THE FUTURE OF WALLETS: A LOOK AT THE PRIVACY IMPLICATIONS OF MOBILE PAYMENTS

Meena Aharam Rajan[‡]

I. INTRODUCTION

What's in your wallet? Normal wallets can be inches thick, containing cash, credit cards, and debit cards, providing a number of payment choices for consumers.[1] While credit and debit cards are the most convenient forms of non-cash payment,[2] consumers often sacrifice privacy and security for the sake of this convenience.[3] As a result, lawmakers have crafted financial privacy legislation that protects consumers who want the convenience of paying by card, while ensuring their security and privacy, and providing recourse in the event of unauthorized transactions.[4]

Imagine, however, leaving your entire wallet at home and still having the ability to make purchases. The increasing ability of consumers to make Mobile Payments ("M-Payments") is close to making the elimination of wallets a reality.[5] New technology, known as Near Field Communication ("NFC"),

---

‡ J.D., May 2012, Catholic University of America, Columbus School of Law. Meena would like to thank Professor Bruce Jackson for his expert advice and guidance while writing this article and the CommLaw Conspectus staff for their invaluable support during the editing process. Meena also greatly appreciates the constant encouragement and support from her family, especially from her husband, Venk Rajan, and for everyone's hard work on Volume 20 of CommLaw Conspectus that made this publication possible.

[1] Other common payment methods include personal checks, money orders, and electronic methods, such as PayPal and online bill payment. Kevin Foster et al., *The 2009 Survey of Consumer Payment Choice*, *in* PUBLIC POLICY DISCUSSION PAPERS, at 10-11 (Fed. Reserve Bank of Boston, No. 11-1, April 2011), *available at* http://commcns.org/JM1dl0.

[2] *Id.* at 18.

[3] *See generally id.* (discussing the study of cash and non-cash payment behavior of U.S. consumers).

[4] *See* discussion, *infra* Parts IV.A-C.

[5] Tony Bradley, *What You Need to Know About NFC Smartphone Payments*, PCWORLD (Feb. 2, 2011), http://commcns.org/LBGboJ.

coupled with mobile purchasing applications, available on smartphones, may revolutionize the way Americans purchase groceries, buy gas, or pay at restaurants.[6] While the introduction of technology that will potentially integrate phones and finances is exciting, it warrants an examination of the scope of current legislation and potential regulations to ensure consumer protection and privacy when using M-Payments.

This Article examines the privacy and consumer protection implications of employing M-Payments in the United States and ultimately recommends the best implementation method from a legal context. Section II begins with an introduction and explanation of M-Payments, as well as a brief history of their global implementation in Section III. Next, Section IV examines the current state of privacy and consumer protection laws as they relate to financial data and payments. Section V continues with an analysis of M-Payment forms and execution methods by identifying the key players involved and discussing the privacy and consumer protection implications of each. Finally, Section VI makes legislative recommendations on how to better serve consumers as they embrace M-Payments in the United States.

II. BACKGROUND ON MOBILE PAYMENTS

Given the dramatic change in commerce over the last century, the adoption of M-Payments is an inevitable evolution of payment systems.[7] With an estimated five billion mobile phone subscriptions worldwide and a population of seven billion people, cell phones have become firmly cemented in the average person's life.[8] In fact, estimates indicate that cell phones have

---

[6] *See generally* Mahil Carr, *Mobile Payment Systems and Services: An Introduction*, MOBILE PAYMENT FORUM OF INDIA (2010), http://commcns.org/KTdClb (addressing the mobile technology landscape, including issues that arise with mobile payment services). For purposes of this Article, M-Payments refer to any use of your phone to assist in purchasing or paying a bill.

[7] The 20th century began with almost sole reliance on hard currency and bank transfer orders for large purchases. However, as technology improved and people became more mobile, payment systems transformed to accommodate. In the mid-1940s the credit card was introduced in a "closed-loop" system involving the merchant, bank (or issuer), and consumer. By the 1960s the credit card quickly evolved to an "open-loop system" which required inter-bank cooperation and fund transfers. It was at this time that issues of privacy and consumer protection became important for customers utilizing these payment methods. Since that time, technology has opened the door for many additional financial conveniences including electronic commerce and online banking. *Secrets of Making Money: The History of Money*, NOVA (Oct. 26, 1996), http://commcns.org/LBGsId. *See generally* Oren Bar-Gill, *Seduction By Plastic*, 19 NW. U. L. REV. 1373 (2004) (providing a detailed history and explanation of the importance of the credit card).

[8] Lance Whitney, *Cell Phone Subscriptions to Hit 5 Billion Globally*, CNET (Feb. 16, 2010), http://commcns.org/LPzWR2. Consumers are becoming increasingly comfortable with mobile phones fulfilling numerous functions. REMCO BOER & TONNIS DE BOER, MOBILE

penetrated ninety-one percent of the population in the United States.[9] Due to their convenience and presence in everyday life, making mobile phones a vehicle for e-commerce is a natural progression.[10] The potential to share in the e-commerce market therefore presents an opportunity to reach consumers who crave convenience.

A. What Are M-Payments and How Do They Work?

For the purpose of this Article, M-Payments are defined as "any payment where a mobile device is used to initiate, authorize, and confirm an exchange of financial value in return for goods and services. . . ."[11] M-Payments occur not only when the mobile phone is involved in the initiation and confirmation of the payment, but also when the mobile phone is used to place an order but not facilitate payment.[12] Other forms of M-Payments include mobile delivery, where consumers use their mobile device to receive delivery of goods or services, such as event tickets, and mobile authentication, where the phone authenticates the user as part of a payment transaction.[13]

There are two main forms of M-Payments: remote M-Payments and proximity M-Payments. Remote M-Payments do not require NFC technology. Instead, customers use phones equipped with either short messaging service ("SMS") or wireless application protocol ("WAP") technology to make payments to merchants or individuals.[14] On the other hand, proximity M-Payments allow customers to use a NFC-enabled phone at the point-of-sale by waving their phone in front of a NFC-equipped terminal.[15] Individuals are able to make proximity M-Payments both at staffed checkout registers or unstaffed vending machines.[16]

PAYMENTS 2010: MARKET ANALYSIS AND OVERVIEW 10 (2009), http://commcns.org/JysOcP.

