holds a script of actions that a user might not otherwise choose, such as turning off some

[53] Pauli, D., “Android app steals contactless credit card data”, SC Magazine, June 21, 2012. See http://www.scmagazine.com.au/News/305881,android-app-steals-contactless-credit-card-data.aspx (last accessed March 22, 2013).

[54] Canadian Financial Institutions (“Industry Initiative Participants”), “Canadian NFC Mobile Payments Reference Model”, version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed February 14, 2013).

[55] Whitwam, R., “How To Have Fun with Near Field Communication on Android”, Tested, April 27, 2011. See http://www.tested.com/tech/android/2234-how-to-have-fun-with-near-field-communication-on-android/ (last accessed March 25, 2013).

[56] Kharif, O., “NFC Stickers Make Smartphones Smarter”, Bloomberg Businessweek: Technology, July 12, 2012. See http://www.businessweek.com/articles/2012-07-12/nfc-stickers-make-smartphones-smarter (last accessed March 25, 2013).

[57] Holly, R., “How to use NFC to automate your mobile routine”, geek.com, February 8, 2012. See http://www.geek.com/articles/mobile/how-to-use-nfc-to-automate-your-mobile-routine-2012028/ (last accessed March 25, 2013).

security protections and visiting a web page that exploits a browser bug to give the attacker access to data on the phone[58]. In the context of mobile payments, an attacker may be able to create a tag that launches the wallet and turns off user verification for high-value payments, for example. This could then be used in conjunction with a rogue reader to skim large dollar amounts from people on a crowded bus or subway.

3.2 Corrupted Channel between Mobile Device and POS Terminal

With Near-Field Communications, messages are being transmitted through the air between a mobile device and a POS terminal. Although the length of the air channel is very short (typically less than 10 cm, and perhaps as low as zero cm if the phone is physically tapped against the reader), some researchers have examined whether it is possible for someone to perform an attack on this channel. The types of attacks that have been investigated include eavesdropping, data corruption, data modification, data insertion, and man-in-the-middle (MITM). At study by Kremer[59] has presented the following conclusions (see also Sections 2.1.2 and 2.2.1 of Kerschberger[60]).

- Eavesdropping on the NFC channel is possible with commercially-available equipment and an attacker of low-to-moderate technical skill, but the quality of the eavesdropped signal will depend on a large number of parameters, including the antenna geometry of both the sender and the attacker, the quality of the attacker's receiver and signal decoder equipment, the location of the attack (walls, metal, ambient noise, and so on), and the signal power from the sender's NFC device. In some cases, successful eavesdropping from distances of up to 10 m from an active transmitting device (1 m from a passive device) has been demonstrated.
- Data corruption is relatively easy to perform (with commercially-available equipment and low-to-moderate technical skill) – this is effectively a denial-of-service attack in which the attacker transmits a jamming signal so that the real signal cannot be understood by the legitimate receiver. In a payment transaction, however, it is not clear what benefit an attacker could derive from this.
- Data modification may be possible, depending on the modulation scheme employed between the sender and the receiver (i.e., 100% amplitude shift keying (ASK) or 10% ASK), but requires sophisticated equipment and good technical skill. If 100% ASK is used, the attacker can modify only some bits (a bit of value 1 can be changed to a bit of value 0 but only if this bit is preceded by a bit of value 1; in all other cases the bits are essentially impossible to change). If 10% ASK is used, it is theoretically possible for the attacker to modify any chosen bits (change 0's to 1's and vice versa). Note that both modulation schemes (referred to as ISO 14443[61] Type A and Type B) are in widespread use for NFC payment transactions.

[58] Cowley, S., "NFC exploit: Be very, very careful what your smartphone gets near", CNN Money, July 26, 2012. See http://money.cnn.com/2012/07/26/technology/nfc-hack/index.htm (last accessed March 25, 2013).

[59] Kremer, J., "NFC: Near Field Communication White Paper", Jan Kremer Consulting Services. See http://jkremer.com/White%20Papers/Near%20Field%20Communication%20White%20Paper%20JKCS.pdf (last accessed March 26, 2013).

[60] Kerschberger, M., "Near Field Communication: A survey of safety and security measures", Bachelorarbeit, Technical University of Vienna, July 17, 2011. See https://www.auto.tuwien.ac.at/bib/pdf_TR/TR0156.pdf (last accessed March 26, 2013).

[61] ISO/IEC Joint Technical Committee 1, Subcommittee 17, Working Group 8, "ISO/IEC 14443 Identification cards – Contactless integrated circuit cards – Proximity cards".

- Data insertion is relatively difficult to perform because it requires a significant amount of luck as well as sophisticated equipment and good technical skill – there is a defined protocol (a set number of specified messages) between the sender and receiver devices and so the attacker will only be able to insert a message if one of the legitimate parties is especially slow to transmit its legitimate message (i.e., if there is an unexpected gap into which the attacker can squeeze his/her fake message). Note that if the legitimate party begins to transmit before the attacker's message has completed, the two messages will overlap and both will be corrupted.
- In a MITM attack, the attacker is positioned between the sender and receiver in such a way that the sender and receiver think they are talking with each other but in fact all their messages are going through the attacker (who can therefore add, delete, or modify messages at will). In NFC, given the very close proximity of the sender and receiver, as well as the fact that the active device is constantly sending a signal to power the passive device, it is essentially impossible for an attacker to remove sent messages, insert new messages, or modify legitimate messages without detection.

On the topic of eavesdropping, a thesis by Berkes[62] at University of Waterloo has examined the possibility of learning sensitive information based on a timing analysis of messages sent between a sender and a receiver in an NFC channel, and concluded that such attacks are feasible (given commercially-available equipment and good technical skill). By looking only at the messages sent and received in the contactless communication (and armed with a reasonable knowledge of the instruction set and processor speed of the smart card chip, which can be found in publicly-available specifications), it may be possible to infer what computation is going on inside the chip and perhaps even learn some of the hidden confidential data (such as portions of a private key). Some data in the tamper-resistant Secure Element (SE; see Section 3.3.1.1 below) of a mobile phone might therefore be vulnerable to simple passive eavesdropping of the over-the-air channel.

One final channel attack that must be mentioned is the relay attack (sometimes referred to as a "wormhole attack"). Although somewhat similar to both an eavesdropping attack and a MITM attack, the goal of the relay attack is different: the attacker is not attempting to learn the content of the messages (as with eavesdropping and MITM) and is not attempting to insert, delete, or modify messages between legitimate parties (as with MITM). Rather, the attacker wishes to take valid messages from a sender and transport them (relay them) some distance so that the distant receiver thinks that the sender is physically nearby. An attack scenario is as follows. The attacker's accomplice stands near a random person with an NFC-enabled mobile payment device (Alex) and relays signals between Alex and Bob, who is some distance away at an NFC POS terminal. Without knowing what is transpiring, Alex pays for Bob's purchase. (This attack may be particularly successful for low-value transactions that do not require user confirmation.)

Tomas Rosa, a Swiss researcher, has demonstrated that such relay attacks are indeed possible using generally available hardware, software, and computing devices[63].

[62] Berkes, J., "Side-Channel Monitoring of Contactless Java Cards", Master's thesis, Dept. of Electrical and Computer Engineering, University of Waterloo, 2008. See http://www.berkes.ca/archive/jb-thesis-final-electronic.pdf (last accessed March 26, 2013).

[63] Rosa, T., "RFID Wormholes: The Case of Contactless Smartcards", SmartCard Forum, Prague, Czech Republic, 2011. See http://crypto.hyperlink.cz/files/rosa_wormhole_v1a.pdf (last accessed March 26, 2013).

The conclusion with respect to NFC channel attacks is that while some attacks are very difficult to perform (perhaps impossible in a practical setting), such as MITM message modification, other attacks can be done fairly easily with commercially-available tools and low-to-moderate technical skills, such as eavesdropping, data corruption, and relay of messages. Even in the easy cases, however, the attacker (or an accomplice) must be physically very close to the victim (typically 0.5 m or less), which can often limit the risk to the user in real-world payment transactions. Note that cryptographic mechanisms such as the encryption of messages can help to protect against eavesdropping, but cannot prevent data corruption or relay attacks.

3.3 Corrupted Mobile Device

In order to understand some of the security and privacy risks of the NFC-enabled mobile, it is useful to look at the architecture of the payments portion of the device – what the various components are and how they interact. Following that, a description of possible avenues of attack will be given.

3.3.1 NFC Architecture of the Mobile Device

An NFC-enabled mobile device such as a smart phone has a combination of hardware and software that allows payment transactions to be made. The hardware includes an SE chip and an NFC chip, and the software includes a wallet and one or more payment applications (along with associated data).

3.3.1.1 Secure Element

The SE is an essential component for mobile payments. It is a tamper-resistant smart card storage chip (possibly with Common Criteria and FIPS certifications) for holding payment applications and account information. According to Elenkov[64],

> A smart card is essentially a minimalistic computing environment on a single chip, complete with a CPU, ROM, EEPROM, RAM and I/O port. Recent cards also come equipped with cryptographic co-processors implementing common algorithms such as DES, AES and RSA. Smart cards use various techniques to implement tamper resistance, making it quite hard to extract data by disassembling or analyzing the chip. They come pre-programmed with a multi-application OS that takes advantage of the hardware's memory protection features to ensure that each application's data is only available to itself. Application installation and (optionally) access is controlled by requiring the use of cryptographic keys for each operation.

Thus, the SE can hold multiple payment applications and is designed in such a way that the applications are isolated from each other and stored application data cannot easily be extracted by any other party.

The SE is composed of separate Security Domains (SDs) and Supplemental Security Domains (SSDs). A Security Domain is a security context within the SE: it includes a set of cryptographic, communication, and data management operations accessed by unique key material and controlled by a set of specific permissions[65]. A payment application in the SE requests cryptographic services (such as encryption or decryption, digital signing, or data authentication) through calls to its associated SD. The owner of an SE

[64] Elenkov, N., "Accessing the embedded secure element in Android 4.x", August 22, 2012. See http://nelenkov.blogspot.ca/2012/08/accessing-embedded-secure-element-in.html#!/2012/08/accessing-embedded-secure-element-in.html (last accessed March 12, 2013).

[65] Sequent Glossary; see http://www.sequent.com/glossary/s (last accessed March 12, 2013).

(a Mobile Network Operator, MNO, for example) manages a set of applications and corresponding SDs on the SE. Additionally, the owner may create and give control of a portion of the SE to another NFC service provider; this portion will contain the service provider's application and a security context for that application. Such a 3rd-party-controlled security context is referred to as a Supplemental Security Domain (SSD). See Global Platform[66] for further discussion of security domains.

Note that the word "owner", as used in the context of the SE, is not necessarily synonymous with "the accountable party". The SE owner is the entity that has possession of the SE prior to delivery into the hands of the consumer, and who has the authority to decide which applications and data will be installed on the SE. This, of course, confers on the owner some accountability (e.g., the owner should be responsible for getting the user back to his/her expected level of functionality if the SE stops working or somehow malfunctions and corrupts any stored data). However, if control of a portion of the SE is given to another party (i.e., an SSD) then some accountability must transfer to that party. Complicating things even further, even though the SE owner determines what applications and data can be installed on the SE, the owner does not see any of this data (it is encrypted under a key known only to the application issuer). Thus, accountability for the actual content of the SE data, which may (entirely at the discretion of the application issuer) include consumer personal information, must rest with the application issuer. Therefore, a number of parties may have obligations related to accountability, only one of whom is the SE owner.

Interestingly, there are three possible locations for the SE within a mobile device[67]. First, the SE can be embedded in the mobile handset itself. Second, the SE can be implemented on a Universal Integrated Circuit Card (UICC, often referred to as a Subscriber Identity Module (SIM) card). Third, the SE can be implemented on a MicroSD memory card. The first method is conceptually simple (the user purchases an NFC-enabled phone and it comes with an SE that is already in place), but does have at least two disadvantages: the SE (since it should be personal) will need to be registered and personalized after the device has been bought; and if/when the user wishes to change devices, all the SE applications and data will somehow have to be transferred to the new device and the SE of the old device will have to be deactivated (and perhaps all its data securely deleted).

The second and third methods (the UICC SE and the MicroSD SE) have the advantage of portability between mobile devices: if the user wishes to change his/her device all that is required is to remove the UICC or MicroSD from the old device and insert it into the new device. One potential disadvantage of the third method is that not every mobile device has a MicroSD slot, which clearly limits deployment possibilities.

The issue of where the SE is implemented is an important one: it typically defines who owns the SE itself. If the SE is embedded into the handset, then the mobile device manufacturer owns the SE. If the SE is implemented on a UICC, then the MNO (who typically issues the UICC to its customers) is the owner of the SE. Finally, if the SE is implemented on a MicroSD card, then whoever gives/sells the memory card to the user is the owner of the SE (for example, a credit card company or a bank may

[66] Global Platform, Card Specification Version 2.2, March 2006. See http://www.win.tue.nl/pinpasjc/docs/GPCardSpec_v2.2.pdf (last accessed March 15, 2013).

[67] Ericsson, D., "The role of SIM OTA and the Mobile Operator in the NFC environment", SmartTrust White Paper, April 2009. See http://www.paymentscardsandmobile.com/research/reports/SIM-OTA-Mobile-Operator-role-NFC.pdf (last accessed March 12, 2013).

decide to issue MicroSD cards containing its specific payment application directly to its own customers). Because the owner of the SE controls what payment applications can be installed on it, this question of ownership is of strategic importance to various players in the payment industry since it ultimately determines what payment instruments are available to any given user. As noted above, however, payment industry actors that are interested in being SE owners need to be aware that some level of accountability is an unavoidable part of that same role.

It is not clear that the location of the SE has any specific implications for privacy because the SE owner does not have access to payment application data regardless of where the SE is implemented (the SE owner controls which applications are installed, but application data is seen only by the application issuer). However, there may be slight implications for security. In particular, it may be easier in practice for a UICC or MicroSD to get lost or broken than a mobile device (simply because they are physically so small); on the other hand, it is clear that it would be easier for thieves to steal a phone than to borrow a phone, remove the UICC/MicroSD card, and return the phone without being noticed.

3.3.1.2 NFC Chip

The NFC chip ("NFC Controller") is a combination of hardware and software (the NFC Controller integrated circuit and the NFC Controller firmware) that controls the NFC radio signals transmitted to and from the antenna[68]. This chip is connected to the Secure Element, as well as to other (non-payment) native NFC applications that reside elsewhere on the mobile device[69]. In particular, the NFC Controller and the SE are physically separate chips that communicate over a channel (1 or 2 wires) via a standardized protocol. If the SE is implemented on a UICC, the protocol between the NFC Controller and the SE is called SWP (Single Wire Protocol[70]). On the other hand, if the SE is embedded in the handset or implemented on a MicroSD card, the protocol between the NFC Controller and the SE is called NFC-WI (NFC Wired Interface[71], also known as S2C)[72].

Note that the NFC Controller may be connected to multiple SEs (e.g., SEs simultaneously present on the UICC, the MicroSD, and handset)[73]. On the mobile device, a software module known as the Host Controller connects to both the NFC Controller (through the Host Controller Interface, HCI) and the SEs (through the ISO 7816[74] interface). The Host Controller, among other things, sets the operating modes

[68] Sequent Glossary; see http://www.sequent.com/glossary/n (last accessed March 15, 2013).

[69] Inside Secure, "Opening the NFC stack to Java and native applications", Corporate Background paper, November 2010. See http://www.insidesecure.com/content/download/1095/12802/version/6/file/WHITE%20PAPER_NEW%20CHARTE-3.pdf (last accessed March 15, 2013).

[70] Wikipedia, the Free Encyclopedia, "Single Wire Protocol". See http://en.wikipedia.org/wiki/Single_Wire_Protocol (last accessed March 15, 2013).

[71] Wikipedia, the Free Encyclopedia, "NFC-WI". See http://en.wikipedia.org/wiki/NFC-WI (last accessed March 15, 2013).

[72] CommTech Knowledge, "NFC-Near Field Communication: General Architecture of NFC Enabled Mobile Phones". See http://mp-nfc.org/nfc_near_field_communication_architecture.html (last accessed March 15, 2013).

[73] Ibid.

[74] ISO/IEC Joint Technical Committee 1, Subcommittee 17, "ISO/IEC 7816 Identification cards – Integrated circuit cards – Cards with contacts".

of the NFC Controller and establishes a connection between the NFC Controller and the SE[75], and so it is responsible for managing any potential conflict if more than one SE is present on the device (e.g., ensuring that only one SE is active at any given time).

The various components associated with the NFC Controller are shown in Figure 2 below (taken from Figure 1 in CommTech[76]).

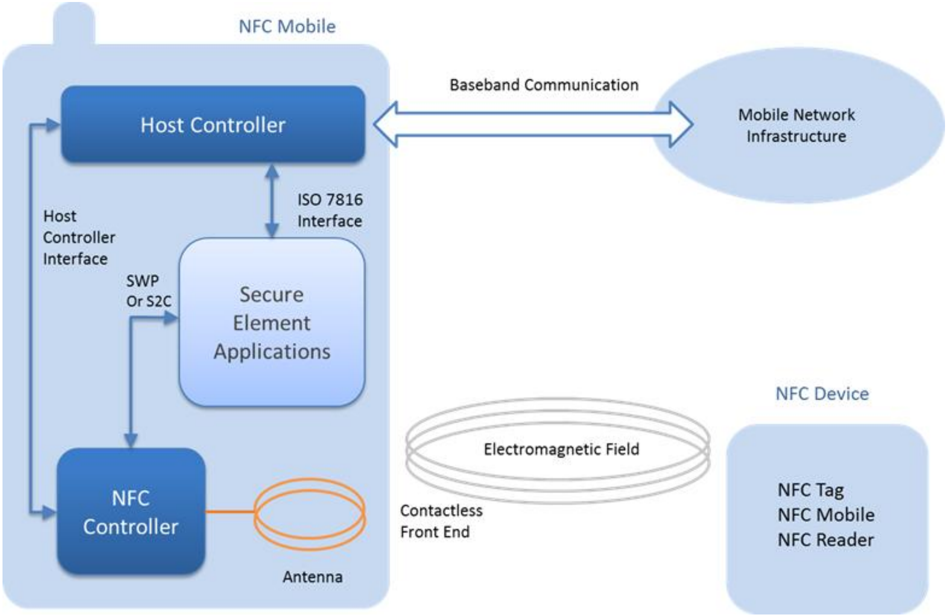

Figure 2. General Architecture of NFC Enabled Mobile Phones

The following is a brief description of how a mobile NFC payment transaction physically works.