[9] Chris Foresman, *Wireless Survey: 91% of Americans Use Cell Phones*, ARS TECHNICA (Mar. 24, 2010), http://commcns.org/K9Ah3k.

[10] Carr, *supra* note 6, at 1. The U.S. Department of Commerce reported preliminary estimates of U.S. e-commerce sales totaling $194.3 billion in 2011, accounting for 4.6% of total retail spending in that year. This also represents an increase of 16.1% over 2010 U.S. e-commerce spending. Press Release, The Census Bureau of the Dep't of Commerce, Quarterly Retail E-commerce Sales 4th Quarter 2011 (Feb. 16, 2012), http://commcns.org/KE1Iz8.

[11] "Mobile devices may include mobile phones, PDAs, wireless tablets and any other device that connect to mobile telecommunication network and make it possible for payments to be made." Carr, *supra* note 6, at 1.

[12] *Id.* at 3-6.

[13] *Id.* at 5.

[14] Timothy R. McTaggart & David W. Freese, *Regulation of Mobile Payments*, 127 BANKING L. J. 485, 486 (2010).

[15] FIRST DATA, CONTACTLESS PAYMENTS: THE 'TIPPING POINT' IS AT HAND 2 (2010).

[16] *Id.* at 17.

1. The Players

The process of completing M-Payment transactions and the stakeholders involved differ from that of traditional payment models. For instance, traditional credit card payments involve only the issuer, acquirer, merchant, and consumer.[17] If a consumer uses a credit or debit card, financial corporations, such as Visa and MasterCard, become involved by authenticating and settling transactions on behalf of the issuing bank and the merchant.[18] Payments via the Internet initially relied on traditional credit and debit cards, but more recently have included "peer-to-peer" models developed by payment service providers like PayPal.[19]

Proximity M-Payments include not only traditional stakeholders like banks, merchants and financial corporations, but also mobile handset manufacturers, wireless carriers, and mobile application developers.[20] Mobile handset manufacturers develop NFC-enabled mobile phones, which require wireless carriers to transmit financial data across their networks.[21] Finally, M-Payments require mobile application developers who create various applications to enable money transfers between customers and merchants.[22]

2. SMS-based Remote M-Payments

The simplest form of remote M-Payment utilizes SMS.[23] Such payment requires a customer to first establish an account with a mobile payment service provider ("MPSP"), such as PayPal, and link his or her bank account or credit or debit card to the account.[24] Next, the customer sends a text message to the MPSP designating the amount of money to be transferred and the mobile phone number of the payee.[25] The MPSP then authenticates the transfer by sending a text message back to the customer requiring the customer to respond with her personal identification number ("PIN").[26] Once the customer texts his or her PIN to the MPSP, it transfers the payment to the payee's MPSP account,

---

[17] *See* Taggart & Freese, *supra* note 14, at 486-87. In a traditional check payment, the issuer issues the payment instrument to the consumer and processes the payment from consumer to merchant, and the acquirer processes the payment on behalf of the merchant. *Id.*

[18] *Id.* at 487.

[19] *Id.*

[20] *Id.*

[21] *Id.* at 488.

[22] JEROEN DE BEL & MONICA GÂZA, MOBILE PAYMENTS 2012, MY MOBILE, MY WALLET? 12-13, 16-18 (2011).

[23] *See* Taggart & Freese, *supra* note 14, at 488.

[24] *Id.*

[25] *Id.*

[26] *Id.*

subsequently notifying the payee that the payment was successful.[27] For added security, if the payee is a business and the customer is remote, the system may require the purchased goods to be shipped to the address tied to the customer's MPSP account.[28]

3. WAP-based Remote M-Payments

Another form of M-Payment occurs through mobile Web payments.[29] While this form of M-Payment offers a quick and reliable payment option for consumers, it is not considered a true M-Payment because it utilizes Wireless Application Protocol ("WAP") for the transaction, rather than a uniquely mobile medium.[30] In this type of M-Payment, customers access a merchant's website using their mobile phone's browser in order to make purchases in the same manner they would from a desktop or laptop computer.[31]

Merchants may also provide a customer with a M-Payment application, which the customer can then use to make purchases. Widely used examples include the Groupon and LivingSocial applications, which allow users to purchase and redeem coupons directly from their phones.[32] Another popular form of mobile Web payment enables customers to pre-load money into an account linked to a gift card that is then displayed on a mobile phone screen, which the merchant scans during the transaction.[33] Starbucks has employed this method, processing over twenty million mobile payments in the past year.[34]

4. NFC Technology

The newest form of M-Payments, and arguably the one with the most potential to impact consumers, is proximity M-Payments using NFC technology. Proximity M-Payments allow consumers to use their phones at merchant stores as they would any other payment card. Therefore, companies

---

[27] *Id.*

[28] KRISTA BECKER, EMERGING PAYMENTS INDUSTRY BRIEFING, MOBILE PHONE: THE NEW WAY TO PAY? 3-4 (2007), http://commcns.org/MVnH7J.

[29] *Id.* at 4-5.

[30] *Id.*

[31] *Id.*

[32] Dan Frommer, *Groupon Is on Its Way to Becoming the Next Big Mobile Ad Network*, BUSINESS INSIDER (May 23, 2011), http://commcns.org/M2hxDp; Rimma Katz, *Living Social Takes a Bite Out of Mobile via New LBS Deal*, MOBILE COM. DAILY (June 8, 2011), http://commcns.org/L14Pjz.

[33] Frederic Lardinois, *Now There's an App That Lets You Pay for Coffee at Starbucks*, READWRITEWEB (Sept. 22, 2009), http://commcns.org/KZISow.