- At provisioning time: The NFC channel is not used in the provisioning step (this is the payment brand / bank downloading the app and data through the MNO to the wallet to the SE). Thus, this download does not go through the NFC Controller, but instead goes over the mobile wireless network to the Host Controller and through the ISO 7816 interface to the SE. This step physically puts the apps and data on the various SEs and does whatever else is required to enable them to make mobile payments.
- At payment setup time: The wallet app interrogates the SEs (through the Host Controller, through the ISO 7816 interface) to find out what payment apps are present, so that it can display these choices to the user. When the user selects a particular payment instrument (e.g., MasterCard debit card), the wallet app instructs the NFC Controller (through the Host Controller, through the Host Controller Interface (HCI)) to bind to the MasterCard debit card on a particular SE (using specific identifiers for that payment instrument and SE). The NFC Controller then puts any other SEs that might be present on the device into "off" mode (by sending a signal through the SWP or S2C protocol), puts the SE that contains the MasterCard debit card app into "you're talking with me" mode (by sending a signal through the SWP or S2C

[75] CommTech Knowledge, "NFC-Near Field Communication: General Architecture of NFC Enabled Mobile Phones". See http://mp-nfc.org/nfc_near_field_communication_architecture.html (last accessed March 15, 2013).

[76] Ibid.

protocol), and binds to this payment instrument by sending a "get ready" message with this app's identifier to this SE (this effectively tells this app to start listening and all the other apps on this SE to ignore the subsequent messages). Finally, the NFC Controller puts this SE into "you're talking with the outside world" mode (by sending a signal through the SWP or S2C protocol).

- At payment time: Messages from the contactless POS terminal (more precisely, from a MasterCard application on a PC connected to the POS terminal) travel the very short distance through the air using the ISO 14443 protocol to the Contactless Front End on the phone, are received by the antenna, are converted from analog to digital, and are channeled by the NFC Controller through the SWP or S2C protocol directly to the MasterCard debit card app on the SE. Similarly, messages from the app are sent in the opposite direction to the POS terminal. Any other application on the mobile device can register to receive a notification whenever an NFC transaction occurs[77], but this notification only says that the event is happening (it doesn't give the data transmitted in the message). Furthermore, such an application needs to pass an Access Control Framework (ACF) check for the SE app involved in the transaction in order to be allowed to receive such transaction notifications[78].
- When the payment transaction has concluded, the NFC Controller will recognize that the NFC message flows have terminated (or that the antenna is no longer within range of the POS device) and will put the SE in "off" mode. Additionally, the user may close the MasterCard debit card app and/or the wallet app.

The next two subsections look at the payment-related software on an NFC-enabled mobile device.

3.3.1.3 Wallet

As mentioned in Part 1 of this report, a wallet is an app that manages the various payment instruments and interfaces with the payer (e.g., to enable him/her to select a particular payment instrument to use at the time of a purchase). A number of organizations have chosen to become wallet providers (as part of their business), including Google, Isis, Visa, MasterCard, and various banks. Not surprisingly, such competition has led to different types of wallet app: mobile wallets; digital wallets; and hybrid wallets[79].

- A mobile wallet is an app on the phone that manages the payment instruments. This wallet is typically installed by the user (although it may come pre-installed when the device is purchased) and will need to be moved / transferred in some way if the user changes the device in the future. An example of this type of wallet is the Rogers/CIBC Mobile Wallet.
- A digital wallet (somewhat confusingly named, since all software apps are digital) is a wallet application that resides off the phone, such as on a server or in the cloud. This wallet is not installed by the user, but is accessed via the web through a login procedure. If the user changes

[77] BlackBerry Support Community Forums, "BlackBerry 10 – NFC Card Emulation", November 2, 2012. See http://supportforums.blackberry.com/t5/Native-Development/BlackBerry-10-NFC-Card-Emulation/ta-p/1940867 (last accessed March 20, 2013). See also "NFC Primer for Developers", February 14, 2012, http://supportforums.blackberry.com/t5/Java-Development/NFC-Primer-for-Developers/ta-p/1334857 (last accessed March 20, 2013).

[78] Ibid.

[79] Crowe, M. and E. Tavilla (Federal Reserve Bank of Boston), "Mobile Phone Technology: 'Smarter' Thank We Thought: How Technology Platforms are Security Mobile Payments in the U.S.", November 16, 2012. See http://www.bos.frb.org/bankinfo/payment-strategies/publications/2012/mobile-phone-technology.pdf (last accessed March 21, 2013).

the device in the future, nothing needs to be done in order for the user to continue using the wallet. An example of this type of wallet is the PayPal Digital Wallet.

- A hybrid wallet is a server- or cloud-based wallet that has some component or portion that resides on the phone. The user must install this portion, and running this portion on the device may automate the login to the server/cloud portion so that the user need not even be aware that there are two portions of the wallet. An example of this type of wallet is Google Wallet.

Wallets (whether mobile, digital, or hybrid) have evolved to include services beyond simply managing payment instruments, such as managing a user's financial portfolio, tracking and using reward / loyalty points, receiving special offers from merchants, and storing digital receipts and warranty information[80]. Protection of all this sensitive information typically comes from a password or PIN which is entered by the user to unlock the wallet. Note that at least one company (Inside Secure) supports the coexistence of multiple wallets on the same mobile device[81] and so the amount of sensitive information on a single mobile device may grow even larger.

3.3.1.4 Payment Applications and Payment Credentials

As mentioned earlier in this section, payment applications and payment credentials (data), which are owned by the payment brand and personalized for the user, are downloaded and installed on the SE of the mobile device at provisioning time. Typically, the owner of the payment app / data and the owner of the SE are different entities (e.g., Visa owns the payment app and Rogers owns the UICC that contains the SE); thus an agreement must be reached between these entities before the app and data can be installed – cryptographic protections prevent access to the SE otherwise. Other payment instruments which are downloaded to the mobile device but do not reside on the SE (coupons and loyalty cards, for example, which are stored within the wallet's memory space) do not require such an agreement and can be installed by the user or by other entities (e.g., merchants) at any time.

Payment apps on the SE may be locked, requiring a password or PIN to unlock them before they can be used. Typically, the wallet application enables this protection (allowing the user to choose whether or not to lock each individual payment instrument[82]). However, wallets normally also allow the user to select a particular payment credential as the default: "A default credential allows end users to initiate a payment without having to take the mobile device out of standby mode and without having to manually select a wallet."[83].

Note that any PINs / passwords used to lock specific payment apps are separate from a PIN / password to unlock the wallet application as a whole (and also separate from a PIN / password / biometric which

[80] Visa, "Digital Wallet Security: Just 'LOK' it". See http://www.cimbbank.com.my/creditcard/index.php?ch=2&pg=14&ac=9&bb=attachment (last accessed March 21, 2013).

[81] Ricknas, M., "Inside Secure Opens Door for Multiple Wallets on One Smartphone", CIO Drilldowns, October 29, 2012. See http://www.cio.com/article/720174/Inside_Secure_Opens_Door_for_Multiple_Wallets_on_One_Smartphone (last accessed March 21, 2013).

[82] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012, p. 2. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed February 14, 2013).

[83] Ibid, p. 26.

may be used to lock the mobile device itself). Thus, several levels of protection are possible, but employing more levels may lead to an increasingly frustrating user experience.

3.3.2 Security and Privacy Risks on the Device

The security and privacy risks on the mobile device can be divided into two categories: hardware-based attacks (requiring physical access to the targeted device) and software-based attacks.

3.3.2.1 Hardware-Based Attacks

The architecture outlined above makes a physical attack possible: if an attacker physically acquires a victim's phone and knows the (standardized or otherwise publicly available) HCI, SWP/S2C, and ISO 7816 interfaces, then the attacker can put clips/probes on these wires (see, for example, Roland, et al.[84]) and send authentic-looking messages to the NFC Controller and the SEs. In this way, the attacker can accumulate charges on the victim's accounts and transfer money to a "merchant" of the attacker's choice (e.g., his/her own registered account). Note that all security protection over this NFC payment system (such as passwords/PINs to unlock the wallet and/or the payment instruments) is almost certainly in software (i.e., in the wallet app, because the user can choose whether to require PINs or not when these apps are used), and so this physical hardware attack will bypass all that protection and talk directly with the SEs and their payment apps.

3.3.2.2 Software-Based Attacks

Mobile payment using NFC is different from card payment using NFC in one fundamental way. In terms of provisioning they are somewhat analogous, and in terms of the actual payment process they look identical. The risks from a malicious reader, or an eavesdropper/MITM between the device/card and the reader, are also identical. Even a physical hardware attack on the wires between integrated circuit components may work in a similar way for mobile devices and cards. Therefore, it seems that the real difference is the potential for a malicious party to install malware on a user's mobile device (it is not currently possible for an attacker to install malware on a user's NFC-enabled credit card).

Because the NFC chip and the SE chip are physically separate integrated circuits connected only by physical wires to each other and to the Host Controller, no software on the phone has direct access to either of these chips. Consequently, malicious software attacks must either come from a corrupted Host Controller or from another corrupt app that causes the uncorrupted Host Controller to send instructions on its behalf.

Corrupt Host Controller

As seen in Section 3.3.1.2 above, the Host Controller sits between the mobile device applications (including the wallet) and the payment applications that are on the SE. In particular, the Host Controller responds to wallet requests to inform the wallet of where each payment application is stored and to provide an identifier by which to locate and interact with a given payment application (see, for example,

[84] Roland, M., C. Saminger, and J. Langer, "Packet Sniffer for the Physical Layer of the Single Wire Protocol", Research report, Upper Austria University of Applied Sciences. See http://research.fh-ooe.at/files/publications/941_PacketSnifferPhysicalLayerSWP.pdf (last accessed March 19, 2013).

the Reference Model[85], p. 68, where the Host Controller is referred to as an "umbrella application" when the SE is on a UICC). The Host Controller also communicates with the NFC Controller to set its operating mode and to tell it which payment application to bind with so that a payment transaction can take place.

Recalling that the Host Controller does not see any of the payment app data (because that data passes through the Host Controller at the time of installation, but only in encrypted form) and does not see any payment transaction details (because payment transactions do not pass through the Host Controller, but go directly from the NFC Controller to the payment app on the SE), it is worth considering what a corrupted Host Controller could actually do to harm security or privacy in mobile payments. Clearly, one thing it can do is to give the wrong payment app identifier to the wallet or to the NFC Controller (so that, for example, the user thinks the payment is being made using MasterCard when in fact it is being made using Visa). This may be surprising or annoying to the user when the bill arrives later in the month (if s/he even notices this) but, since both payment instruments are legitimately associated with the user, this may not constitute a security or privacy breach. On the other hand, the Host Controller could put the NFC Controller into an inappropriate mode at an inappropriate time (for example, turning on active mode so that the phone reads a malicious NFC tag when the user is not expecting it, or turning on card emulation mode to allow a payment transaction to occur without the user's request). Such behaviour could certainly lead to security or privacy breaches. Note, however, that the corrupt Host Controller would need to act in conjunction with an external device (i.e., a corrupt NFC tag or an NFC reader / POS terminal) in order for any breach to occur; the corrupt Host Controller on its own is not able to cause security or privacy problems.

Corrupt Payment App in SE

Another possible software attack is that the payment app that the user wishes to use is corrupt. For example, a corrupt Visa app has been installed on the device so that when the user tries to pay with Visa some malicious activity occurs (e.g., someone else's account gets charged because the wrong account number is sent to the POS, or the correct user's account gets charged too much).

The risk of such an attack, while perhaps not zero, can be presumed to be very low. According to the Canadian NFC Mobile Payments Reference Model[86], p. 14, Section 6.8, payment apps and associated data are installed by the payment brand (e.g., Visa) itself (in encrypted form, through the MNO), following a prior agreement with the owner of the SE (e.g., the MNO). It is highly unlikely that Visa would themselves install a corrupt Visa app on the mobile devices of their own customers, and it is also unlikely that the MNO would permit installation of a payment app by some other "shady" or untrusted payment brand.

[85] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed February 14, 2013).

[86] Ibid.

Other Corrupt App in SE

A variation of the above attack is that some other app (i.e., other than the one that the user wishes to use) is corrupt. For example, a corrupt MasterCard app has been installed on the device so that when the user tries to pay with Visa some malicious activity occurs (e.g., MasterCard learns something about the payment details).

Again, the risk of such an attack is very low. In fact, there are several safeguards to protect against this. First, as with the attack above, the malicious MasterCard app would need to be installed by MasterCard with agreement from the SE owner. Second, the Canadian NFC Mobile Payments Reference Model[87] specifies (p. 28, Section 8.4.1) that only one payment application can be turned on (i.e., available for payment) at a time; if one payment app is turned on, the rest must be turned off. Thus, if the user has selected Visa as the payment instrument for a transaction, the MasterCard app (whether malicious or not) will not be running. Finally, the SE itself has been built in such a way that the apps installed on it are partitioned (i.e., they cannot see each other or each other's data).

Corrupt Wallet

Yet another possibility is that the wallet application is corrupt. Note that the wallet does not reside on the SE and so there are fewer restrictions on how it gets installed on the device (e.g., the user may choose to download a free wallet from some website). A corrupt wallet may try to learn something about a payment transaction and communicate this to another party (e.g., the wallet provider); it may also try to modify payment messages (e.g., change account numbers or transaction amounts) or manipulate sensitive stored data (e.g., loyalty program balance data).

According to the Canadian Reference Model[88] (p. 31), a mobile wallet may capture transaction data for all payment applications to which it is linked; however, if it does capture this data, access to and usage of this data must be restricted as per the standards in the Data and Security section of the model. The Data and Security section (pp. 82-90) states that the wallet can collect and store all financial data, loyalty data, payment product data, and loyalty balance data, but no one else (including the wallet provider) should have access to this data. These stipulations are an important implementation guideline for a wallet that wishes to comply with the model, but how can this be enforced for a malicious wallet? In particular, what prevents a malicious wallet from doing whatever it pleases with the data that it holds?

One potential safeguard is that the payment and loyalty data stored in the wallet may be encrypted (using a key known only to the associated payment / loyalty application). This is definitely helpful, but it is important to note that encryption is not mandatory (the payment / loyalty app can choose to encrypt this data or not) and even if encryption is used, some data remains unencrypted, including credit card number, name on the credit card, and card verification value; this data may therefore be available to a malicious wallet. Another safeguard is that the wallet is not able to see the transaction details (i.e., the protocol message contents, such as the amount of the purchase) because these travel directly from the NFC Controller to the app on the SE and are therefore not accessible to the wallet.

[87] Ibid.

[88] Ibid.

Another Corrupt App on the Phone (Not in SE)

Finally, some other app (i.e., not the wallet) that is installed on the phone (i.e., not in the SE) may be corrupt. Is it possible that such an app could access the payment transaction messages (e.g., read or modify the data between the NFC chip and the legitimate payment app on the SE) so that the user sees and approves a $2 Visa payment to Starbucks but in fact $200 is charged to the user's Visa account? As above, there are multiple safeguards to protect against this. First, payment transaction messages are sent over physical wires from the NFC Controller to the SE; no software on the device has any way of accessing these messages[89,90]. As mentioned in Section 3.3.1.2, an application can register to receive notifications when NFC transmissions occur, but these notifications only indicate that a transmission is taking place (they do not reveal the content of the transmissions). Second, even if it was somehow possible for an app to access the payment messages, such messages are normally encrypted between, for example, the Visa app on the POS terminal and the Visa app on the SE; any other app intercepting the messages would not know the key and would therefore be unable to decrypt the content.

3.3.2.3 Other considerations

Some other security and privacy considerations are as follows. First, some payment instruments (such as coupons and loyalty cards) may be stored not on the SE, but rather in the regular memory of the mobile device (e.g., in the memory space of the mobile wallet app). As noted above, a corrupt wallet would be able to access and manipulate this data for malicious purposes (if the data is not encrypted), but are other apps able to see, use, or modify these instruments? On some devices (such as Android phones), app isolation has been enforced so that an app cannot see the data or internal state of any other app. Note, however, that if the phone has been "rooted" (or "jailbroken"), apps may be able to elevate their privileges and such protections may be circumvented. Consequently, a good mitigation for this threat is to encrypt the payment instrument data. Alternatively, a digital wallet (as opposed to a mobile wallet) may offer some protection: if these payment instruments are stored on a server or in the cloud, rather than on the device, then other apps on the device will not have access to this stored data even if the device has been rooted (note, however, that these apps may have access to the data as it moves from the cloud through the device to the merchant in a payment transaction).

Second, it is worth raising the question of whether there are security, privacy, or accountability implications for different flavours of wallet. For example, with a mobile wallet all payment data is on the device itself and may be vulnerable if the device is lost or stolen; on the other hand, with a digital wallet all payment data is in the server / cloud and may be visible to others if not protected properly. As another example, a PIN might not be used to unlock the mobile wallet on the device (this is a choice made by the user), whereas a password / PIN must always be used to login to a digital wallet on a server (no user choice). As an additional example, a mobile wallet (i.e., on the device) talks to the SEs through the Host Controller, whereas a digital wallet (i.e., in the cloud) presumably talks to the SEs through the browser through the Host Controller: thus, there could be security/privacy considerations if the browser has any known security vulnerabilities.

[89] Jackson, B., "Google Wallet and NFC security: guarding against 'sharks with lasers'", IT Business, September 29, 2011. See http://www.itbusiness.ca/news/google-wallet-and-nfc-security-guarding-against-sharks-with-lasers/16531 (last accessed April 4, 2013).

[90] Pipenbrinck, N., "Secure Element communication with PCD/reader", stackoverflow, June 22, 2012. See http://stackoverflow.com/questions/11152614/secure-element-communication-with-pcd-reader (last accessed April 4, 2013).

Third, the Canadian NFC Mobile Payments Reference Model (p.2, 3rd paragraph) ensures that the consumer has the ultimate say over whether his/her payments have passcode protection and which payment types are enabled on the mobile device. It is certainly worth considering whether the average consumer will do a good job with this.

Fourth, according to the Canadian Reference Model (p.63, Section 10.6.1), even if mobile service is disconnected, the payment application may continue to work for NFC payments. It is worth considering whether this is always a good thing – is there a chance that payment transactions might occur when the user is not expecting them?

Finally, the Canadian Reference Model describes not only single-tap payments (i.e., for convenience transactions), but also single-tap reimbursements (i.e., for returns), perhaps with an electronic receipt for the return. No signature, pass code, or PIN is required from the user in order to process a return (p. 45). For receipts sent via SMS, mobile OTA (over-the-air), or NFC, it is recommended that the receipts be in text format; receipts sent via e-mail to the device can use text or PDF (p. 42). This, of course, raises the question as to whether it may be possible to steal someone else's receipt (e.g., by eavesdropping on the NFC or wireless channel at payment transaction time, or by breaking into the e-mail account) and then go back to the store at some later time to get reimbursed (e.g., for a stolen item that is similar to the one purchased by the real customer).

3.4 Summary

The NFC mPOS payment model appears to have a carefully-considered hardware and software design with a number of safeguards built into the overall architecture and transaction flow. However, no model is invulnerable (particularly when intended to be implemented in a usable way in widely-deployed consumer / commercial settings). This section has highlighted a set of potential security and privacy concerns ranging from malicious readers, to malicious parties on the wireless NFC channel, to attackers using hardware or software tools in order to subvert the proper operation of the mobile device. Finally, some questions are raised regarding storage of some payment instrument data, different types of wallet, passcode protection, continued availability of payments when mobile service has been disconnected, and reimbursements using electronic receipts.

4. Some mP2P Payment Models

This section looks briefly at two mP2P payment models: M-Pesa and MintChip.

4.1 M-Pesa

M-Pesa, the payment system built around text messaging on mobile phones, has been operating in Kenya since 2007 and has since been deployed in several other Asian, Middle Eastern, and African countries. (For an interesting discussion of the initial rollout of M-Pesa in rural areas of Kenya, see the M-Pesa Project Analysis by Télécoms Sans Frontières[91].)

[91] Hermon-Duc, S. (TSF Project Manager), "MPESA project analysis: Exploring the use of cash transfers using cell phones in pastoral areas", Télécoms Sans Frontières Project Report, 2012. See http://www.alnap.org/pool/files/mpesa-project-analysis-tsf-vsfg.pdf (last accessed April 12, 2013).

By all accounts, M-Pesa has achieved high acceptance rates and has been an unqualified success in Kenya and elsewhere, particularly in making money transfers available to users who have no other access to traditional banking services. Not surprisingly, however, where there is money, there are malicious actors who will try to attack the system in some way in order to steal money. The following two examples are real attacks on the M-Pesa system that have been documented. It is important to note, however, that neither of these attacks can be fully automated: involvement of a human attacker or accomplice is required, which limits the extent to which the attack can be operated on a large scale.

One interesting attack was documented in 2010[92]. On February 1, 2010, two people approached an M-Pesa agent on the outskirts of Nairobi, claiming to be employees of Safaricom (a mobile network operator in Kenya) conducting an audit of the agent (the two people presented M-Pesa publicity material and Safaricom identity documents). This was not suspicious because such audits are carried out on a regular basis across Kenya. They asked to see the accounts and were allowed to examine the accounts for a period of time; the two people then departed. About 20 minutes later, another man approached the agent and requested an amount of cash. He appeared to start the M-Pesa transaction on a mobile device. Following this, the agent received a message purporting to be an M-Pesa transaction authorization, which contained the agent's current account balance. The agent verified the man's name on his national identity card and gave him the requested cash. Later, while processing another (legitimate) M-Pesa transaction, the agent discovered that the previous transaction had not been recorded. Thus, the agent lost roughly $450. This attack worked because a fake transaction authorization message from the attacker was accepted as a true transaction authorization message from Safaricom. It turns out that the "shared secret" (between Safaricom and an agent) that authenticates such messages is the agent's account balance with Safaricom. The two men posing as Safaricom auditors were able to look at the agent's books and learn this balance; hence they were able to create a convincing transaction authorization message and succeed in getting the agent to give money to their accomplice. As mentioned in the report[93], it is interesting to note that M-Pesa's own security system – regular audits – was used to obtain the information required to attack M-Pesa. As noted above, this attack cannot be fully automated (at the very least a human accomplice needs to physically visit a target agent), which limits the extent to which it can be conducted on a large scale.

A second type of security attack on the M-Pesa system has also been documented[94]. When M-Pesa was introduced, old SIM cards would not work with the new service; only users with new SIM cards could register as M-Pesa users (users of phones with old SIM cards could use the service, but only as unregistered users who had to pay more to retrieve money at an agent). Malicious parties took advantage of the fact that many mobile money users have old phones with old SIM cards and use prepaid services. A malicious party would take a new SIM card and register as one of the users of an old SIM; thus, anyone logging into the Safaricom database of users would see the legitimate name as the user of the phone number, but in fact the malicious party is the M-Pesa registered user associated with that number. According to Safaricom rules, money sent via M-Pesa is returned to the sender if not

[92] Telco 2.0 News Review (blog), "Security Breach at M-PESA: Telco 2.0 Crash Investigation", Telco 2.0, February 12, 2010. See http://www.telco2.net/blog/2010/02/security_breach_at_mpesa_telco.html (last accessed April 12, 2013).

[93] Ibid.

[94] Wanjiku, R., "Security issues hit African mobile money providers", Computerworld, November 17, 2009. See http://news.idg.no/cw/art.cfm?id=03381EE0-1A64-6A71-CE896C46D67B6FFC (last accessed April 12, 2013).

withdrawn within seven days. During this window of opportunity, then, the malicious party would quickly withdraw the money sent to the legitimate party (i.e., the unregistered user with the old SIM card). The legitimate party would subsequently go to an M-Pesa agent to retrieve the money that had been sent to him/her and discover that the money had already been retrieved. Again, this attack requires physical involvement of the human attacker and so cannot be easily automated and operated on a large scale.

Given the primary motivation for M-Pesa (i.e., enabling money transfers among a large user population without any access to traditional banking services), it is unlikely that this payment scheme will find widespread use in Canada. However, an examination of this scheme raises points that may apply equally to other schemes (such as the vulnerabilities that arise from malicious human actors, or the (mis)use of a security mechanism like an audit to ultimately defeat the system). Thus, the lessons learned from looking at M-Pesa can be helpful in analyzing the security of other payment schemes.

4.2 MintChip

As described in Part 1 of this report, the Royal Canadian Mint's MintChip system has a P2P model that allows users to transfer MintChip value using mobile texting (SMS), e-mail, or NFC communication. The devices exchange Request and Value messages. The Request message includes (among other things) the amount to be paid, the currency of the payment, the ID of the payee (receiver), an address telling the sender where to send the money, and a random 32-bit integer. The (digitally signed) Value message includes essentially the same information, along with a date and time, the payer's ID, and the payer's public key certificate (for verification of the payer's signature). Creating the Value message at the sender end decrements the sending chip's balance; verifying the validity of the Value message at the receiver end increments the receiving chip's balance.

The MintChip system is still in the proposal stage and has not yet been deployed to Canadians. Consequently, a security and privacy analysis can only be performed on the basis of the few implementation details given on the MintChip website[95]. However, there are some possible concerns / questions. First, it is interesting to note that the MintChip Request message does not appear to be protected in any way (the Value message is digitally signed, but the Request message is not). Therefore, anyone can create Request messages at will. More importantly, anyone can modify the Request message in transit between the sender (the payee) and the receiver (the payer). In particular, it is likely that a Request message will be received by the payer, a dialog will be displayed to the user to confirm the transaction, and then the Request message will be processed in order to create the corresponding Value message. Malicious software on the user device may therefore be able to modify the Request message between confirmation and processing, so that the payer pays more than expected, for example.

Second, it is curious to see that the amount field in the Request and Value messages is a 24-bit unsigned integer representing the transaction amount in cents. With 24 bits, this field can hold values in the range (0 – 16777215). This is more than $167,000 – hardly a micropayment or a nanopayment! It is not clear why this field is so large when the Royal Canadian Mint has stated that it hopes MintChip will be used for transactions under $10.

[95] The Royal Canadian Mint, "MintChip Developer Resources: MintChip Messages", April 4, 2012. See http://developer.mintchipchallenge.com/devguide/developing/common/mintchip-messages.html (last accessed April 8, 2013).

Third, once a Value message has been created and sent, the value is subtracted from the chip and this transaction is irrevocable. In particular, if the Value message is not received by the payee, or if it is received but corrupted (e.g., the digital signature does not verify), the payer will have lost money but the payee will not have gained money. This is analogous to dropping coins down a drain while trying to pay someone with physical currency. This seems somewhat risky, but it is not clear that better alternatives exist (for example, one could envision a 3-message protocol in which the final message is a Confirmation from the payee which then causes a deduction from the payer's account; however, if this final message gets lost or corrupted, the payee's account would have been incremented and the payer's account would not have been decremented, so money would just have been created out of nothing). On the other hand, the defined 2-message protocol is clearly vulnerable to a denial-of-service attack where Value messages are corrupted in transit, resulting in a draining of the payer's account without the payer receiving any corresponding goods or services.

Fourth, the Value message includes a payerID and a payeeID, along with a payer certificate (required to be included so that the digital signature can be verified). Even if these values are not stored long-term by anyone (including the MintChip system and the various payees), this does raise the question of whether it is possible for payers to conduct MintChip transactions anonymously (as can clearly be done with physical currency, which the MintChip system is intending to mimic in the digital economy).

Finally, the website[96] claims that MintChip Value messages use RSA SHA-1 digital signatures. Given that the cryptographic hash function SHA-1 has been deprecated since January 2011 and is not to be used for digital signature generation after 2013[97,98] (and that there are some doubts about the SHA-2 variants), this standard was replaced by the new hash function SHA-3 as of October, 2012[99]. Digital signatures should evolve to using SHA-3 in the very near future, and continue to evolve to employ the most secure and privacy protective solutions.

5. The mAccept Payment Model

In the mAccept payment model, the merchant has a mobile device (such as a tablet or a smart phone) which has been enhanced in some way to allow it to accept traditional (magnetic stripe) credit cards. A variation of this model enables the consumer to use a mobile device instead of a traditional credit card but, in any case, the defining feature of the mAccept model is that the merchant has replaced the POS terminal with a mobile device.

[96] The Royal Canadian Mint, "MintChip Developer Resources: Message Validation", April 4, 2012. See http://developer.mintchipchallenge.com/devguide/developing/common/message-validation.html (last accessed April 8, 2013).

[97] Barker, E., and A. Roginsky, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST Special Publication 800-131A, January 2011, pp. 13-14. See http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf (last accessed May 13, 2013).

[98] Moffa, T. (Communications Security Establishment Canada), "CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within the Government of Canada", CSEC ALERT ITSA-11E, March 2011, Section on "Hashing Algorithms and Status of SHA-1". See http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11e-eng.html (last accessed May 13, 2013).

[99] U.S. National Institute of Standards and Technology (NIST), "NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition", NIST Tech Beat, October 2, 2012. See http://www.nist.gov/itl/csd/sha-100212.cfm (last accessed April 8, 2013).

One of the emerging companies / technologies in this area is Square[100]. Square was started by Jack Dorsey, one of the co-founders of Twitter, and has recently achieved $10 billion in payments processed. There are over 200,000 businesses that accept payment using Square, and a deal with Starbucks allows payment by Square at over 7,000 Starbucks locations (Starbucks has also invested $25 million in Square and sits on their Board of Directors)[101]. The Square payment system has two pieces: Square Register (for the merchant); and, optionally, Square Wallet (for the customer).

Square Register consists of a software app that is installed on the merchant device, along with a small plastic square (actually a cube) that plugs into the headphone jack of an iPhone, iPad, or Android device. The cube has a small slit where a credit or debit card can be swiped. The cube and app are free, but the merchant pays Square 2.75% per swipe for payment transactions. Once the purchase is complete, a digital receipt can be e-mailed or texted to the customer, or a paper receipt can be printed and given. The primary benefit of Square Register is that credit / debit card payments can be accepted anytime and anywhere (e.g., at a garage sale, a farmers' market, or a roadside flower stand); from the customer's point of view, the transaction seems very similar to a traditional card swipe at a POS terminal. On the other hand, unlike with a traditional POS terminal, the merchant's business data is stored on Square servers, not on the mobile device (the motivation, of course, is that the merchant need not worry if the device is lost or stolen). So, information such as business profile settings, deposit schedule, rewards programs, bank account settings, in-depth business analytics, employee permissions, transaction history, and staff management data all reside with Square[102]. This may raise some security and / or privacy concerns, particularly around how securely this data is stored and who has access to it.

Square Wallet is an optional extension of the Square payment system that allows customers to pay at businesses in the Square directory (i.e., businesses that use Square Register) using a mobile device instead of a magnetic stripe card. (Square Wallet will reportedly be available in Canada sometime in 2013.) The user downloads the free Square Wallet app, signs up for the service, and enters a credit / debit card (several are accepted, including Visa, MasterCard, AMEX, and Discover). During sign-up, the user is able to upload a photo of him/herself. Once registered, the customer can use the built-in discovery tool to find a nearby business that accepts Square payments; the customer then clicks on the business and opens the tab ("Slide to Pay" – note that the tab can be left open for businesses that the customer visits regularly). When the phone is within range of the merchant's Square Register app (interestingly, the phone may still be in a pocket or a purse), the customer's name and picture will appear on the merchant's screen in a list of available payers. The customer tells the cashier his/her name, the cashier compares the customer's face to the photo, the cashier selects that payer, and the transaction goes through[103]. In terms of security / privacy concerns, it is interesting to note that there is no password or PIN for the Square Wallet app (the only way to prevent payments is if the tab is closed). Furthermore, the merchant sees the photo and name of potential buyers (those with the app running

[100] Square, Inc. See https://squareup.com/ca?country_code=ca (last accessed April 5, 2013).

[101] Terdiman, D., "Prowling the streets of San Francisco with Square Wallet", CNET News, November 20, 2012. See http://news.cnet.com/8301-1023_3-57552199-93/prowling-the-streets-of-san-francisco-with-square-wallet/ (last accessed April 5, 2013).

[102] Square, Inc., Square Register. See https://squareup.com/ca/register (last accessed April 5, 2013).

[103] Duffy, J., "Pay With Square (for iPhone)", PC Magazine (pcmag.com), August 9, 2012. See http://www.pcmag.com/article2/0,2817,2408287,00.asp (last accessed April 5, 2013).

and the tab open – a likely combination at Starbucks, for example), even if they decide to pay by cash. Finally, it is worth noting that Square (the company) learns the customer's name, photo, and purchase history (including precise location and items purchased); this is more information than a credit card company currently knows.

The use of Square, particularly the pay-by-name feature, also gives rise to an additional security concern. Say Bob walks into Starbucks and sees his colleague Ted sitting in the corner with a hot chocolate and a muffin. Bob knows that Ted has an open tab with Square for this Starbucks and that he and Ted look somewhat similar. So, Bob goes to the counter, orders a latte, tells the cashier he'd like to pay using Square, and says the name "Ted". The latte now gets charged to Ted's credit card (Ted may not discover this until his next credit card bill arrives and, even then, he might not notice because he's not likely to remember whether he ordered a latte several weeks ago and may not see that it was charged on the same day as his hot chocolate and muffin). Even worse, Bob may see a similar-looking stranger ahead of him in line make a purchase with Square and hear him as he says his name. By the time Bob gets to the counter (especially if the Starbucks is extremely busy or if the cashier has changed) he may be able to use this stranger's name to pay for his latte. One can imagine that the impact of this attack would increase significantly if the merchant was not Starbucks but another establishment in which the payment amounts are routinely much higher.

Clearly the pay-by-name feature, although convenient and easy to use, appears to be vulnerable to a simple impersonation attack. This is intended to be mitigated by having each user upload a photo when registering for Square, but it is well known that a photo can be a very rough approximation of a person's face, particularly if hair length or style has changed, a beard has been grown or removed, or a hat or sunglasses are worn. The notification message sent to Ted's mobile confirming successful payment is also helpful, but may not completely prevent this attack if Bob has already left the store with his latte.