[34] Paula Berger, *Starbucks Hits 20M M-Payments*, NEAR FIELD COMM. WORLD (Nov. 8, 2011), http://commcns.org/JKO8NN.

are touting this form of payment as a seamless way to integrate all of consumers' financial needs in an easy-to-use device that consumers already carry.[35]

Proximity M-Payments require a NFC chip in a customer's mobile phone. The NFC chip accesses the customer's financial account information through device software and allows the phone to communicate with a point-of-sale ("POS") terminal.[36] The NFC chip is installed in the device thereby allowing a customer to be able to wave his or her phone near the POS terminal, which then reads the chip, receives the phone's serial number and the unique transaction code, and sends this data to the merchant's acquiring bank.[37] The acquiring bank sends the transaction data to the customer's bank, which uses the data to authenticate the phone's validity, identify the account from which to authorize payment, and determine whether to authorize or decline the transaction.[38]

B. Technology and Security

Concerns over the security of information as it is transferred from consumer to recipient dominate the discussion surrounding M-Payments.[39] While proximity M-Payments utilize the same security features as contactless payment—encrypted data and unique transaction codes—SMS-based remote M-Payments are facilitated with data traveling in plain text, a much less secure option.[40] WAP-based remote M-Payments, however, provide greater security as the data is encrypted as it travels from customer to merchant.[41]

1. SMS-based Remote M-Payments

In order for customers to use SMS-based remote M-Payments, they must have a SMS capable phone that is both charged and able to receive cellular

---

[35] Nancy Gohring, *Visa, MasterCard and AmEx Join Google Wallet Competitor*, PCWORLD (July 19, 2011), http://commcns.org/KCpvz1.

[36] Erica Ogg, *How Mobile Payments Will Work (FAQ)*, CNET NEWS (Apr. 7, 2011), http://commcns.org/LE92rQ.

[37] VERIFONE, NFC PAYMENTS AND POINT OF SALE 8 (2011), http://commcns.org/LBYflY.

[38] *Id.*

[39] James Linlor, Chief Exec. Officer, Black Lab Mobile, Federal Trade Commission Public Hearings on Protecting Consumers in the Next Tech-ade: Mobile Payment Systems and Threats, (Nov. 8, 2006), *available at* http://commcns.org/JrEObh.

[40] Manoj V, Bramhe, *SMS Based Secure Mobile Banking*, 3 INT'L J. OF ENGINEERING & TECH. 472, 472 (2011).

[41] Seema Nambiar et al., *Analysis of Payment Transaction Security in Mobile Commerce*, *in* PROCEEDINGS OF THE 2004 IEEE INTERNATIONAL CONFERENCE ON INFORMATION REUSE AND INTEGRATION 475, 477 (2004).

service.[42] SMS enables customers to send messages to a receiver to authorize payment and provide goods, either directly to the user's phone or to another device, such as a vending machine or parking meter.[43] Due to the need for a strong cellular signal, utilizing this form of payment may be problematic if consumers are inside of a building or out of reach of their mobile network.[44] This often causes communication failures to occur or SMS texts to be lost.[45]

Though SMS M-Payments are inexpensive and relatively easy, they have severe security implications. First, SMS messages are sent as clear text, which lacks the encryption capability necessary to secure confidential information from unauthorized access.[46] Moreover, because the merchant stores confidential information after it is transmitted by the consumer, the security of the transaction also depends on the security of the merchant's data systems.[47] Finally, SMS messages do not contain the necessary authentication protocols to ensure parties requesting the transaction are not impostors.[48] For these reasons, SMS M-Payments are not considered a viable option for transfers of large sums of money or as a widespread payment option.

2. WAP-based Remote M-Payments

WAP-based remote M-Payments are made frequently through applications that are downloaded and installed on a mobile device.[49] To access the Internet through wireless networks, these applications use the Wireless Application Environment ("WAE"), an effort to create and maintain an industry-wide standardized framework designed to connect a variety of different wireless platforms with the rest of the Internet.[50] This allows information to travel over the Internet via WAP through a mobile service provider's network.[51] Payments

---

[42] Marianne Crowe et al., *Mobile Payments in the United States at Retail Point of Sale: Current Market and Future Prospects*, *in* PUBLIC POLICY DISCUSSION PAPERS, at 8 (Fed. Reserve Bank of Boston, No. 10-2, 2010).

[43] *Id.* at 7.

[44] *Id.* at 8.

[45] There is no automatic proof of delivery mechanisms for SMS communication, and thus consumer will have no assurance that payment was received. Such a system may be expensive to implement, thereby making it unavailable. BOER & BOER, *supra* note 8, at 12.

[46] *Id.* at 41.

[47] *Id.* at 42.

[48] *Id.* This is mainly true for post-SMS billing services, where a stolen cell phone may incur numerous charges until a cell phone account is manually blocked. *Id.*

[49] MOBILE RETAIL INITIATIVE, NAT'L RETAIL FED'N, MOBILE RETAILING BLUEPRINT: A COMPREHENSIVE GUIDE FOR NAVIGATING THE MOBILE LANDSCAPE 67 (2011).

[50] OPEN MOBILE ALLIANCE, WIRELESS APPLICATION PROTOCOL: WIRELESS APPLICATION ENVIRONMENT OVERVIEW 3, 10 (1999).