6. General Technological Risks of Electronic Financial Transactions

As should be clear from Part 1 of this report, a number of different mobile payment models have been proposed and/or deployed; it is likely that new ones will continue to appear over time[104]. The mobile payment industry is already quite sizeable and is expected to grow by substantial amounts in the next few years (see, as one example, Collins[105], in which Visa predicts that by the year 2020 over half the transactions made by consumers in Europe will be done through mobile payments). Therefore, even though the previous sections of this report have discussed specific payment models and technologies, it is useful to consider security and privacy risks that pertain to all (or many) payment models simultaneously. This section, then, discusses some risks and dangers inherent to purely electronic payment systems on mobile devices.

[104] Bradley, M., "Digital Wallets Executive Briefing", Information Technology Association of Canada (ITAC) Digital Commerce Forum: How Your Wallet is Going Digital, April 16, 2013. See http://itac.ca/files/2013_april_16_digital_wallet_presentation.pdf (last accessed May 1, 2013).

[105] Collins, J., "Mobile payments deal between Visa and Monitise is formed", Mobile Commerce News, March 11, 2013. See http://www.qrcodepress.com/mobile-payments-deal-between-visa-and-monitise-is-formed/8518094/ (last accessed April 16, 2013).

In general, the privacy concerns discussed below relate to the OECD Fair Information Principles of Safeguards, Consent, Accuracy, and Individual Access. Where appropriate, relevant Personal Information Protection and Electronic Documents Act (PIPEDA) Privacy Principles are mentioned explicitly; this is for the benefit of readers that may be particularly interested in a Canadian perspective.

6.1 Payment Tracking

Perhaps the most obvious privacy risk that is common to many electronic payment models is payment tracking (i.e., the ability to track the movement of money in a payment transaction, which effectively leads to the loss of the choice / ability for a consumer to pay anonymously). It is well known that the credit card company knows when, and at which merchant, a person has used his/her credit card but, as mentioned above, in some payment models other parties learn much more detailed purchase information than that. With physical currency, a consumer always has the option to purchase goods or services "off the record", but the transition to electronic transactions (including virtually all forms of mobile payments) removes this possibility. Anonymous payments have certainly been envisioned from the earliest days in electronic cash schemes (see Chaum[106], for example), but the identifiers included in the MintChip Request and Value messages seem to preclude anonymity in the MintChip proposal.

One approach is to consider alternatives to anonymity within the existing legal framework. If the payment models and protocols do not technically enable anonymity, then it is all the more important to ensure that, to the extent payment information constitutes personal information, it is protected according to applicable privacy legislation, including PIPEDA (for merchants, payment brands, etc.) and the Privacy Act (for government reimbursements to citizens, for example). In this way, financial transactions are legally constrained in terms of who can discover them and what such entities can do with that information. This is clearly not identical to anonymity, but it puts some controls in place regarding the collection, use, disclosure, and retention of payment information, which is at least a step in the right direction. On the other hand, technical solutions can assist and enforce legal solutions, and so payment models that can allow true anonymity in financial transactions would be of significant interest.

6.2 Small Screens on Mobile Devices

A sometimes-overlooked privacy concern in mobile payment systems is the physical size of mobile devices. In particular, the small screen size on a smartphone or tablet, compared with a desktop or even a laptop computer, can make it very challenging to display privacy policies or other forms of user notice, thereby making it difficult to obtain meaningful consent from users (since they are unlikely to read through pages of text on a small screen).

PIPEDA Principles 4.8 (Openness: "An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.") and 4.3 (Consent: "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.") may be relevant to this concern.

[106] Chaum, D., A. Fiat, and M. Naor, "Untraceable Electronic Cash", in Advances in Cryptology: Proceedings of CRYPTO '88, S. Goldwasser (Ed.), Springer-Verlag, 1989, pp. 319-327.

6.3 Employees of the Payment Instrument Company

As mentioned in Section 5, in some mobile payment models the company offering the payment instrument or service learns much more consumer and/or merchant information than a credit card company learns in a traditional card and POS payment transaction. This leads to a potential privacy concern regarding unauthorized access or use of this information by company employees. Such employees may attempt to access or use this information in ways that could violate PIPEDA principles, particularly Principles 4.3 (Consent: "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.") and 4.5 (Limiting Use, Disclosure, and Retention: "Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law."). Unauthorized access or use may also highlight weaknesses in the organization's adoption of safeguards, as required by Principle 4.7 (Safeguards: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.").

Strict audit controls and other technological and procedural measures with respect to employee access to payment data may be required in order to mitigate this concern.

6.4 Natural or Man-Made Disaster

In this electronic age, societies are increasingly vulnerable and constrained (literally "powerless", in all senses of the word) when the power goes off: virtually all devices and appliances in the home, workplace, and public environment stop functioning. This, of course, includes all forms of electronic payment transactions.

Power outages can occur from many types of natural phenomena (earthquakes, violent storms, extreme sunspot activity, and so on), but can also occur as a result of man-made disasters (for example, nuclear explosions or other terrorist activities). Some of these natural and man-made events can not only cause outages, but also render memory systems (such as computer hard drives, USB memory sticks, etc.) permanently unreadable. What are the dangers in having no paper trail of financial transactions: no backup records, no bank account information, no purchase receipts, in fact nothing at all in a form that can survive a disabling of electronic memory? Commerce of any kind would be almost impossible. And yet, this is the risk society rushes toward as more and more financial transactions transition to the purely electronic domain.

An interesting mini-case-study of this situation occurred with the M-Pesa system near the end of 2012. According to Walubengo[107], a power outage on a Vodafone server in Germany damaged server disks which caused a collapse of Safaricom's M-Pesa money transfer services in Kenya for close to 24 hours from a Saturday night to Sunday evening. "Dates were cancelled, people went hungry, medication could not be bought, people quarreled, travel plans were cancelled, bookings could not be paid for, utilities were not paid on time, and the weekend could generally not be enjoyed." In addition, there were other tangible financial consequences: M-Pesa agents had to go the whole day without work and some of them who spoke to the media complained of huge losses owing to the outage. As noted in Walubengo[108], "If a few hours of the outage can cause huge losses, then a complete fail of the systems

[107] Walubengo, N., "The Mobile Money Apocalypse; What Would Happen to Your Money?", PesaTalk, November 2, 2012. See http://pesatalk.com/the-mobile-money-apocalypse-what-would-happen-to-your-money/ (last accessed April 17, 2013).

[108] Ibid.

will not only cause losses in revenue generated, but will render a good number of the 49,079 agents jobless."

Of perhaps more interest are the questions that this outage raised for money platforms and industry regulators generally. For example, Walubengo[109] (citing a 2008 presentation by Ananda and Kiptum[110]) states that the Banking Act [Sec. 2(1)] [this is the Kenyan banking law, although it is conceivable that it is similar in at least some other countries] defines "banking business" as the acceptance of money from the public on deposit or on current account AND the use of this money by lending, investment or any other manner for the account and at the risk of the person so employing the money. According to Walubengo, funds collected by Safaricom from M-Pesa account holders are held by M-Pesa Trust Company Limited in a pooled account, and the interest earned on this account apparently does not accrue to or benefit Safaricom Limited. Thus, Safaricom is not using M-Pesa deposits to earn or accrue any benefits, and so it exonerates itself from engaging in "banking business". Therefore, the laws that govern mainstream banking institutions in Kenya may not apply to Safaricom's mobile money operations, and so the risk to users may be quite different. It is unlikely that most Kenyan users will have understood this prior to the outage.

Essentially, the questions that arose with M-Pesa in Kenya[111] may also be relevant to other mobile payment models around the world and may therefore need to be considered in many jurisdictions:

- Who will compensate customers if a mobile platform collapses (the operator? the payment brand? the bank? the government?)?
- If there is a system in place to repay the millions of mobile money users, what mode will be used to repay them since the system they were using collapsed (recall that in Kenya a large percentage of the population does not have access to any bank)?
- How are the operators prepared for server security issues in order to safeguard subscribers' money?

Note that the consequences of natural or man-made disaster are not limited to security concerns. In particular, Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA[112]) includes Principles 4.7 (Safeguards: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.") and 4.9 (Individual Access: "Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information."), which pertain to the privacy concerns of personal information. It is worth considering whether an organization that fails to keep any non-electronic records might have difficulty meeting these requirements following an event that destroyed all electronic memory systems.

[109] Ibid.

[110] Ananda, F. and J. Kiptum, "Security Issues in M-Banking", presentation given at the Information Security and Cyber Forensics Conference, October 29-31, 2008. See http://www.strathmore.edu/pdf/m-pesa.pdf (last accessed June 12, 2013).

[111] Walubengo, N., "The Mobile Money Apocalypse; What Would Happen to Your Money?", PesaTalk, November 2, 2012. See http://pesatalk.com/the-mobile-money-apocalypse-what-would-happen-to-your-money/ (last accessed April 17, 2013).

[112] Personal Information Protection and Electronic Documents Act. The Act is available at http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html; some surrounding discussion is available at http://www.pipeda.info/a/1.html (each site last accessed June 12, 2013).

6.5 Lack of Security Implementation

Technological advancements in the world of mobile payments offer the potential for increased security for financial information (compared with traditional card and POS payment systems) in at least three specific ways[113].

- In a traditional payment system, financial data is often transmitted or stored in an unencrypted form at some point during the payment process. Mobile payment technology, on the other hand, allows for encryption throughout the entire payment chain (referred to as "end-to-end encryption"). Note that PCI compliance requires end-to-end security, but "end-to-end" (or "point-to-point") in the PCI standard refers to the path from the merchant POS terminal to the final destination of the payment transaction[114]. In the context of mobile payments, "end-to-end" begins with the consumer's mobile device, not with the merchant's terminal.
- In a traditional payment system, financial information on a card's magnetic stripe is transmitted in precisely the same form each time a consumer makes a payment. If this information is intercepted, it can be used repeatedly by malicious parties for subsequent unauthorized transactions. Mobile payments, however, can use dynamic data authentication, whereby a unique set of payment information is generated for each transaction. Thus, even if the data is intercepted, it cannot be used for a subsequent transaction.
- On a mobile device, payment information can be stored in the tamper-resistant Secure Element, which is separate from the rest of the device's memory. Thus, hackers who access the device (either physically or only through software) are prevented from accessing or compromising sensitive financial information.

Therefore, the technology to provide enhanced security in mobile payments is available but, according to the FTC Workshop Report[115] (pp. 11-12), it is not clear that all companies in the mobile payment market are employing it. If less responsible companies do not implement the secure technologies available to collect and store payment information, consumers (and the industry as a whole, if consumers come to believe that poor security practices are the norm) may be harmed. PIPEDA Principle 4.7 (Safeguards: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.") may be relevant to this concern.

[113] U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), "Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments", FTC Staff Report, March 2013, pp. 11-12. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed April 5, 2013).

[114] PCI Security Standards Council Emerging Technology Whitepaper, "Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance for Transmissions of Cardholder Data and Sensitive Authentication Data", Program Guide Version 1.0, October 5, 2010, p. 5. See https://www.pcisecuritystandards.org/pdfs/pci_ptp_encryption.pdf (last accessed May 1, 2013).

[115] U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), "Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments", FTC Staff Report, March 2013. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed April 5, 2013).

6.6 Buggy Implementations

Payment applications, like all other applications on a mobile device, are implemented in software. It is common knowledge in the software industry that most software programs are large and complex (even a program of a few lines of code can quickly swell to several kilobytes or even megabytes in length because of libraries and packages that get linked in, for example). Large and complex software programs are rarely “bug free”: unexpected inputs, uses, and situations can all cause a program to act in ways that were unanticipated by the original developer. Consequently, it is likely that at least some payment applications will be “buggy”; this creates a real risk that these bugs will be discovered and exploited by malicious entities.

This leads to the question of what happens when a payment application does the wrong thing. Due to bugs in the software, undetected transmission errors, or some other problem, a situation may arise in which two parties disagree about a payment transaction. When it is one person’s word against another, who is believed? How can the discrepancy be resolved? Who is the final arbiter? Ultimately, where does the final accountability lie? Naturally disputes can arise in hard currency transactions as well, but in those cases there is at least a tangible, physical object (the cash) that is transferred from one party to another: after the transaction, one party has $10 less than before and the other party has $10 more. In an electronic payment, one party might have a confirmation message on the screen saying that $10 has been paid, but the other party has a confirmation message on his/her screen saying that $1 has been received. Who do the parties complain to, and what can be done about it? Examination of any transaction logs that are kept may help but, depending on the amount of detail recorded, may not be sufficient to fully resolve the dispute.

A related problem has to do with “buggy implementations” not of software programs, but of human processes. What happens when human errors occur during a payment transaction? An example of this has been seen a number of times in the case of the M-Pesa payment system in Kenya[116]: a user makes an M-Pesa payment transfer, but accidentally sends it to the wrong account. There is a mechanism to halt the transfer (the user calls an M-Pesa Customer Care number), but this can only work if the recipient who accidentally received the transfer has not already cashed it or used it to make a purchase. If the accidental recipient has already retrieved the payment, then the unfortunate sender has lost the money. Buggy software programs can also be connected with this: after the human error of sending money to the wrong account, the sender calls M-Pesa to have the transfer reversed and is assured by the M-Pesa representative that the reversal has occurred, but the money does not show up in the sender’s account.

A more serious problem can occur if the recipient is a service provider, rather than a user, and the sender is malicious. Consider the situation in which a sender makes an M-Pesa transfer to a service provider, consumes the good or service, and then contacts the M-Pesa Customer Care number to have the payment reversed (claiming that the transfer was accidentally sent to the wrong account). Such a scheme can work because cases have been documented in which Safaricom accessed a provider’s account and initiated a reversal without notifying the provider (see Yawe[117], for example).

[116] Bankelele (a Nairobi writer on Banking, Finance, Technology, and Investments), “How to Get n M-Pesa Refund and other Safaricom tales”, June 29, 2009. See http://www.bankelele.co.ke/2009/06/how-to-get-m-pesa-refund.html (last accessed April 22, 2013).

[117] Yawe, R., “How secure is mpesa”, KICTAnet (Kenya ICT Action Network), July, 2011. See http://www.kictanet.or.ke/?p=713 (last accessed April 22, 2013).

For cases of buggy implementations, in addition to PIPEDA Principle 4.7 (Safeguards: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information"), Principle 4.6 (Accuracy: "Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.") may be relevant. It is worth considering whether the owner / operator of a payment application or service may contravene this Principle if buggy implementations lead to errors in payment transactions or payment amounts.

6.7 Dispute Resolution Inconsistency

Following on from the previous concern, if there is any kind of discrepancy in a payment transaction, some form of dispute resolution process needs to take place. Unfortunately, this process is handled inconsistently across different payment instruments. According to a recent FTC workshop on mobile payments in the U.S.[118] (pp. 5-7),

> One of the most significant concerns for users of mobile payments is how to resolve disputes in the case of fraudulent payments or unauthorized charges. Depending on the payment source used to fund the mobile payment (*e.g.*, credit card versus prepaid card versus mobile carrier billing), consumers may or may not have statutory protections regarding unauthorized charges. […]
>
> Mobile payment users may not recognize that their protections against fraudulent or unauthorized transactions can vary greatly depending on the underlying funding source. Generally, credit cards provide the strongest level of statutory protection, capping liability for unauthorized use at $50. If a mobile payment is linked to a bank debit card, a consumer's liability for unauthorized transfers is limited to $50 if reported within two business days, and up to $500 for charges reported after two business days. However, if consumers do not report unauthorized debit transactions on their bank account within 60 days after their periodic statement is mailed to them, they can face unlimited liability, whether or not the charges result from a lost or stolen card or another electronic transfer.
>
> Other types of funding mechanisms, however, do not have the same statutory protections as credit cards and debit cards. For example, there are no federal statutes besides the FTC Act that protect consumers from unauthorized charges if their mobile payment mechanism is linked to a pre-funded account or stored-value card such as a gift card or general purpose reloadable card, also known as a pre-paid debit card. […] Certainly, the inconsistency in protections complicates the landscape for consumers who may not understand the differences between these funding sources. […]
>
> Some companies have filled in gaps in the statutory protections by contractually promising consumers protections in the event that there is a dispute about a payment. [… However,] because the protections are voluntary, such protections are not consistent, and companies that provide them could withdraw or modify them at their discretion.

The FTC workshop report concludes its dispute resolution section by stating that consumers "should understand their rights and protections when choosing whether to pay using a mobile device, what mobile payment service to use, and what funding mechanism to use. To assist consumers in making these choices, companies should develop clear policies regarding fraudulent and unauthorized charges and clearly convey these policies to consumers." Such advice is clearly applicable to jurisdictions outside the U.S. as well, including Canada.

[118] U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), "Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments", FTC Staff Report, March 2013. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed April 5, 2013).

6.8 Proprietary Payment Protocols

A trend is beginning to emerge among some merchants, financial institutions, and payment brands to create proprietary payment models or wallet technology rather than adopting existing solutions[119]. Some of these players may see this as a way to offer features or a user experience that differs from other products and thus gives them a competitive advantage. This is not surprising, especially in those societies that value a free market economy.

However, payment transactions are among the most security sensitive transactions that can be performed on a mobile device and the complexities involved in "getting them right" can be non-trivial. Merchants, financial institutions, and payment brands may understand finance and commerce very well, and may even employ highly-skilled developers that can create useable and feature-rich mobile apps, but it is uncertain whether they will also employ enough people with sufficient security and privacy expertise to ensure that the mobile payment transactions are properly protected. Thus, it is unclear whether proprietary payment models or wallets will have the expert design, review, and analysis needed to minimize the risk to consumers.

Concerns with respect to proprietary offerings center around unintended security / privacy vulnerabilities in payment protocols: might there be ways to create / erase money; do opportunities for money laundering exist; can payments be replayed, blocked, ignored, or "disappeared"? In general, confidentiality, integrity, authenticity, and availability of payments may be at risk. (Consider, as one example, the vulnerabilities that led to the loss of millions of dollars in Bitcoin value in 2011[120].) PIPEDA Principles 4.7 (Safeguards: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information") and 4.6 (Accuracy: "Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.") may be relevant here since it is important to ensure that the personal information of users (i.e., their payment transactions) cannot be modified, deleted, or replayed in malicious ways.

In parallel with protection under PIPEDA, it may be worth examining whether a false or malicious payment constitutes identity theft and/or identity fraud under the *Criminal Code* (the malicious party pretends to be either the user or the merchant).

6.9 Confiscation of Money, Blocked Transactions

A concern with electronic payment (including mobile payment) systems is that, completely aside from payment tracking, some parties may have the ability to block transactions from taking place at all. It is easy to conceive of a scenario in which an individual or group of individuals is targeted as "undesirable": the authorities may choose to prevent such persons from making payments or receiving money ("Sorry, that transaction is not authorized…"), effectively constraining the movements and freedom of the target

[119] Bradley, M., "Digital Wallets Executive Briefing", Information Technology Association of Canada (ITAC) Digital Commerce Forum: How Your Wallet is Going Digital, April 16, 2013. See http://itac.ca/files/2013_april_16_digital_wallet_presentation.pdf (last accessed May 1, 2013).

[120] Mick, J., "Inside the Mega-Hack of Bitcoin: the Full Story", DailyTech, June 19, 2011. See http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm (last accessed May 3, 2013).

group. This is clearly possible: page 29 of the Canadian NFC Mobile Payments Reference Model[121] states that a credential issuer can block a payment application (i.e., restrict use at the device or the account level), rendering the application unavailable to make payments until approved steps are performed between the end user and the credential issuer to unblock the payment application. Note that authorities in a corrupt government could coerce a credential issuer to block a payment application for a particular user or group, but simple human error or negligence could also cause the same thing to happen to completely innocent people in any society.

On a related note, one wonders if it might be possible for an authority to "confiscate" an individual's digital cash (i.e., essentially mark their cash as "bad money" so that it cannot be spent anywhere). Again, this seems technically feasible and, again, one can also imagine errors causing this to happen to innocent people.

6.10 Theft of Device

Clearly, mobile devices such as tablets and smartphones are a desirable commodity and, consequently, are an attractive target for thieves (who wish to profit either from reselling the devices or from selling the information contained on the devices). It is worth considering whether there is an increased risk of theft if the device is able to make mobile payments, and particularly if the device holds some form of digital cash. If there is an increased risk (as seems likely), then there may be an associated increased risk of violence / harm to those carrying such devices.

Widespread use of protection measures (including passwords / PINs to unlock payment instruments, remote deletion of data on a lost or stolen device, and so on) thus takes on greater importance in a mobile payment world (i.e., not only for general security and privacy of payment transactions, but also for lowering the risk of device theft and therefore potentially increasing the physical safety of device owners).

6.11 Burdensome Notification Process after Loss or Theft

Related to the previous concern regarding device theft is a concern around the whole process of notification after loss or theft of a device. If a device is lost or stolen, who does the owner notify? If a single device might hold multiple credit cards, debit cards, membership discount cards, loyalty cards, and store coupons from many different issuers, how will the owner remember who to notify in order to block these various payment instruments? Aside from the mobile network operator, the owner might potentially need to contact each of these payment brands and financial institutions individually (and do it quickly before the finder / thief is able to use any of them in a payment transaction). This may be a significant burden to place on an ordinary user.

One suggestion, of course, is to encourage users to lock the wallet and payment applications with passwords / PINs so that a thief does not immediately gain access to these apps. However, there is no way to force users to use PINs at all (this is currently an optional feature). If PINs are used, there is no way to force users to use different PINs for different payment applications and no way to guarantee that

[121] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed February 14, 2013).

any PINs used will be sufficiently strong. But the situation is even worse than this: a German research team has found that, at least for some devices (the experiments were done on a Samsung Galaxy Nexus Android phone), cooling the device to below -10 degrees Celsius and then connecting and disconnecting the battery put the phone into a vulnerable mode[122]. Once the phone was in this mode, they could start it with some custom-built software rather than with the onboard Android system and subsequently find cryptographic keys to decrypt data, and copy data to a separate computer for analysis. Thus, the payment data on a stolen device (i.e., any data not stored in the SE) may be at risk even if that data has been encrypted and/or PIN-protected. Note that this is one recent attack, but over time more attacks are likely to be developed.

PIPEDA Principle 4.7 (Safeguards: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.") may be relevant to this situation. In particular, it is worth considering whether device or OS manufacturers might contravene this principle if freezing the phone, or any other form of attack, can render the personal information vulnerable (i.e., if the manufacturers have not put adequate safeguards in place to protect against such attacks). In addition, manufacturers might find themselves in contravention of this Principle if they become aware of such vulnerabilities and fail to communicate them to users and address them.

6.12 Uncertainties Regarding "Remote Wipe"

Some mobile device OS manufacturers have embraced "remote wipe / remote delete" as a way of offering their customers peace-of-mind: if the device is ever lost or stolen, the customer can remotely send a command to delete the data on the device, rendering the device much less attractive to the finder or thief. This is a compelling idea, especially in the case of mobile payments where sensitive financial information (such as credit card numbers and expiry dates, coupons, loyalty cards, and even digital cash) may be vulnerable to access and use by a malicious party that acquires the lost or stolen phone.

The concept of remote wiping does raise at least two concerns, however. First (and perhaps most important), does this technology really work? In the early days of computing, experts would suggest deleting sensitive data from a hard drive prior to disposing of a computer, but it was quickly discovered that normal file deletion does not delete the file at all (it simply deletes the pointer to the file, thereby marking the file as "available disk space" that can be used for other storage). This led to the creation of "secure delete", in which the selected file was overwritten multiple times with completely random data prior to deletion of the file pointer, so that the data was truly unrecoverable even by a high level of forensic analysis. The concern is that we may still be in the early days of file deletion on mobile platforms (i.e., that, on some platforms at least, remote delete may not truly delete anything). Preliminary investigations at University of Ottawa suggest that this may be the case (see Appendix). Alternatively, remote wiping can easily be defeated if the new possessor of the device is fast enough to shield it in some way (e.g., putting it in a metal box) before the owner discovers that it is missing. The shielded environment would block the remote wiping signal from reaching the device. In either case, there are clearly both security and privacy implications if financial data is still recoverable from the device when the owner believes it has been deleted.

[122] BBC News Technology, "Frozen Android phones give up data secrets", March 7, 2013. See http://www.bbc.co.uk/news/technology-21697704 (last accessed April 19, 2013).

Second, there may be some concern even if remote wiping works perfectly well. In particular, is it the case that wiping will destroy any digital cash that may reside on the device? If so, is that money then gone forever? If so, does the owner have any recourse (for example, could this loss be covered by insurance, especially for substantial sums?)? If there is the possibility of recourse (e.g., insurance), how can the owner prove how much money was on the device? It seems more likely that the digital money will simply be lost (analogous to losing one's physical wallet: the cash is unrecoverable regardless of whether the wallet contained $10 or $1000). Given the number of mobile phones that are lost or stolen every day[123], one wonders whether consumers will be either reluctant to put large sums of digital cash on their phones, or reluctant to use remote wipe at all (in hopes that they will soon find their phone again behind the sofa cushions). A related concern arises if the phone is dual-purpose (i.e., business and personal use): it is possible that a remote wipe executed by the business will destroy personal information (including digital cash), so again there may be motivation to not put large sums on the device.

Relevant PIPEDA Principles (whether remote wiping does not work, or whether it works and destroys all stored digital money, coupons, loyalty cards, etc.) may include 4.1 (Accountability: "An organization is responsible for personal information under its control.") and 4.7 (Safeguards: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."). Any entity offering a remote wipe service is implicitly in control of the information on the device (at least in control of its existence) and so must be accountable if the user believes the information has been destroyed when, in fact, it is recoverable.

6.13 Increasing Hacker Attention on Mobile Devices

In the past few years, mobile devices have received increasing attention from hackers, malware writers, and other malicious parties, and it seems likely that this trend will continue. As more mobile devices include payment instruments of many different kinds, including digital cash, these devices become an even more attractive target. One can expect that the security and privacy risks surrounding mobile devices in general, and mobile payments in particular, will only increase in variety, breadth, and complexity over time.

7. Conclusion

This second part of the mobile payments report provides an analysis of some specific mobile payment models. Detailed discussion is given with respect to the NFC-enabled mPOS payment model, and other models, including mP2P (M-Pesa and MintChip as examples) and mAccept (Square as an example), are also included. A general discussion of security and privacy concerns that pertain to most/all electronic payment models is provided as well. For the sake of completeness, this part begins with a look at the transition phase toward true mobile payments which is seeing significant use in many societies (online banking/shopping and mobile carrier payments).

[123] Knight, S., "Americans lost $30 billion worth of mobile phones in 2011", TechSpot, March 23, 2012. See http://www.techspot.com/news/47930-americans-lost-30-billion-worth-of-mobile-phones-in-2011.html (last accessed April 23, 2013).

In general, there are many security and privacy concerns, ranging from very minor (such as message modification over the NFC wireless channel) to more significant (including skimming attacks on NFC-enabled devices, malware – including a malicious wallet – on the mobile device, potential impersonation attacks in Square, lack of anonymity in payment transactions, burdensome notification process after loss or theft, uncertainties regarding remote wipe, and a number of others). The discussion has attempted to describe these as clearly as possible (in both technical and non-technical terms) and to explain what the corresponding risks are. The third and final part of this report will provide some recommendations that derive from the analysis given in this second part.

Have Money, Will Travel:
A Brief Survey of the Mobile Payments Landscape

Part 3 – Recommendations

Abstract

This third of 3 parts provides recommendations for security and privacy protection that arise from the analysis in Part 2 of various mobile payment models. Some of the recommendations are divided into categories that target specific audiences, including mobile device manufacturers, payment instrument companies, standards bodies, and end users.

The recommendations presented are those of the author and are intended to contribute to the privacy and security research of the Office of the Privacy Commissioner of Canada and other interested parties; as such, they should be viewed as input for consideration as the OPC and others formulate their own policies and guidelines in the area of mobile payments.

1. Introduction

This report on mobile payments is divided into three pieces: Context; Analysis; and Recommendations. This third piece, *Part 3 – Recommendations*, looks at how the security and privacy risks of various payment models discussed in Part 2 can be minimized.

The remainder of Part 3 is structured as follows. Section 2 looks at some recommendations from other sources that are applicable to mobile devices and mobile payments. Section 3 begins the collection of recommendations that arise from the analysis of Part 2, looking at recommendations that pertain to specific payment models. Section 4 continues the set of recommendations that arise from Part 2, looking at those that are relevant generally to all electronic payment models. This latter group of recommendations is categorized according to specific audiences: device and OS manufacturers, mobile network operators, wallet/app developers, standards bodies, merchants, and end users. Finally, Section 5 provides some concluding comments.

2. Relevant Recommendations from Other Sources

A number of different groups have put together recommendations regarding security and privacy in mobile environments. Some of these are specific to mobile payments and others are directed toward good practices for mobile devices generally. In no particular order, several examples are given in the following subsections.

2.1 FTC

The U.S. Federal Trade Commission (FTC) convened a workshop on Mobile Payments in April, 2012, “to learn more about the mobile payments industry and its effects on consumers”. Pages 11-13 of the subsequent report[124] discuss consumer data security in mobile payments and include recommendations such as using password protection to unlock the device, using a second password for payment apps, and contacting the mobile carrier immediately if the device is stolen in order to have the device and all payment apps disabled. Pages 13-15 discuss privacy and recommend that companies in the mobile payments marketplace adopt (1) privacy-by-design, including considering privacy at every stage of product development and limiting data collection to that which is consistent with the context of a consumer's interaction with that company, (2) simplified choice for businesses and consumers, especially regarding disclosure of information that is not necessary for completing a payment transaction, and (3) greater transparency regarding data practices.

2.2 LAP and M^{3}AAWG

Members of the International Cybersecurity Enforcement Network known as London Action Plan (LAP) joined with members of the Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) to produce a report entitled "Best Practices to Address Online and Mobile Threats", dated October 15, 2012[125]. This report is not specific to mobile payments, but contains recommendations and best practices that are useful for countering a range of concerns, including malware and botnets, phishing and social engineering, Internet Protocol (IP) and Domain Name System (DNS) exploits, and mobile threats. The mobile threats discussed include an attacker setting up a rogue base station and an illicit wireless network, fraud via premium rate scams (i.e., premium rate services billed to a subscriber's account without consent), mobile spam, security (or insecurity) of app stores, mobile malware, and the modification of mobile devices (jailbreaking, rooting, and unlocking).

2.3 OPC

The Office of the Privacy Commissioner of Canada (OPC) has issued several guidelines and recommendations in the area of mobile devices and online privacy. In particular, the main OPC website (http://www.priv.gc.ca/) includes, among others, the following resources.

- "Privacy on the Go: 10 Tips for Individuals on Protecting Personal Information on Mobile Devices" (http://www.priv.gc.ca/resource/fs-fi/02_05_d_47_dpd_e.asp), January 2011.
- "The Transformation of the Canadian Payments System: Why Privacy is Essential for Trust and Innovation in the Payments System" (http://www.priv.gc.ca/information/research-recherche/sub/sub_psr_1109_e.asp), September 2011.
- OPC Guidance Documents: "Identity Theft and You" (http://www.priv.gc.ca/information/pub/guide_idt_e.asp), March 2009.
- "Recognizing Threats to Personal Data: Four Ways That Personal Information Gets Hijacked Online" (http://www.priv.gc.ca/resource/fs-fi/id/phishing_e.asp), March 2007.

[124] U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), "Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments", FTC Staff Report, March 2013. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed May 17, 2013).

[125] London Action Plan (LAP) and Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG), "Best Practices to Address Online and Mobile Threats", October 15, 2012. See http://www.maawg.org/sites/maawg/files/news/M3AAWG_LAP_Best_Practices_to_Address_Online_and_Mobile_Threats_0.pdf (last accessed May 17, 2013).

- “Protecting your Privacy Online: Frequently Asked Questions” (http://www.priv.gc.ca/resource/fs-fi/02_05_d_13_rev_01_e.asp), last modified May, 2011.
- OPC Guidance Documents: “Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps” (http://www.priv.gc.ca/information/pub/gd_app_201210_e.asp), October 2012.
- “Securing Personal Information: A Self-Assessment Tool for Organizations” (http://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1) March, 2011.

Specific OPC recommendations in the area of mobile devices include getting familiar with the device’s privacy and security settings, removing unnecessary personal information stored on the device, using a strong password, locking the device when it is not in use, installing security (antivirus, antispyware, firewall, and encryption) software on the device, setting Wi-Fi and Bluetooth to “off” by default, preparing a plan in the case of device loss or theft, using a privacy screen on the device, always installing the latest security patches, and limiting the number of people that have access to the mobile number.

2.4 PCI

The Payment Card Industry (PCI) has issued a document[126] whose purpose is “to provide guidance to merchants on how to implement a secure mobile payment-acceptance solution”. Sections 4, 5, and 6 (“Objectives and Guidance for the Security of a Payment Transaction”, “Guidance for Securing the Mobile Device”, and “Guidance for Securing the Payment-Acceptance Solution”) form the substantive content of the report (see also Appendix B: “Best Practices and Responsibilities”) and include guidelines such as preventing unauthorized physical device access, protecting the device from malware, ensuring the device is in a secure state, disabling unnecessary device functions, inspecting system logs and reports, securely wiping data on the device, and ensuring the secure disposal of the device.

Note, however, that this report focuses on the mobile device at the merchant end of the payment transaction (i.e., as a POS terminal, a payment acceptance device). It does not specifically propose any guidelines regarding the mobile device at the consumer (payer) end of the transaction, although many of the guidelines discussed would also be applicable to the user device.

3. Recommendations Arising from this Report (Specific Mobile Payment Models)

Part 2 of this report looked at a few mobile payment models and, in particular, at some specific mobile payment technologies. The following subsections discuss the recommendations that come out of that analysis.

3.1 Online Banking / Shopping using a Mobile Browser

As noted in Part 2 (Section 2.1), mobile browser vulnerabilities can lead to loss or misuse of data, as well as to the possibility of malicious software being downloaded to the device. Consequently, the usual recommendations

[126] Payment Card Industry (PCI) Security Standards Council, Emerging Technologies, “PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users”, Version 1.0, February 2013. See https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf (last accessed May 17, 2013).

- to stay current with browser and OS security patches and updates,
- to download software only from trusted sources, and
- to use a device that has not been jail broken / rooted

are relevant to this payment model.

3.2 Mobile Carrier Billing

The mobile carrier billing payment model raises two primary concerns: the possibility that the carrier may misuse the additional information that it learns about its customers (i.e., detailed purchase history and merchants involved); and the increased possibility of phone bill cramming (unauthorized charges, perhaps under ambiguous or misleading headings such as “service charge” or “other fees”). Recommendations that arise from this model, then, include the following (the first three are taken from the FTC Workshop Report[127], pp. 8-9):

- mobile carriers should give customers the ability to block all 3rd-party charges on their mobile accounts (i.e., customers should be able to choose not to allow/use any 3rd-party services);
- a clear and consistent process should be established for consumers to dispute suspicious charges and obtain reimbursement;
- carriers should standardize and prominently highlight billing descriptions of 3rd-party charges;
- customers should carefully monitor their bills each month, particularly looking for any suspicious or poorly-explained charges;
- carriers should be vigilant in protecting the security and privacy of all additional personal information that they learn about their customers through the mobile carrier billing payment model.