[51] Andrew Stucken, *What is WAP?*, BBC WEBWISE (Sept. 9, 2010), http://commcns.org/KXMYt9.

that utilize applications and WAP allow users to access mobile merchant sites directly through their mobile network.[52]

WAP-based remote M-Payments have more practical applicability than SMS payments, allowing users to purchase higher-value items by linking credit or bank accounts to merchant sites.[53] However, such payments require a customer to have at least a web-enabled phone or smartphone.[54] Additionally, although proposals have been advanced to create a Secured Wireless Application Protocol ("SWAP"), WAP is not currently a secured network.[55] Further security risks include malware or spyware that may be unintentionally downloaded and may steal data off a phone.[56] For example, it was recently discovered that Google's Android marketplace was hosting malicious applications, the second such instance of this happening.[57]

3. NFC Technology

As discussed, NFC technology allows two autonomous devices to communicate over short distances.[58] To complete NFC payments, two devices must "shake hands" and, if allowed, provide the user specified credit or debit card information to the merchant's device.[59] NFC technology has been compared to Bluetooth, but is considered a superior technology for financial payments due to its closer proximity requirement and the fact that the mobile wallet may still be used even when the device battery is dead.[60]

If NFC reaches its full potential, it may be an incredibly attractive option for consumers, but also may make consumers vulnerable to information theft. While losing a phone is normally a traumatic experience, imagine losing a

---

[52] *Id.*

[53] *See* Taggart & Freese, *supra* note 14, at 488.

[54] *Id.*

[55] Niels Christian Juul & Niels Jorgensen, *Security Issues in Mobile Commerce Using WAP*, *in* 15TH BLED ELECTRONIC COMMERCE CONFERENCE, E-REALTY: CONSTRUCTING THE E-ECONOMY 2 (2002).

[56] Katie Murphy, *Build Up Your Phone's Defenses Against Hackers*, N.Y. TIMES, Jan. 25, 2012, http://commcns.org/KZK5fs.

[57] See Dan Goodin, *Google's Official App Market Found Hosting Malicious Android Apps—Again*, ARS TECHNICA (Apr. 14, 2012), http://commcns.org/LbesMo.

[58] NFC Technology is based off of Radio Frequency Identification Tags ("RFID"), which allows for a reader to accept input from short distances. Examples of RFID use include: product tracking, passports, libraries, and animal identification. However, RFID only allows for one-sided communication. In the mid-1990s, Phillips and Sony in a joint venture developed NFC as a standard for two-way communication. *See* BOER & BOER, *supra* note 8, at 32-33; Crowe, *supra* note 42, at 1, 5.

[59] INNOVISION RESEARCH & TECH., NEAR FIELD COMMUNICATION IN THE REAL WORLD: TURNING THE NFC PROMISE INTO PROFITABLE, EVERYDAY APPLICATIONS 8 (2011), http://commcns.org/N5MZNV.

[60] *See* BOER & BOER, *supra* note 8, at 32-33.

phone, driver's license, credit cards, debit cards and information about recent purchases. Moreover, hackers may be able to steal transaction data "out of the air" or from the phone itself.[61] Though there are security issues that need to be addressed, NFC payments offer consumers more convenience with only minimally greater security threats than experienced with a normal credit card.[62]

III. GLOBAL IMPLEMENTATION OF M-PAYMENTS

While the United States has been preparing itself for the introduction of M-Payments, other countries have already embraced the technology for several years, including parts of Europe, Japan, and Korea.[63] Apart from M-Payments, NFC technology has been widely adopted as a useful method to identify persons, increase speed for transfers via Bluetooth, and facilitate transferring of small files such as business cards or contact information.[64]

A. Adoption of NFC and M-Payments in Europe and Asia

NFC implementation trials are currently underway in Europe. The United Kingdom has successfully adopted NFC technology for systems including their subway.[65] Wider adoption for M-Payments is in the works, as the European Union ("EU") attempts to create a multi-country system where mobile wallets will be able to be used interchangeably within the Single Euro Payment Area ("SEPA").[66] However, potential broadening of M-Payments has raised friction with EU privacy legislation, which requires that users must agree to each exchange of data.[67] Therefore, before the M-Payment can take place users must accept the communication from the POS terminal.[68]

---

[61] *See* Crowe, *supra* note 42, at 7.

[62] *Id.*

[63] STAMATIS KARNOUSKOS & ANDRIAS VILMOS, THE EUROPEAN PERSPECTIVE ON MOBILE PAYMENTS 2 (2004); SEAN CHOI ET AL., KPMG INT'L, MOBILE PAYMENTS IN ASIA PACIFIC 4 (2007).

[64] *Frequently Asked Questions*, NFC-FORUM, http://commcns.org/KZKJJX (last visited Apr. 21, 2012).

[65] James McDonald, *Contactless NFC Payment to Aid Boom in British Transport*, COMPUTER WORLD UK (Nov. 11, 2011), http://commcns.org/LPD3IE.

[66] SEPA encompasses all countries which are part of the EU and who have adopted the Euro as their official monetary unit. *See* CHOI, *supra* note 63, at 37.

[67] Kevin J. O'Brien, *E.U. to Tighten Web Privacy Law, Risking Trans-Atlantic Dispute*, N.Y. TIMES, Nov. 9, 2011, http://commcns.org/KE5xUX; David Ruddock, *PSA: California's New App Privacy Policy Requirement Just Made Life Harder For Developers Everywhere, Here's What You Need To Know*, ANDROID POLICE (Feb. 22, 2012), http://commcns.org/JKQ8FM.

[68] Mary Catherine O'Connor, *European Commission Issues Framework for Measuring and Mitigating RFID's Privacy Impact*, RFID J. (Apr. 6, 2011), http://commcns.org/K9E1St.