3.3 NFC-Enabled mPOS

Mobile devices that can make payments through the use of Near-Field Communications (NFC) with contactless Point-of-Sale terminals raise a number of security and privacy concerns that have been discussed in Part 2 (Section 3) of this report. These concerns lead to the following recommendations.

- To avoid skimming attacks (in which an actual payment transaction is made without the knowledge or consent of the device owner, or in which a credit card number and expiry date are surreptitiously read from the device), the NFC capability should be disabled when the screen is off and all payment transactions (not just high-value ones) should require a confirmation from the user. Instructions from an NFC tag should also require user approval before they are executed on the device.
- To avoid corrupted channel attacks (such as eavesdropping and relay), users should be vigilant in observing anyone who is physically close to them as they conduct their transactions (e.g., users should be suspicious of a lurker with a huge antenna!). Furthermore, all payment transactions should require user confirmation to reduce the threat that a malicious party at a distance is using a relay attack to make a legitimate user pay for the malicious party’s purchases.

[127] U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), “Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments”, FTC Staff Report, March 2013. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed May 17, 2013).

- Through Standards Statements that must be complied with, the Canadian NFC Mobile Payments Reference Model[128] ensures (p. 2, 3rd paragraph, and pp. 30-31, S15-S17) that the consumer has the ultimate say over whether their payments have pass code protection and which payment types are enabled on their mobile device. Since there is no guarantee that the average consumer will do a good job with this, wallet apps should set default values that take security and privacy into consideration (e.g., pass codes are requested for all payment apps by default).
- The Reference Model (p. 26) says, "A default credential allows an end user to initiate a payment without having to take the mobile device out of standby and without having to manually select a wallet." Given the security risks in enabling such a default credential (i.e., unintended transactions with malicious readers), users should be fully informed of the implications and potential consequences of setting up a default credential on their device.
- The Reference Model (p. 41) suggests that if an electronic receipt is issued, it should include not just the credit/debit card number (truncated to the last 4 digits) for tracking purposes, but also the mobile number (truncated) for tracking purposes. Given that it will likely be much easier for a malicious party who acquires a user's receipt to derive the mobile number from its truncated value than the card number from its truncated value (since the mobile number may have fewer digits and several of these may be easy to guess), the truncated mobile number should not be included on the receipt.
- The Reference Model (p. 45) describes "single-tap reimbursements": no signature, pass code, or PIN is required from the user in order to process a return. This may lead to a risk to merchants (e.g., a malicious party uses a stolen receipt to obtain a reimbursement for a stolen item) and so consideration should be given as to what appropriate level of user authentication should be required for returns, particularly looking at practices that are not privacy invasive.
- The Reference Model (p. 63, Section 10.6.1) states that even if mobile service is disconnected, the payment application may continue to work for NFC payments. Such a feature may not be intuitive to users (who might naturally think that if they have no mobile service they would be unable to use the phone to make payments), which may lead to situations in which payment transactions occur when the user is not expecting them. Thus, either this feature should not be offered, or carriers should ensure that users are fully aware of this capability.
- Payment and loyalty data stored in the wallet (i.e., not in the SE) should be encrypted by the providers of that data to minimize risk of misuse by any malicious software on the device.
- Users should make their best effort to only download and install trusted wallet apps (e.g., a wallet app from a known and trusted provider), since a malicious wallet can learn payment data that is not encrypted (such as credit card number and card verification value (CVV)) and misuse it in some way.
- Users should not root or jailbreak their mobile devices because this renders the devices more vulnerable to malicious software.
- Payment apps in the SE should always encrypt payment transaction data that is transmitted to a POS terminal (this reduces the risks arising from corrupted readers and from eavesdroppers on the NFC channel; see, for example, Section 4.2 of a white paper by Kremer[129]).

[128] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed May 23, 2013).

[129] Kremer, J., "NFC: Near Field Communication White Paper", Jan Kremer Consulting Services. See http://jkremer.com/White%20Papers/Near%20Field%20Communication%20White%20Paper%20JKCS.pdf (last accessed May 23, 2013).

- As stated in the Reference Model (p. 91), each ecosystem participant should put processes in place to track, monitor, and mitigate fraud and security concerns including malware, hacking, and theft of mobile devices.
- As stated in a CNN Money article[130], "Devices should at least ask permission before accepting data from unfamiliar devices or NFC tags that just happen to be nearby." While it is true that users may not always be able to properly assess the potential risk from unfamiliar devices or tags, it is still the case that having the user grant permission seems preferable to the device simply accepting data from anywhere without any assessment from the user.

Finally, a white paper by GSMA[131] presents a discussion of the motivation for, and benefits of, using NFC technology in the retail sector. Sections 8 and 9 of that document ("Defining Roles and Responsibilities" and "What to Consider") focus on how to move mobile NFC in retail forward and present a significant number of recommendations for various parties in the retail ecosystem. (Specific items discussed include "Educate consumers on how to use mobile NFC", "Develop a robust and secure framework for the management of customer data", "Identify what needs to reside in the secure domain and what doesn't", "Use standardized solutions to ensure interoperability and economies of scale", and "Ensure an NFC phone with a flat battery can still interact with an NFC terminal", among many others.) These sections are worth reading to supplement the above bullet points with respect to recommendations pertaining to the NFC-enabled mPOS payment model.

3.4 mP2P

The analysis of Part 2, Section 4.1, leads to the following recommendations for payment technologies in the mAccept model.

- If, between two entities, there is shared secret information that authenticates a transaction authorization message, it should not be (or at least should be more than) something that can be easily obtained by a malicious party[132]. A better solution may be to use cryptography (e.g., digitally sign the transaction authorization message at the payment company's server and have the agent software verify the signature of incoming authorization messages).
- Rigorous authentication should be performed when a user attempts to sign up for, or make changes to, his/her account (e.g., register a new SIM card with an existing (old SIM card) number). This would make it more difficult for a malicious party to obtain money sent to another user.
- Careful attention should be paid to any ways in which security mechanisms (such as audits) may be misused to harm the payment system, and to any areas in which vulnerabilities may arise due to the presence of malicious human actors somewhere in the payment transaction.

[130] Cowley, S., "NFC exploit: Be very, very careful what your smartphone gets near", CNNMoney, July 26, 2012. See http://money.cnn.com/2012/07/26/technology/nfc-hack/index.htm (last accessed May 23, 2013).

[131] Groupe Speciale Mobile Association (GSMA), "Mobile NFC in Retail", White Paper, Version 1.0, September 2012. See http://www.gsma.com/mobilenfc/wp-content/uploads/2012/10/Mobile-NFC-in-Retail-White-Paper-Oct-2012.pdf (last accessed May 23, 2013).

[132] For example, in Part 2, Section 4.1, the current account balance is used as shared secret information. The account balance is stored – probably securely – on the payment company's server, but is also stored in a place known to everyone: the agent's account book. Anyone who is able to access this book (either by posing as an auditor, or by surreptitiously looking at the book while the agent is distracted with other things) will be able to create a fake transaction authorization message that is accepted as legitimate by the agent.

Furthermore, for jurisdictions in which the payment app provider may appear to be conducting “banking business” but according to a strict legal interpretation is not, customers should be made fully aware of any risks or liabilities that they may face if their transactions or account balances experience unexpected losses.

3.5 Electronic Cash Systems

Electronic cash systems can raise some security and privacy concerns, as exemplified in Part 2 (Section 4.2). These concerns lead to the following recommendations.

- All messages should be (cryptographically) protected in some way, perhaps through a digital signature by the sender of the message. This would ensure that a request message cannot be modified in transit (to the detriment of the payer) and a response message cannot be modified in transit (to the detriment of the payee).
- The amount field in request and response messages should have a size that is appropriate for its intended use (e.g., micropayments). Leaving some additional room for future growth is fine, but a size that is too large opens the door to potential abuse (particularly if messages are unprotected, as noted in the previous bullet).
- In order to more closely approximate hard currency, electronic cash systems should incorporate an option make a truly anonymous payment. For some proposals it is not obvious how to do this (since messages are digitally signed and the participants need trusted public keys with which to verify that the signatures are valid), but some design alternatives should be explored in this area.
- All cryptographic algorithms used in the transaction protocols should be periodically reviewed to ensure that best practices are always being followed (e.g., transitioning from (the deprecated) SHA-1 to SHA-3).

3.6 mAccept

The analysis of Part 2, Section 5, leads to the following recommendations for payment technologies in the mAccept model.

- For some proposed technologies, on the merchant side a significant amount of sensitive business data is stored on the servers of the payment service provider (potentially including bank account settings, deposit schedule, in-depth business analytics, employee permissions, transaction history, and staff management data). Thus, the recommendation is for payment service companies to be vigilant in protecting the security and privacy of all information that they learn about their customers (i.e., merchants and, indirectly, the merchants’ customers).
- On the payer (customer) side, it is recommended that additional precautions be taken to mitigate the threat of impersonation attacks. Specifically, this means ensuring that the person at the register is actually the one making the payment (and not one of the other “available payers” that happen to be nearby). This may mean requiring all app users to upload a photo when registering for the payment service, but of course this has its own privacy concerns and is therefore not recommended. Alternative technical mechanisms to do this authentication should be explored. On a related note, despite the convenience, users are not recommended to leave their payment app enabled indefinitely (so as to reduce the possibility of unintentionally paying for a malicious party’s purchases). Rather, users should enable the app only when they are actually ready to make a payment; they should then make the payment and immediately close the app again.

4. Recommendations Arising from this Report (All Electronic Payment Models)

Along with specific mobile payment technologies, Part 2 of this report also examined some security and privacy concerns that are generally applicable to all / many electronic payment models. The following subsections discuss the recommendations that come out of that part of the analysis, categorizing them by target audience (in particular, device/OS manufacturers, mobile network operators, wallet/app developers, standards bodies, merchants, and end users).

Note: There is some repetition of text across the subsections in this section, but that is a result of the expectation that a given member of a target audience is likely to only read the subsection that particularly pertains to him/her.

4.1 For the Device / OS Manufacturer

The recommendations in this subsection are targeted primarily at the manufacturers of mobile devices and the manufacturers of the operating systems (OSs) that run on them (these are sometimes, but not always, the same entity).

4.1.1 Small Screens

Even the largest mobile phones and tablets have screens that are much smaller than the monitors that are typically used with desktop computers. As noted in Part 2, small screens can make it difficult to obtain meaningful consent from users, who are unlikely to read carefully through a lengthy privacy policy on a mobile device, for example. Manufacturers are encouraged to explore ways in which this problem can be solved including, perhaps, alternative methods for usefully conveying information to a user (such as layered policies and “just-in-time” policies).

4.1.2 Buggy Implementations

As mentioned in Part 2, large complex software systems (such as OSs) have a high probability of containing bugs. The same is true of large complex hardware systems (such as integrated circuits). Manufacturers are encouraged to continue, and even extend, their rigorous design and testing procedures to ensure that the systems they deliver are as bug-free as possible. Certification by an external body (such as a Common Criteria Evaluation Lab; see the CSEC site[133] for a list of certified products in Canada) can be a very useful component of this process.

4.1.3 Loss or Theft of Device

Mobile devices are often subject to loss or theft; at such times, data stored on the device is vulnerable and may be compromised. Manufacturers are encouraged to continue and increase their efforts to provide useful protection mechanisms for these situations, such as remote locking of the device, remote encryption of data, and remote wiping of data.

[133] Common Criteria Certified Products, available at http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html (last accessed June 12, 2013).

4.1.4 Failure of Protection Mechanisms

As illustrated by the "frozen phone" attack described in Part 2, Section 6.11, protection mechanisms such as encryption of data can fail in unexpected ways. Manufacturers are encouraged to continue, and to extend, their rigorous testing of data protection mechanisms, especially when the device is subjected to unusual or extreme operating conditions.

4.1.5 Remote Wipe

As noted in Part 2, Section 6.12 and the Appendix, there are uncertainties regarding the effectiveness of the remote wipe operation in rendering data unrecoverable. Manufacturers are encouraged to explore this area carefully to see if techniques can be found that will securely wipe data without unnecessarily wearing down the flash memory.

4.1.6 Increasing Hacker Attention

Part 2, Section 6.13, notes that mobile devices have received increasing attention from hackers, malware writers, and other malicious parties in the past few years, and that this trend is likely to continue. Manufacturers are encouraged to continue their extensive efforts to eradicate security and privacy vulnerabilities from their OSs and device hardware, and to contribute actively to keeping devices malware free by creating and disseminating patches, improved versions, and so on, in as timely a fashion as possible.

4.2 For the MNO

The recommendations in this subsection are targeted primarily at the mobile network operators.

4.2.1 Loss or Theft of Device

If a mobile device is lost or stolen, the user will typically notify the MNO (as well as other entities). MNOs are encouraged to continue their efforts to make the transition process for users as streamlined and as painless as possible. This may include assisting the user to lock the device, encrypt or wipe data, determine the physical location of the device, and list the device in a national registry[134], among other things. The Canadian NFC Mobile Payments Reference Model[135], Section 10.5.4 (pp. 59-61), includes a high-level flowchart outlining the main tasks of the MNO after being informed by the user of the loss or theft of a device.

[134] Lewis, M., "Registry targets smartphone black market", The Toronto Star: Business, November 8, 2012. See http://www.thestar.com/business/2012/11/08/registry_targets_smartphone_black_market.html (last accessed June 12, 2013).

[135] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed May 23, 2013).

4.2.2 Remote Wipe

As noted in Part 2, Section 6.12 and the Appendix, there are uncertainties regarding the effectiveness of the remote wipe operation in rendering data unrecoverable. MNOs are encouraged to explore this area carefully to see if techniques can be found that will enable them to ensure that data has actually been securely wiped when requested.

4.2.3 Increasing Hacker Attention

Part 2, Section 6.13, notes that mobile devices have received increasing attention from hackers, malware writers, and other malicious parties in the past few years, and that this trend is likely to continue. MNOs are encouraged to continue their efforts to keep devices malware free by disseminating patches, antivirus tools, and so on, to their customers in as timely a fashion as possible and to assist users to install these protective measures as soon as they are available.

4.3 For the Wallet / App Developer

The recommendations in this subsection are targeted primarily at the wallet and payment app developers and providers.

4.3.1 Payment Tracking

Part 2, Section 6.1, discusses tracking in electronic payment systems, and the inability for a user to make or receive an anonymous payment. Although tracking is useful for audit, taxation, and other purposes, today's electronic payment systems do not appear to provide a mechanism for anonymous transactions (as the physical currency, which it is replacing, does). Wallet and app developers are encouraged to explore ways in which truly anonymous payment transactions can be offered as an additional feature to existing payment models.

4.3.2 Small Screens

As discussed in Section 4.1.1, small screens can make it difficult to obtain meaningful consent from users, who are unlikely to read carefully through a lengthy privacy policy on a mobile device, for example. Wallet and payment app developers are encouraged to explore ways in which this problem can be solved including, perhaps, alternative methods for usefully conveying information to a user.

4.3.3 Malicious employees

Section 6.3 of Part 2 discusses the situation in which a company offering a payment instrument or service learns much more consumer and/or merchant information than a credit card company learns in a traditional card-and-POS payment transaction. If any employees of such a company are malicious, this leads to a concern that this information could be accessed or used in ways that violate privacy principles. Wallet and payment app developers and providers are encouraged to implement strict audit controls and other technological and procedural measures with respect to employee access to payment and other sensitive data.

4.3.4 Natural or Man-made Disasters

Section 6.4 of Part 2 discusses the potential consequences of natural or man-made disasters, particularly those that render memory systems permanently unreadable. Wallet and payment app developers are encouraged to store critically important records (such as account balances) in a recoverable form, at least periodically, in order to allow some possibility of business continuity in the event of such a disaster. The individual policies of the wallet and app developers may specify where such records would be stored, the form in which they would be stored, for how long they would be kept, and who would have access to them.

4.3.5 Lack of Security Implementation

As mentioned in Part 2, Section 6.5, the technology to provide enhanced security in mobile payments is available but, for a variety of reasons, some companies in the mobile payment market do not make use of it. Wallet and app developers are encouraged to employ all security mechanisms at their disposal to ensure that payment and other sensitive data is properly protected at all times.

4.3.6 Proprietary Payment Protocols

As noted in Part 2, Section 6.8, some merchants, financial institutions, and payment brands consider creating proprietary payment models or wallet technology rather than adopting existing solutions, perhaps as a way to offer features or a user experience that appears to give them a competitive advantage. It is well known, however, that payment transactions are highly security- and privacy-sensitive, and can be quite difficult to “get right”. Wallet and payment app developers are encouraged to adopt standardized or well-scrutinized solutions wherever possible and to ensure that any proprietary aspects are designed, reviewed, and analyzed by security and privacy experts prior to customer roll-out in order to minimize risks.

4.3.7 Dispute Resolution

Part 2, Section 6.7, discusses the inconsistency of dispute resolution practices across different payment instruments and across different merchants. In accordance with the position of the FTC Workshop on Mobile Payments[136], pp. 5-7, wallet and payment app developers are encouraged to develop clear policies regarding fraudulent and unauthorized charges and clearly convey these policies to consumers.

4.3.8 Confiscation of Money, Blocked Transactions

Part 2, Section 6.9, discusses the possibility that, at the request of an authority or by accident, electronic money and payment transactions can blocked, confiscated, or otherwise marked as “unacceptable”. Wallet and payment app developers and providers are encouraged to make their policies in this area clear to end users, and are also encouraged to make every effort to ensure that such situations do not occur as a result of error or negligence on the part of any of the entities involved.

[136] U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), “Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments”, FTC Staff Report, March 2013. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed May 17, 2013).