Conversely, Asian countries have seen more success with NFC and M-Payment implementation. Mobile payments were introduced to Asia in 1999 with the creation of Smart Money[69] in Japan.[70] Since their initial introduction, Korea, Thailand, India, Singapore, China, and Vietnam have adopted various forms of M-Payments,[71] which have been implemented in a variety of industries, including transportation, banking, telecommunications, retail, and media.[72] Today, the greatest usage of M-Payments occurs in Japan and Korea, who have systems in place to accommodate NFC mobile transactions.[73]

For several years, Asian countries have explored implementation of M-Payments in various forms.[74] M-Payment success in Japan in particular can be cited to NTT DoCoMo, a wireless company who subsidized the cost of NFC readers for merchants and entered the credit business by purchasing a bank.[75] Other countries, such as Hong Kong, Singapore, China, and India, have adopted various forms of M-Payments, for example SMS transactions and various mobile apps as secured payment.[76] The emergence of M-Payments in this densely populated region of the world is becoming increasingly important as mobile phone popularity and usage increases.[77]

In general, M-Payments in Asia have faced few regulatory challenges.[78] While both Japan and China make no specific guarantee of privacy in their Constitution,[79] Articles 16 and 18 of the Korean Constitution provide specific

---

See generally COMM'N OF THE EUROPEAN COMMUNITIES, COMMISSION RECOMMENDATION ON THE IMPLEMENTATION OF PRIVACY AND DATA PROTECTION PRINCIPLES IN APPLICATIONS SUPPORTED BY RADIO-FREQUENCY IDENTIFICATION (Dec. 5, 2009) (outlining suggested privacy objectives for use by the European Commission's 27 member states.).

[69] Smart Money in the Philippines introduced mobile payments for pre-paid cell phone service by allowing consumers to "re-load" their phones by sending a SMS. The SMS or text authorizes a linked account to release funds to pay for minutes on the specified phone. Michael Trucano, infoDev ICT and Social Sector Innovation Specialist, Presentation at Nigeria FSS 2020 Workshop: M-Banking, M-Remittances – Case Studies from the Philippines (Dec. 19, 2006), *available at* http://commcns.org/MVqxtk.

[70] *The History of Mobile Payments – How and Where It Started*, ELECTRONIC BANKING OPTIONS (Apr. 23, 2010), http://commcns.org/JKQvjw.

[71] *See* CHOI, *supra* note 63, at 4.

[72] *Id.* at 17 fig.5.

[73] *Id.* at 4.

[74] *Id.*

[75] *Id.* at 10.

[76] *See* CHOI, *supra* note 63, at 20.

[77] An Hodgson, *Regional Focus: Asia Pacific - The World's Largest Mobile Phone Market*, EUROMONITOR GLOBAL MARKET RES. BLOG (Mar. 10, 2010), http://commcns.org/KE6QTT.

[78] Most regulatory challenges to M-Payments in Asia have been financially related to ensuring prudential compliance and determining if wireless providers should be subject to financial regulation. *See* CHOI, *supra* note 63, at 29.

[79] *Caslon Analytic Privacy Guide: Asia and the Pacific*, CASLON ANALYTICS, http://commcns.org/JKQJaq (last visited Apr. 21, 2012).

protections for privacy.[80] South Korea has legislated further on privacy issues, ensuring that all personal information collected through e-commerce is protected and disclosed to consumers.[81] In recent years privacy concerns have gained prominence throughout the region and sparked the signing of regional declarations such as the 1995 Seoul Declaration[82] and the 1998 Singapore Declaration,[83] aimed at ensuring the free flow of information while protecting privacy and data security.

B. Adoption of NFC and M-Payments in the United States

Though NFC-enabled phones are now available in the United States,[84] a number of hurdles must be overcome for proximity M-Payments to become widely adopted.[85] Barriers to adoption include the high cost for merchants to invest in NFC capable readers, lack of consumer demand, and regulatory oversight concerns.[86] With the cost of NFC capable card readers exceeding $200 per reader, merchants are hesitant to upgrade to a payment form that currently services only 1.1% of the population.[87] Recently, however, payment giant Visa has provided incentives and pressured merchants to adopt NFC readers, setting a deadline of April 2013 for merchants to adopt NFC readers.[88]

Another barrier to adoption is the coordination and payment mechanisms by which proximity M-Payments will be processed. Specifically, the relationship between banks, card issuers, and mobile providers must be mapped out and implemented, ensuring that all parties agree on who is responsible for verifying

---

[80] DAEHANMINKUK HUNBEOB [HUNBEOB] [CONSTITUTION] art. 16-18 (S. Kor.).

[81] Pi, *PHR2006 – Republic of South Korea*, PRIVACY INT'L (Dec. 18, 2007), http://commcns.org/JyvreD; Act on the Protection of Personal Information Maintained by Public Institutions, Act. No. 4734, Jan. 7, 1994, art. 1,4 (S. Kor.); Act on Disclosure of Information By Public Agencies, Act No. 5242, Dec. 31, 1996, art. 1, 3, 5, 7 (S. Kor.). Specific laws pertaining to e-commerce privacy include: 1994 Act on the Protection of Personal Information Managed by Public Agencies, 1995 Act Relating to Use and Protection of Credit Information, 1996 Act on Disclosure of Information by Public Agencies and 1999 Basic Act on Electronic Commerce.

[82] Ministerial Statement, Asian-Pacific Econ. Cooperation Ministers, Seoul Declaration for the Asia Pacific Information Infrastructure (May 29-30, 1995), *available at* http://commcns.org/LBLSTz.

[83] *Id.*

[84] Casey Johnston, *P2P PayPal Payments Coming via NFC-Capable Phones*, ARS TECHNICA (Feb. 2, 2012), http://commcns.org/LC4IgQ.

[85] *See* Crowe, *supra* note 42, at 7-8.

[86] *Id.* at 17.

[87] This is according to a 2008 and 2009 Consumer Payment Choice Survey. *Id.* at 13, 19

[88] Currently card issuers absorb fraud liability for unauthorized purchases. Larry Dignan, *Visa Sets Deadlines on NFC Efforts,* CNET NEWS (Feb. 2, 2012), http://commcns.org/KpHyKo.

customer identification, resolving disputes, and handling customer service.[89] This is particularly important for mobile providers, who have never been involved in the financial service industry, as it likely would require much work to tackle the associated legal and regulatory issues.[90]

IV. PRIVACY AND CONSUMER PROTECTION LAWS IN THE U.S.

The U.S. has very thorough privacy legislation, due mostly to the fact that it is not specifically elucidated as a right enumerated in the Constitution.[91] While the First, Fourth and Ninth Amendments create the basis for privacy legislation, this area remains a highly litigious.[92] For instance, financial accounts initially were protected by the Fourth Amendment, which prohibits unlawful and unwarranted search and seizures.[93] However, the Supreme Court qualified this right by holding that information divulged by a customer to a bank employee does not fall within the shield of privacy, since the bank employee is a third party.[94] Though regulators have yet to specify which U.S. laws and regulations apply to M-Payments, they implicate many of the same laws and regulations as traditional payments.