4.3.9 Loss or Theft of Device

If a mobile device is lost or stolen, the user will typically need to notify the payment app providers (as well as other entities). Developers and providers are encouraged to continue their efforts to make the transition process for users as streamlined and as painless as possible. This may include ensuring that the payment apps can be easily remotely locked and/or that the app data can be remotely wiped. Knowing who to notify can be a burdensome process for the user because the mobile device may contain many more payment instruments and much more payment data than a physical wallet. Providers are encouraged to seek ways to make the notification process easier for users, perhaps including periodically sending emergency contact information to the user's physical address.

4.3.10 Increasing Hacker Attention

Part 2, Section 6.13, notes that mobile devices have received increasing attention from hackers, malware writers, and other malicious parties in the past few years, and that this trend is likely to continue. Developers are encouraged to continue their efforts to keep the wallet and apps on any mobile device as free from security and privacy vulnerabilities as possible.

4.4 For the Standards Bodies

The recommendations in this subsection are targeted primarily at those who create the standard protocols / interfaces for operation and communication in mobile payment transactions.

4.4.1 Default Credentials

The Canadian NFC Mobile Payments Reference Model[137], p. 26, states that "A default credential allows end users to initiate a payment without having to take the mobile device out of standby mode and without having to manually select a wallet." Such a feature can potentially increase the risk of skimming attacks, in which the malicious party uses a reader to surreptitiously acquire credit/debit card information or conduct a payment transaction without the knowledge of the user. Standards bodies (particularly the editors of the next version of the Reference Model, if appropriate) are encouraged to either reconsider the inclusion of this feature, or make it a mandatory requirement that user consent is obtained before a transaction undertaken with a device in standby mode can be completed.

4.4.2 Disabled Mobile Service

The Reference Model[138], p. 63, Section 10.6.1, states that "Even if [mobile] service is disconnected, the payment application may continue to work for NFC payments." Such a feature can potentially increase the risk of attacks in which a payment transaction is conducted without the knowledge of the user. Standards bodies (particularly the editors of the next version of the Reference Model, if appropriate) are encouraged to either reconsider the inclusion of this feature, or ensure that user consent is obtained

[137] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed May 23, 2013).

[138] Ibid.

before a transaction undertaken with a device that is disconnected from mobile service can be completed.

4.5 For the Merchant

The recommendations in this subsection are targeted primarily at merchants.

4.5.1 Natural or Man-made Disasters

Section 6.4 of Part 2 discusses the potential consequences of natural or man-made disasters, particularly those that render memory systems permanently unreadable. Merchants are encouraged to store critically important records in a recoverable form, at least periodically, in order to allow some possibility of business continuity in the event of such a disaster. The individual policies of the merchants may specify where such records would be stored, the form in which they would be stored, for how long they would be kept, and who would have access to them.

4.5.2 Buggy Implementation of Human Processes

The risk of buggy implementations of human processes is discussed in Part 2, Section 6.6. Such flaws can lead to disputes or to losses for both merchants and customers. Merchants are encouraged to have clear, succinct, plain-language policies in place to handle these situations; they are also encouraged to ensure that these policies are conveyed to their customers as appropriate (e.g., sent as periodic reminders).

4.5.3 Dispute Resolution

Part 2, Section 6.7, discusses the inconsistency of dispute resolution practices across different payment instruments and across different merchants. In accordance with the position of the FTC Workshop on Mobile Payments[139], pp. 5-7, merchants are encouraged to develop clear policies regarding fraudulent and unauthorized charges and clearly convey these policies to consumers.

4.5.4 Increasing Hacker Attention

Part 2, Section 6.13, notes that mobile devices have received increasing attention from hackers, malware writers, and other malicious parties in the past few years, and that this trend is likely to continue. Merchants are encouraged to continue their efforts to keep the OS and apps on any mobile device used as a POS terminal malware-free by installing patches, antivirus tools, and so on, in as timely a fashion as possible (see Part 3, Section 2.4, above).

4.6 For the End User

The recommendations in this subsection are targeted primarily at end users.

[139] U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), "Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments", FTC Staff Report, March 2013. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed May 17, 2013).

4.6.1 Small Screens

As noted in Part 2, Section 6.2, small screens on mobile devices can make it difficult for users to read carefully through lengthy privacy policies or other disclosures. Users are encouraged to make every effort to thoroughly examine such information in any case, perhaps by accessing it through some other platform (such as a desktop PC), in order to be able to provide consent that is as meaningful as possible.

4.6.2 Buggy Implementations of Human Processes

The risk of buggy implementations of human processes is discussed in Part 2, Section 6.6. Such flaws can lead to disputes or to losses for both merchants and customers. Users are encouraged to make sure that they understand merchant policies that are relevant to these situations so that they are aware of their risks and associated rights.

4.6.3 Dispute Resolution

Part 2, Section 6.7, discusses the inconsistency of dispute resolution practices across different payment instruments and across different merchants. In accordance with the position of the FTC Workshop on Mobile Payments[140], pp. 5-7, users are encouraged to become familiar with merchant policies regarding fraudulent and unauthorized charges so that users understand their rights and responsibilities in this area.

4.6.4 Confiscation of Money, Blocked Transactions

Part 2, Section 6.9, discusses the possibility that, at the request of an authority or by accident, electronic money and payment transactions can blocked, confiscated, or otherwise marked as “unacceptable”. Users are encouraged to become familiar with wallet and payment app policies (and perhaps any relevant laws) that apply to these situations so that they are aware of their risks and associated rights and protections.

4.6.5 Loss or Theft of Device

If a mobile device is lost or stolen, the user will typically need to notify the mobile network operator and the payment app providers (and perhaps other entities). Users are encouraged to make use of all protections available to them from the device / OS manufacturers, the MNO, and the wallet and app providers. This may include using passwords or PINs to lock the device, the wallet, and the payment apps, using a device location finder tool, using remote encryption of data, and using a remote wipe feature. Knowing who to notify can be a burdensome process for the user because the mobile device may contain many more payment instruments and much more payment data than a physical wallet. Users are encouraged to store the emergency contact information for every entity that they may need to notify in a location that is readily accessible but independent of the mobile device. The Canadian NFC

[140] U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), “Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments”, FTC Staff Report, March 2013. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed May 17, 2013).

Mobile Payments Reference Model[141], Section 10.5.4 (pp. 59-61), includes a high-level flowchart outlining the main tasks of the user after discovering the loss or theft of a device.

4.6.6 Remote Wipe

As noted in Part 2, Section 6.12 and the Appendix, there are uncertainties regarding the effectiveness of the remote wipe operation in rendering data unrecoverable. Users are encouraged to be cautious in assuming that this mechanism will wipe data as expected and should take steps to minimize the amount of unnecessary personal data stored on the device. Furthermore, users may wish to explore other technical options for secure deletion of data, including a variety of apps or services (see Blancco[142] or Section 3.4.3 of the CSEC note on clearing electronic storage devices[143], for example).

4.6.7 Increasing Hacker Attention

Part 2, Section 6.13, notes that mobile devices have received increasing attention from hackers, malware writers, and other malicious parties in the past few years, and that this trend is likely to continue. Users are encouraged to take all available precautions to protect their devices, including downloading and installing only a trusted wallet (i.e., a wallet from a trusted source) and making every attempt to keep the device malware-free (such as installing the most current security patches, antivirus tools, and so on). Users are also encouraged not to root or jailbreak their mobile devices because this renders the devices more vulnerable to malicious software.

5. Conclusion

This third part of the mobile payments report provides security and privacy recommendations that pertain to various specific mobile payment models, as well as recommendations that pertain generally to all (many) electronic payment models. Some of these recommendations have been categorized according to particular target audiences, including device and OS manufacturers, mobile network operators, wallet/app developers, standards bodies, merchants, and end users.

[141] Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed May 23, 2013).

[142] Blancco Mobile, "Erase all data securely from smartphones and tablets", 2011. See http://www.blancco.com/en/products/total-data-erasure/mobile/ (last accessed May 27, 2013).

[143] Communications Security Establishment Canada (CSEC), "Clearing and Declassifying Electronic Data Storage Devices – ITSG-06", July 2006. See http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg06-eng.html (last accessed June 12, 2013).

References

Ananda, F. and J. Kiptum, "Security Issues in M-Banking", presentation given at the Information Security and Cyber Forensics Conference, October 29-31, 2008. See http://www.strathmore.edu/pdf/m-pesa.pdf (last accessed June 12, 2013).

Bankelele (a Nairobi writer on Banking, Finance, Technology, and Investments), "How to Get n M-Pesa Refund and other Safaricom tales", June 29, 2009. See http://www.bankelele.co.ke/2009/06/how-to-get-m-pesa-refund.html (last accessed April 22, 2013).

Barker, E., and A. Roginsky, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST Special Publication 800-131A, January 2011, pp. 13-14. See http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf (last accessed May 13, 2013).

BBC News Technology, "Frozen Android phones give up data secrets", March 7, 2013. See http://www.bbc.co.uk/news/technology-21697704 (last accessed April 19, 2013).

BlackBerry Support Community Forums, "BlackBerry 10 – NFC Card Emulation", November 2, 2012. See http://supportforums.blackberry.com/t5/Native-Development/BlackBerry-10-NFC-Card-Emulation/ta-p/1940867 (last accessed March 20, 2013). See also "NFC Primer for Developers", February 14, 2012, http://supportforums.blackberry.com/t5/Java-Development/NFC-Primer-for-Developers/ta-p/1334857 (last accessed March 20, 2013).

Berkes, J., "Side-Channel Monitoring of Contactless Java Cards", Master's thesis, Dept. of Electrical and Computer Engineering, University of Waterloo, 2008. See http://www.berkes.ca/archive/jb-thesis-final-electronic.pdf (last accessed March 26, 2013).

Blancco Mobile, "Erase all data securely from smartphones and tablets", 2011. See http://www.blancco.com/en/products/total-data-erasure/mobile/ (last accessed May 27, 2013).

Bradley, M., "Digital Wallets Executive Briefing", Information Technology Association of Canada (ITAC) Digital Commerce Forum: How Your Wallet is Going Digital, April 16, 2013. See http://itac.ca/files/2013_april_16_digital_wallet_presentation.pdf (last accessed May 1, 2013).

Canada Newswire, "CIBC and Rogers Unveil the Future of Mobile Payments in Canada", May 15, 2012. See http://www.newswire.ca/en/story/974935/cibc-and-rogers-unveil-the-future-of-mobile-payments-in-canada (last accessed February 22, 2013).

Canadian Financial Institutions ("Industry Initiative Participants"), "Canadian NFC Mobile Payments Reference Model", version 1.03, May 14, 2012. See http://collaboration/lib-bib/Library%20Document%20Collection/Canadian%20NFC%20Mobile%20Payments%20Reference%20Model.pdf (last accessed May 23, 2013).

Canadian Radio-television and Telecommunications Commission (CRTC), "You have rights", Guide for understanding rights with respect to local home phone services, section on "Disputing phone charges". See http://www.bell.ca/web/common/en/all_regions/pdfs/wireline/SCR_Final.pdf (last accessed May 10, 2013).

Carrington, D., "US Mobile Payments Forecast 2013 – 2017: Mobile Payments to Reach $90B by 2017", Forrester Research, Inc., January 16, 2013. See http://blogs.forrester.com/denee_carrington/13-01-16-us_mobile_payments_forecast_2013_2017_mobile_payments_to_reach_90b_by_2017 (last accessed February 27, 2013).

Charrat, B., "Debunking NFC Peer-to-Peer Myths", Inside Secure, February 2012. See http://insidesecure.com/eng/Media/White-papers (last accessed February 20, 2013).

Chaum, D., A. Fiat, and M. Naor, "Untraceable Electronic Cash", in Advances in Cryptology: Proceedings of CRYPTO '88, S. Goldwasser (Ed.), Springer-Verlag, 1989, pp. 319-327.

Collins, J., “Mobile payments deal between Visa and Monitise is formed”, Mobile Commerce News, March 11, 2013. See http://www.qrcodepress.com/mobile-payments-deal-between-visa-and-monitise-is-formed/8518094/ (last accessed April 16, 2013).

Common Criteria Certified Products, available at http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html (last accessed June 12, 2013).

CommTech Knowledge, “NFC-Near Field Communication: General Architecture of NFC Enabled Mobile Phones”. See http://mp-nfc.org/nfc_near_field_communication_architecture.html (last accessed March 15, 2013).

Communications Security Establishment Canada (CSEC), “Clearing and Declassifying Electronic Data Storage Devices – ITSG-06”, July 2006. See http://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg06-eng.html (last accessed June 12, 2013).

Constine, J., “Bump Pay Lets You PayPal Someone With A Tap, But Only In-Person”, TechCrunch Hot Topics, March 29, 2012. See http://techcrunch.com/2012/03/29/bump-pay/ (last accessed February 20, 2013).

Cowley, S., “NFC exploit: Be very, very careful what your smartphone gets near”, CNNMoney, July 26, 2012. See http://money.cnn.com/2012/07/26/technology/nfc-hack/index.htm (last accessed May 23, 2013).

Crowe, M. and E. Tavilla (Federal Reserve Bank of Boston), “Mobile Phone Technology: ‘Smarter’ Thank We Thought: How Technology Platforms are Security Mobile Payments in the U.S.”, November 16, 2012. See http://www.bos.frb.org/bankinfo/payment-strategies/publications/2012/mobile-phone-technology.pdf (last accessed March 21, 2013).

Dolcourt, J., “Making Sense of Mobile Payment”, CNET, August 13, 2010. See http://www.cnet.com/8301-17918_1-20013480-85.html (last accessed February 14, 2013).

Dolcourt, J., “Start Your Own Business with Square for Android”, CNET, May 19, 2010. See http://www.cnet.com/8301-19736_1-20005441-251.html (last accessed February 14, 2013).

Dolcourt, J., “Who Will Profit from NFC, Mobile Payments?”, CNET, April 7, 2011. See http://www.cnet.com/8301-17918_1-20049894-85.html (last accessed February 14, 2013).

Duffy, J., “Pay with Square (for iPhone)”, PC Magazine (pcmag.com), August 9, 2012. See http://www.pcmag.com/article2/0,2817,2408287,00.asp (last accessed April 5, 2013). [This technology is also mentioned, without detail, at https://squareup.com/ca/wallet]

Elenkov, N., “Accessing the embedded secure element in Android 4.x”, August 22, 2012. See http://nelenkov.blogspot.ca/2012/08/accessing-embedded-secure-element-in.html#!/2012/08/accessing-embedded-secure-element-in.html (last accessed March 12, 2013).

Emerging Technologies, Payment Card Industry Security Standards Council, “PCI Mobile Payment Acceptance Security Guidelines, Version 1.0”, February 2013. See https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf (last accessed March 1, 2013).

Ericsson, D., “The role of SIM OTA and the Mobile Operator in the NFC environment”, SmartTrust White Paper, April 2009. See http://www.paymentscardsandmobile.com/research/reports/SIM-OTA-Mobile-Operator-role-NFC.pdf (last accessed March 12, 2013).

Evans, P., “Rogers Wants to Start a Bank”, CBC News, September 6, 2011. See http://www.cbc.ca/news/business/story/2011/09/06/rogers-bank.html (last accessed February 22, 2013).

Gabriel, C., “PayPal extends mobile wallet, but no NFC”, Rethink Wireless, January 15, 2013. See http://www.rethink-wireless.com/2013/01/15/paypal-extends-mobile-wallet-nfc.htm (last accessed February 22, 2013).

Global Platform, Card Specification Version 2.2, March 2006. See http://www.win.tue.nl/pinpasjc/docs/GPCardSpec_v2.2.pdf (last accessed March 15, 2013).

Google Play, "Purchase with carrier billing". See http://support.google.com/googleplay/bin/answer.py?hl=en&answer=167794&topic%20=1046%20718&ctx=topic (last accessed April 8, 2013).

Groupe Speciale Mobile Association (GSMA), "Mobile NFC in Retail", White Paper, Version 1.0, September 2012. See http://www.gsma.com/mobilenfc/wp-content/uploads/2012/10/Mobile-NFC-in-Retail-White-Paper-Oct-2012.pdf (last accessed May 23, 2013).

Hardy, I., "WIND Mobile goes live with BlackBerry World carrier billing", MobileSyrup, April 1, 2013. See http://mobilesyrup.com/2013/04/01/wind-mobile-goes-live-with-blackberry-world-carrier-billing/ (last accessed April 30, 2013).

Hermon-Duc, S. (TSF Project Manager), "MPESA project analysis: Exploring the use of cash transfers using cell phones in pastoral areas", Télécoms Sans Frontières Project Report, 2012. See http://www.alnap.org/pool/files/mpesa-project-analysis-tsf-vsfg.pdf (last accessed April 12, 2013).

Holly, R., "How to use NFC to automate your mobile routine", geek.com, February 8, 2012. See http://www.geek.com/articles/mobile/how-to-use-nfc-to-automate-your-mobile-routine-2012028/ (last accessed March 25, 2013).

Inside Secure, "Opening the NFC stack to Java and native applications", Corporate Background paper, November 2010. See http://www.insidesecure.com/content/download/1095/12802/version/6/file/WHITE%20PAPER_NEW%20CHARTE-3.pdf (last accessed March 15, 2013).

Isis Mobile Wallet (Isis was founded by AT&T Mobility, T-Mobile USA, and Verizon Wireless to realize their shared vision of mobile commerce). See http://www.paywithisis.com/ (last accessed February 28, 2013).

ISO/IEC Joint Technical Committee 1, Subcommittee 17, "ISO/IEC 7816 Identification cards – Integrated circuit cards – Cards with contacts".

ISO/IEC Joint Technical Committee 1, Subcommittee 17, Working Group 8, "ISO/IEC 14443 Identification cards – Contactless integrated circuit cards – Proximity cards".