A. The Electronic Funds Transfer Act and Regulation E

Congress passed the Electronic Funds Transfer Act ("EFTA") in 1978 to provide protection to consumers and define rights and responsibilities of participants in electronic fund transfer systems, which the Federal Reserve Board implemented the Act through Regulation E.[95] In doing so, the Board defined an electronic fund transfer ("EFT") as any transfer that is electronically initiated, including ATM transfers, debit card transactions, and direct deposits.[96] It also subjected "any bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a

---

[89] *See* Crowe, *supra* note 42, at 21.

[90] *Id.*

[91] U.S. CONST. amend. I. First Amendment rights have been interpreted to include privacy, although privacy is not explicitly mentioned in the Constitution. *See* Griswold v. Connecticut, 381 U.S. 479, 483 (1965).

[92] U.S. CONST. amend. IV; U.S. CONST. amend. IX; Andrew B. Serwin, *Poised on the Precipace: A Critical Examination of Privacy Litigation*, 25 SANTA CLARA COMPUTER & HIGH TECH L.J. 883, 884 (2009) (explaining the common law basis of privacy litigation and how the theories of cases has evolved to include data security).

[93] United States v. Miller, 425 U.S. 435, 439 (1979).

[94] *Id.* at 435.

[95] Electronic Fund Transfer Act, 15 U.S.C. § 1693 et seq. (2006); Regulation E, 12 C.F.R. § 205.3 et. seq. (2011).

[96] 12 C.F.R. § 205.3(b) (2011).

customer, or that issues an access device or indirectly holds an account belonging to a consumer" to Regulation E.[97] These institutions are required to disclose all terms and conditions regarding their financial charges and must limit consumer liability to $50 dollars for unauthorized transactions reported within two days and $500 dollars for transactions reported after two days.[98]

If a consumer uses a debit card to make an M-Payment, even though the debit card is linked to his or her phone, the bank that issued the card is still required to comply with Regulation E—it does not lose its status as a financial institution.[99] Less clear, however, is whether MPSPs are subject to Regulation E.[100] Regardless, PayPal already complies with Regulation E, providing "advance disclosure of changes to its service, follow[ing] specified error resolution procedures and reimburse[ing] consumers for losses above $50 from transactions not authorized by the consumer."[101]

There has also been no indication from the Federal Reserve Board regarding the application of Regulation E to wireless carriers.[102] Non-financial institution service providers that facilitate an EFT service, but do not hold the consumer's account (as would be the case with wireless providers), are subject to Regulation E if they issue a debit card or other access device to the consumer and have no agreement with the account-holding institution regarding such access.[103] To come under the umbrella of Regulation E, the Federal Reserve Board would have to classify mobile devices as access devices and the traveling of M-Payment data across wireless providers' networks as an EFT service.[104]

The purpose of subjecting these institutions to Regulation E, however, is "to prevent a situation in which the service provider fails to provide a Regulation E requirement, like a periodic statement, and the account-holding bank does not know to provide one because it has not contracted with the service provider."[105] With consumers signing up for M-Payment access through their bank, rather than their wireless provider, banks will know to provide Regulation E disclosures, likely freeing wireless providers from inclusion under Regulation E.[106]

---

[97] *Id.* § 205.2(i)
[98] *Id.* § 205.6(b)(1) and (2).
[99] *See* Taggart & Freese, *supra* note 14, at 491.
[100] *Id.*
[101] EBAY, ANNUAL REPORT 2009, at 29 (2009), http://commcns.org/LPFzyO. *See also* Taggart & Freese, *supra* note 14, at 491 (discussing how PayPal conducts business).
[102] *See* Taggart & Freese, *supra* note 14, at 491-92.
[103] 12 C.F.R. § 205.14(a)(1) and (2) (2011).
[104] *See* Taggart & Freese, *supra* note 14, at 491-92.
[105] *Id.* at 492.
[106] *Id.*

B. The Truth in Lending Act and Regulation Z

The Federal Reserve Board promulgated Regulation Z to govern credit card transactions following the passage of the Truth in Lending Act ("TILA") in 1968.[107] Regulation Z contains provisions governing to the resolution of credit card billing errors, limiting consumers' liability for unauthorized credit card transactions to $50, and requiring credit card issuers to make certain disclosure requirements.[108] As with debit card transactions, issuing banks are not free from complying with Regulation Z because a consumer links his or her credit card to an M-Payment account.

Similar to EFTA and Regulation E, the question again is whether MPSPs and wireless providers are subject to Regulation Z. The Federal Reserve Board has indicated that, when consumers purchase of goods over the Internet using M-Payment accounts linked to credit cards, the burden of resolving billing errors under Regulation Z is on the credit card issuers, not the MPSP.[109] Additionally, in 2006, twenty-eight state attorney generals sued PayPal over its customer service and fraud protection policies.[110] In settling the suit, PayPal explicitly agreed that it would not "advertise that its [p]ayments services give consumers the rights and privileges expected of a credit card transaction," except in cases where it actually was the credit card issuer.[111] Furthermore, PayPal's dispute resolution policy is narrower than Regulation Z's requirements. All these examples seemingly indicate that MPSPs are not subject to the full slate of Regulation Z provisions for facilitating M-Payments.[112]

It is similarly unlikely that wireless providers are, or will be, subject to Regulation Z. Though there is a question as to whether credit is being advanced when wireless subscribers download games or ring tones to their phone—in which case Regulation Z would apply—it has been noted that these transactions likely are governed by the Federal Communications Commission's Truth in Billing Requirements and state telecommunications

---

[107] Truth in Lending Act, 15 U.S.C. §§ 1601-1693 (2006); Regulation Z, 12 C.F.R. § 226 (2011).