Jackson, B., "Google Wallet and NFC security: guarding against 'sharks with lasers'", IT Business, September 29, 2011. See http://www.itbusiness.ca/news/google-wallet-and-nfc-security-guarding-against-sharks-with-lasers/16531 (last accessed April 4, 2013).

Kerschberger, M., "Near Field Communication: A survey of safety and security measures", Bachelorarbeit, Technical University of Vienna, July 17, 2011. See https://www.auto.tuwien.ac.at/bib/pdf_TR/TR0156.pdf (last accessed March 26, 2013).

Kharif, O., "NFC Stickers Make Smartphones Smarter", Bloomberg Businessweek: Technology, July 12, 2012. See http://www.businessweek.com/articles/2012-07-12/nfc-stickers-make-smartphones-smarter (last accessed March 25, 2013).

Knight, S., "Americans lost $30 billion worth of mobile phones in 2011", TechSpot, March 23, 2012. See http://www.techspot.com/news/47930-americans-lost-30-billion-worth-of-mobile-phones-in-2011.html (last accessed April 23, 2013).

Kremer, J., "NFC: Near Field Communication White Paper", Jan Kremer Consulting Services. See http://jkremer.com/White%20Papers/Near%20Field%20Communication%20White%20Paper%20JKCS.pdf (last accessed May 23, 2013).

Kessler, S., "Bank Lets Customers Pay Friends By Bumping iPhones", April 29, 2011. See http://mashable.com/2011/04/29/ing-direct-customers-bump/ (last accessed February 20, 2013).

Lewis, M., "Registry targets smartphone black market", The Toronto Star: Business, November 8, 2012. See http://www.thestar.com/business/2012/11/08/registry_targets_smartphone_black_market.html (last accessed June 12, 2013).

London Action Plan (LAP) and Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG), "Best Practices to Address Online and Mobile Threats", October 15, 2012. See http://www.maawg.org/sites/maawg/files/news/M3AAWG_LAP_Best_Practices_to_Address_Online_and_Mobile_Threats_0.pdf (last accessed May 17, 2013).

Mick, J., "Inside the Mega-Hack of Bitcoin: the Full Story", DailyTech, June 19, 2011. See http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm (last accessed May 3, 2013).

Mobile Transaction, "Growing Use of SMS Payments Around the World". See http://www.mobiletransaction.org/sms-payments/around-the-world (last accessed February 20, 2013).

Moffa, T. (Communications Security Establishment Canada), "CSEC Approved Cryptographic Algorithms for the Protection of Sensitive Information and for Electronic Authentication and Authorization Applications within the Government of Canada", CSEC ALERT ITSA-11E, March 2011, Section on "Hashing Algorithms and Status of SHA-1". See http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11e-eng.html (last accessed May 13, 2013).

NFC Times, "Topic: 'Trusted Service Manager'", 2013 (this is a collection of recently-signed TSM contracts). See http://nfctimes.com/tags/trusted-service-manager (last accessed February 28, 2013).

NFC World, "A Definitive List of NFC Phones, Last updated on 19 February 2013". See http://www.nfcworld.com/nfc-phones-list/ (last accessed February 19, 2013).

Pauli, D., "Android app steals contactless credit card data", SC Magazine, June 21, 2012. See http://www.scmagazine.com.au/News/305881,android-app-steals-contactless-credit-card-data.aspx (last accessed March 22, 2013).

Payment Card Industry (PCI) Security Standards Council, Emerging Technologies, "PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users", Version 1.0, February 2013. See https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf (last accessed May 17, 2013).

PayPal, "Texting with PayPal – easy as lifting a finger". See https://personal.paypal.com/ca/cgi-bin/?cmd=_render-content&content_ID=marketing_ca/mobile_text (last accessed February 20, 2013).

PCI Security Standards Council Emerging Technology Whitepaper, "Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance for Transmissions of Cardholder Data and Sensitive Authentication Data", Program Guide Version 1.0, October 5, 2010. See https://www.pcisecuritystandards.org/pdfs/pci_ptp_encryption.pdf (last accessed May 1, 2013).

Personal Information Protection and Electronic Documents Act. The Act is available at http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html; some surrounding discussion is available at http://www.pipeda.info/a/1.html (each site last accessed June 12, 2013).

Pipenbrinck, N., "Secure Element communication with PCD/reader", stackoverflow, June 22, 2012. See http://stackoverflow.com/questions/11152614/secure-element-communication-with-pcd-reader (last accessed April 4, 2013).

Ricknas, M., “Inside Secure Opens Door for Multiple Wallets on One Smartphone”, CIO Drilldowns, October 29, 2012. See http://www.cio.com/article/720174/Inside_Secure_Opens_Door_for_Multiple_Wallets_on_One_Smartphone (last accessed March 21, 2013).

Roland, M., C. Saminger, and J. Langer, “Packet Sniffer for the Physical Layer of the Single Wire Protocol”, Research report, Upper Austria University of Applied Sciences. See http://research.fh-ooe.at/files/publications/941_PacketSnifferPhysicalLayerSWP.pdf (last accessed March 19, 2013).

Rosa, T., “RFID Wormholes: The Case of Contactless Smartcards”, SmartCard Forum, Prague, Czech Republic, 2011. See http://crypto.hyperlink.cz/files/rosa_wormhole_v1a.pdf (last accessed March 26, 2013).

Samuel, S., “New in the Android Market: Updated PayPal Mobile App Featuring P2P NFC Capabilities”, The PayPal Blog, November 8, 2011. See https://www.thepaypalblog.com/2011/11/new-in-the-android-market-updated-paypal-mobile-app-featuring-p2p-nfc-capabilities-2/ (last accessed February 20, 2013).

Sequent Glossary; see http://www.sequent.com/glossary/s (last accessed March 12, 2013).

Sequent Glossary; see http://www.sequent.com/glossary/n (last accessed March 15, 2013).

Smart Card Alliance, “Security of Proximity Mobile Payments”, A Smart Card Alliance Contactless and Mobile Payments Council White Paper, Publication CPMC-09001, May 2009. See http://collaboration/lib-bib/Library%20Document%20Collection/Security%20of%20Proximity%20Mobile%20Payments.pdf (last accessed February 14, 2013).

Snopes.com, “Electronic Pickpocketing”, October 4, 2012. See http://www.snopes.com/fraud/identity/pickpocket.asp (last accessed March 22, 2013). See also http://www.youtube.com/watch?v=EKks3vfiy6Q

Square, Inc. See https://squareup.com/ca?country_code=ca (last accessed April 5, 2013).

Square, Inc., Square Register. See https://squareup.com/ca/register (last accessed April 5, 2013).

Square pricing, as shown at https://squareup.com/ca/pricing (last accessed February 27, 2013).

Stark, J., “Mobile Payments: Starbucks App”, June 20, 2011. See http://jonathanstark.com/blog/mobile-payments-starbucks-app (last accessed February 27, 2013). [See also http://www.starbucks.ca/coffeehouse/mobile-apps/mystarbucks]

Task Force for the Payments System Review, “Going Digital: Transitioning to Digital Payments”, Report issued to the Minister of Finance, 2011. See http://paymentsystemreview.ca/wp-content/themes/psr-esp-hub/documents/r03_eng.pdf (last accessed February 13, 2013).

Telco 2.0 News Review (blog), “Security Breach at M-PESA: Telco 2.0 Crash Investigation”, Telco 2.0, February 12, 2010. See http://www.telco2.net/blog/2010/02/security_breach_at_mpesa_telco.html (last accessed April 12, 2013).

Terdiman, D., “Prowling the streets of San Francisco with Square Wallet”, CNET News, November 20, 2012. See http://news.cnet.com/8301-1023_3-57552199-93/prowling-the-streets-of-san-francisco-with-square-wallet/ (last accessed April 5, 2013).

The Paypers: Insights in Payments, “Brazil: PagSeguro, Nokia to introduce NFC P2P payments”, May 3, 2012. See http://www.thepaypers.com/news/mobile-payments/brazil-pagseguro-nokia-to-introduce-nfc-p2p-payments/747502-16 (last accessed February 22, 2013).

The Royal Canadian Mint, “MintChip Developer Resources”. See http://developer.mintchipchallenge.com/devguide/index.php (last accessed February 14, 2013).

The Royal Canadian Mint, “MintChip Developer Resources: Message Validation”, April 4, 2012. See http://developer.mintchipchallenge.com/devguide/developing/common/message-validation.html (last accessed April 8, 2013).

The Royal Canadian Mint, “MintChip Developer Resources: MintChip Messages”, April 4, 2012. See http://developer.mintchipchallenge.com/devguide/developing/common/mintchip-messages.html (last accessed April 8, 2013).

U.S. Federal Communications Commission (FCC) Infographic on Cramming. See http://www.ftc.gov/os/2011/12/111227crammingcomment.pdf (last accessed April 8, 2013).

U.S. Federal Trade Commission (FTC) Division of Financial Practices (D. Pozza, P. Poss, J. Chen, et al.), “Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments”, FTC Staff Report, March 2013. See http://www.ftc.gov/os/2013/03/130306mobilereport.pdf (last accessed May 17, 2013).

U.S. National Institute of Standards and Technology (NIST), “NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition”, NIST Tech Beat, October 2, 2012. See http://www.nist.gov/itl/csd/sha-100212.cfm (last accessed April 8, 2013).

VeriFone, PAYware Mobile. See http://www.paywaremobile.com/ (last accessed February 14, 2013).

Visa, “Digital Wallet Security: Just ‘LOK’ it”. See http://www.cimbbank.com.my/creditcard/index.php?ch=2&pg=14&ac=9&bb=attachment (last accessed March 21, 2013).

Walubengo, N., “The Mobile Money Apocalypse; What Would Happen to Your Money?”, PesaTalk, November 2, 2012. See http://pesatalk.com/the-mobile-money-apocalypse-what-would-happen-to-your-money/ (last accessed April 17, 2013).

Wanjiku, R., “Security issues hit African mobile money providers”, Computerworld, November 17, 2009. See http://news.idg.no/cw/art.cfm?id=03381EE0-1A64-6A71-CE896C46D67B6FFC (last accessed April 12, 2013).

Whitwam, R., “How To Have Fun with Near Field Communication on Android”, Tested, April 27, 2011. See http://www.tested.com/tech/android/2234-how-to-have-fun-with-near-field-communication-on-android/ (last accessed March 25, 2013).

Wikipedia, the Free Encyclopedia, “Digital Wallet”. See http://en.wikipedia.org/wiki/Digital_wallet (last accessed February 15, 2013). See also “A Global Overview of Digital Wallet Technologies”, published by the ID Lab, University of Toronto, on May 28, 2011: http://propid.ischool.utoronto.ca/digiwallet_overview/ (last accessed February 15, 2013).

Wikipedia, the Free Encyclopedia, “NFC-WI”. See http://en.wikipedia.org/wiki/NFC-WI (last accessed March 15, 2013).

Wikipedia, the Free Encyclopedia, “PayPal”. See http://en.wikipedia.org/wiki/PayPal (last accessed February 20, 2013).

Wikipedia, the Free Encyclopedia, “Single Wire Protocol”. See http://en.wikipedia.org/wiki/Single_Wire_Protocol (last accessed March 15, 2013).

Yawe, R., “How secure is mpesa”, KICTAnet (Kenya ICT Action Network), July, 2011. See http://www.kictanet.or.ke/?p=713 (last accessed April 22, 2013).

Appendix: Remote Wiping on Mobile Devices

[The first two paragraphs below are a summary of a private e-mail sent to a colleague of mine by an R&D employee at a Mobile Device Management (MDM) company.]

Mobile devices typically use flash memory technology, which is significantly different from the hard drive technology used on desktop and (some) laptop computers. In particular, flash memory has the peculiar characteristic that every memory location has an expected lifetime for the number of writes that can be performed. To extend the lifetime of the flash, an algorithm exists on the device that spreads the data over the flash evenly to prevent wear-out. The data is thus spread all over the flash chips and some clever logic converts it into a readable format that looks like a hard drive file system.

Now consider file deletion on a mobile device flash memory. In order to implement “secure delete” (as mentioned in Part 2, Section 6.12 above, where a file is overwritten several times with purely random data) it would be necessary to do a lot of writing all over the memory, which would wear the flash unnecessarily. Consequently, this is not done. Thus, it seems likely that if an attacker were to do a forensic recovery by reading every memory location on the flash, s/he could conceivably recover the files stored there.

Furthermore, on some mobile operating systems (iOS and Android, for example) apps are partitioned so that an app can only write to its own space; it cannot access the files of other apps. Thus, it is not even possible on such operating systems to create a single app that performs remote wipe across the device.

Note that Apple does supply its own remote management software which includes an option to return a device to “factory state”. Initial testing indicates that this is secure with respect to forensics (little to no data is recoverable after such an operation). However, the option to wipe the device after a fixed number of incorrect password attempts is not secure and almost all data are recoverable.

Finally, although Apple’s remote wiping feature works well (at least for factory-reset), most MDM companies implement their own version, and this is often insecure. For example, a pre-owned Android tablet (Acer Iconia) purchased from eBay had supposedly been reset to factory settings. A forensic recovery was attempted on the device to see what was available: analysis revealed that photos and web page images of the previous owner were included among the files recovered.

List of Acronyms

AES	Advanced Encryption Standard
ASK	Amplitude Shift Keying
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
CVV	Card Verification Value
DES	Data Encryption Standard
DNS	Domain Name System
EEPROM	Electrically-Erasable Programmable Read-Only Memory
FI	Financial Institution
FIPS	(U.S.) Federal Information Processing Standards
FTC	(U.S.) Federal Trade Commission
HCI	Host Controller Interface
HSM	Hardware Security Module
I/O	Input / Output
IP	Internet Protocol
ISO	International Organization for Standardization
LAP	London Action Plan
M^{3}AAWG	Messaging, Malware and Mobile Anti-Abuse Working Group
mAccept	Mobile Acceptance
mCommerce	Mobile Commerce
MDM	Mobile Device Management
MicroSD	(Micro-sized) Secure Digital memory card
MITM	Man-in-the-Middle
MNO	Mobile Network Operator
mP2P	Mobile Peer-to-Peer
mPOS	Mobile Point-of-Sale
NFC	Near-Field Communications
NFC-WI	NFC Wired Interface
OEM	Original Equipment Manufacturer
OPC	Office of the Privacy Commissioner of Canada
OS	Operating System
OTA	Over-the-Air
PC	Personal Computer
PCI	Payment Card Industry
PCISSC	Payment Card Industry Security Standards Council
PDF	Portable Document Format
PIN	Personal Identification Number
PIPEDA	Personal Information Protection and Electronic Documents Act
POS	Point-of-Sale
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman cryptographic algorithm
S2C	SignalIN / SignalOUT Connection
SD	Security Domain
SE	Secure Element
SHA-1	Secure Hash Algorithm 1 (similarly, SHA-2 and SHA-3)

SIM	Subscriber Identity Module
SMS	Short Message Service
SSD	Supplemental Security Domain
SWP	Single Wire Protocol
TLS	Transport Layer Security
TSM	Trusted Service Manager
UICC	Universal Integrated Circuit Card
USB	Universal Serial Bus

Glossary

Card Verification Value (CVV): A 3- or 4-digit value printed on the front of a credit or debit card, or on the signature strip on the back of the card. It is not encoded on the magnetic stripe and is used as a security measure (merchants may require this value for “card not present” transactions).

Jailbreaking a Mobile Device: The process of removing limitations on Apple devices running the iOS operating system. Jailbreaking permits root access to the operating system, allowing the download of additional applications, extensions, and themes that are unavailable through the official Apple App Store. Jailbreaking is a form of privilege escalation.

Malware (Malicious Software): Hostile or intrusive software that is used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Man-in-the-Middle (MITM) Attack: A form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Mobile Acceptance (mAccept): The mobile payment model in which financial transactions take place between an individual and a merchant, and the merchant’s device is a mobile device (rather than a traditional point-of-sale terminal).

Mobile Commerce (mCommerce): The mobile payment model in which an individual uses an app or the browser on a mobile device to do online shopping / banking at a remote website.

Mobile Device: A small, handheld computing device (such as a smart phone or a tablet), typically having a display screen with touch input and/or a miniature keyboard. The device has an operating system and can run various types of application software (apps); additionally, it often also has Internet connectivity, a camera, and a multimedia player.

Mobile Peer-to-Peer (mP2P): The mobile payment model in which financial transactions (typically money transfers) take place between individuals, neither of whom is a registered merchant. Both individuals use a mobile device for the transaction.

Mobile Point-of-Sale (mPOS): The mobile payment model in which financial transactions take place between an individual with a mobile device and a merchant with a (possibly contactless) point-of-sale (POS) terminal.

NFC Tag: A short-range RFID chip that communicates with a reader using NFC technology. It is passive, meaning that it does not have its own power source (a battery), but rather draws its power to operate from the device that reads it.

Rooting a Mobile Device: Similar to jailbreaking (see above), but for mobile devices running the Android operating system. Rooting gives “root” privileges to user-installed apps, which allows such apps to run privileged commands typically unavailable in the stock configuration, including modifying or deleting system files, removing carrier- or manufacturer-installed applications, and enabling low-level access to the hardware.

Secure Element: A tamper-resistant integrated circuit capable of securely hosting applications (including payment applications) and their confidential and cryptographic data (e.g., cryptographic keys).

Unlocking a Mobile Device: Bypassing the constraints that have been put in place to restrict the use of a device to specific countries and network providers.

Wallet (Electronic Wallet): An app (“mobile wallet”) or server/cloud service (“digital wallet”) that manages payment instruments and associated data. The wallet has a user interface so that the user can select and enable specific payment instruments (including debit and credit cards, loyalty cards, and coupons) at the time of a payment transaction.