[108] 12 C.F.R. §§ 226.6, 226.9, 226 .12, 226.13 (2011).

[109] Truth in Lending, 74 Fed. Reg. 5244, 5364-66. (Jan. 29, 2009) (Final Rule). *See* Truth in Lending, 75 Fed. Reg. 7925 (Feb. 22, 2010) (discussing the subsequent withdrawal of the January 2009 Final Rule because Regulation Z was amended by a further new rule due to provisions of the Credit Card Accountability Act).

[110] *Paypal Settles with States*, N.Y. TIMES, Sept. 29, 2006, http://commcns.org/JKRzDZ.

[111] Assurance of Voluntary Compliance or Discontinuance at 12(h)(i), *In re* PayPal, Inc., *available at* http://commcns.org/KpTwUo. *See also* Taggart & Freese, *supra* note 14, at 493 (discussing the terms that PayPal agreed to in the settlement).

[112] *See* Taggart & Freese, *supra* note 14, at 493.

regulators.[113] Unless the Federal Reserve Board specifically applies Regulation Z's provisions to wireless providers, these transactions likely will remain under the purview of telecommunications regulators.[114]

C. Gramm-Leach-Bliley Act

In order to ensure consumer protection and confidence in their financial privacy, Congress passed the Right to Financial Privacy Act of 1978 ("RFPA").[115] Legislated in direct response to *United States v. Miller*,[116] RFPA was specifically aimed at protecting consumers from government invasion of privacy. More recently, consumers have been provided with further protection in the form of legislation such as the Gramm-Leach-Bliley Act ("GLBA").[117]

GLBA was passed as part of a sweeping banking regulation reform.[118] In general, large banks, brokerages, and insurance companies supported the Act because it removed many banking barriers and allowed a single institution to act as a commercial bank, investment bank, and insurance broker.[119] In exchange for the de-regulation of financial institutions, consumer protection measures were added in the form of the financial privacy rule, safeguard rule, and pretexting protections.

1. Financial Privacy Requirement

GLBA's financial privacy requirement applies to all companies who have individual consumers that obtain its services.[120] This requirement differentiates between customers and consumers, with only customers receiving automatic privacy notices from the company.[121] The Federal Trade Commission ("FTC") has defined a customer as "a consumer who has a customer relationship with

---

[113] *Id.*

[114] *Id.*

[115] Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (1978) (codified at 12 U.S.C. §§ 3401-3422 (1982)).

[116] Matthew N. Kleiman, *The Right to Financial Privacy Versus Computerized Law Enforcement: A New Fight in an Old Battle*, 86 NW. U. L. REV. 1169, 1187 (1992).

[117] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in Titles 12 and 15 of the United States Code).

[118] R. Bradley McMahon, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why is Identity Theft the Most Prevalent Crime in America?*, 49 VILL. L. REV. 625, 634-35 (2004).

[119] Lawrence J. White, *The Gramm-Leach-Bliley Act of 1999: A Bridge Too Far? Or Not Far Enough?*, 43 SUFFOLK U. L. REV. 937, 937 (2010).

[120] This rule does not apply to companies obtaining data about companies, because company data is either public or will be governed by contractual obligations. 15 U.S.C. § 6802(a) (2006).

[121] *Id.* § 6802(a)-(b).

you . . . a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes," while a consumer is "an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative."[122] If an individual is deemed to be a customer rather than consumer, the financial institution must notify them of the company's financial privacy notice every year for so long as the relationship exists.[123] Given that mobile phone users usually have long-term contracts with their wireless provider, they would most likely fall under the FTC definition of customers, and if a company is considered a financial institution, they would need to abide by the financial privacy requirements of GLBA.

To be GLBA-compliant, companies who qualify as financial institutions must send customers a clear, conspicuous, and accurate statement of the company's privacy practices relating to non-public personal information.[124] Additionally, they must allow both customers and consumers an opt-out provision that will prevent the company from sharing any personal information with third parties.[125]

2. Safeguard Rule

GLBA's financial safeguard rule requires all companies that qualify as financial institutions to ensure the security and confidentiality of customer personal data such as name, address, phone number, account numbers, social security numbers, income, and credit histories.[126] The open-ended nature of the FTC's definition of a financial institution[127] has exposed a variety of industries to GLBA's safeguard rule, including banks, check cashing businesses, real estate appraisers, professional tax preparers, and courier services.[128] The fact that so many different industries have been subject to this definition seemingly indicates that wireless providers also will be subject to this rule if they become substantially involved in the operations of M-Payments and NFC technology.

---

[122] 16 C.F.R. § 313.3(e)(1), (h)-(i)(1) (2011).
[123] 15 U.S.C. § 6802(a)-(e) (2006).
[124] *Id.* § 6803(a).
[125] *Id.* § 6802(b).
[126] *Id.* § 6801(b).
[127] The FTC defines a financial institution, as "an institution that is significantly engaged in financial activities is a financial institution." FTC Privacy of Consumer Financial Information, 16 C.F.R. § 313.3(k)(1) (2010). *See also* FED. TRADE COMM'N, FTC FACTS FOR BUSINESS, FINANCIAL INFORMATION AND CUSTOMER INFORMATION: COMPLYING WITH THE SAFEGUARDS RULE 1 (2006), http://commcns.org/M2oqEZ.
[128] FTC Privacy of Consumer Financial Information, 16 C.F.R. § 313.3(k)(2) (2010).

To comply with the safeguard rule, each company must assess risks to customer information, create and monitor a safeguard program, and adjust the program as necessary.[129] Common components of safeguard programs include ensuring data security, training employees to be mindful of customer information, and disciplinary action for policy violation.[130] However, given that wireless providers already protect customer non-personal private information as required by the Telecommunications Act of 1996[131] and the CTIA Consumer Code,[132] it is unlikely that the safeguard rule would greatly affect providers that implement NFC technology.

3. Pretexting Protection

Under GLBA, Fraudulent Access to Financial Information, also known as the Pretexting Protection, requires financial institutions to safeguard against unauthorized access to personal accounts and information.[133] Pretexting includes account holder impersonation and "phishing scams."[134] To comply with this provision, companies must educate and train employees on procedures to ensure customer identity and recognize fraudulent access attempts.[135] Additionally, many companies are proactively educating customers on the dangers of phishing scams, how to detect scams, and warning customers of existing threats to personal information.[136] Since providers are already required to protect customer information from unauthorized users, they would need to change little to comply with this provision.

---

[129] FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.4 (2002). *See also* FED. TRADE COMM'N, *supra* note 127, at 2.

[130] *See generally* FED. TRADE COMM'N, *supra* note 127, at 2.

[131] 47 U.S.C. § 222 (2006). *See also* Telecommunications Act of 1996, Pub L. No. 104-104, 110 Stat. 149 (codified as amended in scattered sections of 26 U.S.C.).

[132] CTIA-THE WIRELESS ASS'N, CONSUMER CODE FOR WIRELESS SERVICE 4 (2011), http://commcns.org/KCwgRz. The CTIA Code signatories cover 97% of U.S. wireless subscribers and include the major wireless network operators such as: AT&T, Sprint, T-Mobile USA, and Verizon Wireless. *Consumer Code Participants*, CTIA-THE WIRELESS ASS'N, http://commcns.org/LC70wq (last visited Apr. 21, 2012).

[133] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6821-6827 (2006).

[134] *See generally* FED. TRADE COMM'N, FTC CONSUMER ALERT: HOW NOT TO GET HOOKED BY A 'PHISHING' SCAM (2006), http://commcns.org/MVsJ3V.

[135] FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.4 (2002).

[136] *See generally* Paul Roberts, *Paypal Users Warned of Spoof Site*, PCWORLD, (July 9, 2003), http://commcns.org/MVt0nJ; *Protect Yourself from Fraudulent Emails*, AM. AIRLINES, http://commcns.org/LbktIN (last visited Apr. 21, 2012); *Defending Against Fraud*, FEDEX, http://commcns.org/N5ZJEj (last visited Apr. 21, 2012); *Microsoft Security Advisory (2524375), Fraudulent Digital Certificates Could Allow Spoofing*, MICROSOFT, http://commcns.org/KCxCeS (last visited Apr. 21, 2012); *Fraud Protection Center*, AM. EXPRESS, http://commcns.org/N607To (last visited Apr. 21, 2012).

D. The Durbin Amendment

Effective October 1, 2010, The Durbin Amendment is part of the Consumer Protection Act of 2010.[137] The Amendment limits the amount banks may charge merchants for debit interchange fees to twenty-two cents and five basis points of the transactions value, which amounts to a nearly 50% reduction of the current average of forty-four cents per transaction.[138] The major difference between debit and credit cards is the transaction fees faced by retailers and banks.[139] In an online debit transaction, money is immediately accessed and drawn from the purchaser's account, providing less recourse for consumers than transactions completed through the credit system.[140] While the Durbin Amendment's purpose was to benefit consumers, it has faced criticism due to the fact that banks are passing on the lost revenue to consumers for using the debit function of ATM cards.[141]

The Durbin Amendment will most likely apply to M-Payments initiated through NFC technology if they are facilitated via an EFT transaction linked to a consumer's bank account. However, if M-Payments are implemented through means of a credit transaction, where the money would not be drawn immediately from the attached bank account, or through a pre-loaded card, the Durbin Amendment would not apply.[142]

---

[137] Consumer Protection Act of 2010, Pub. L. No. 111-203, 124 Stat. 2068 (codified in scattered sections of 15 U.S.C.).

[138] Federal Reserve System Debit Card Interchange Fees and Routing, 12 C.F.R. §235.3(b) (2011); Anisha, *Federal Reserve Issues Final Ruling on Durbin Amendment*, NERD WALLET (June 29, 2011), http://commcns.org/MVtjyI (last visited on Apr. 21, 2012).

[139] David A. Balto, *Creating a Payment System Network: The Tie that Binds or an Honorable Peace?*, 55 BUS. LAW. 1391, 1394 (2000).

[140] Daniel M. Mroz, *Credit or Debit? Unauthorized Use and Consumer Liability Under Federal Consumer Protection Legislation*, 19 N. ILL. U. L. REV. 589, 622 (1999).

[141] Richard A. Epstein, *Durbin's Folly: The Erratic Course of Debit Card Markets?*, 7 COMPETITION POL'Y INT'L 58, 59 (2011) (explaining that Bank of America, Wells Fargo, and several other banks offset any revenue loss from the Durbin price caps by raising the direct fees that they charged their own customers for debit card use).

[142] The Durbin Amendment only limits interchange rates applied to "electronic *debit* transaction[s]." 15 U.S.C. § 1693o-2(a) (Supp. IV 2010) (emphasis added). "[E]lectronic debit transaction means a transaction in which a person uses a debit card." *Id.* § 1693o-2(c)(5). The term "debit card" includes "any card, or other payment code or *device*, issued or approved for use through a payment card network to debit an asset account." *Id.* § 1693o-2(c)(2) (emphasis added). The interchange fee limitations do not apply to transactions using reloadable, general-use prepaid cards. *Id.* § 1693o-2(a)(7)(B). However, the exemption will expire after July 21, 2012. *Id.*

V. MOBILE PAYMENTS IN THE UNITED STATES

A. The Players

Financial institutions, such as banks or credit card companies, will play perhaps the biggest role in the proliferation of M-Payments. Many industry insiders believe that financial institutions will define the mobile payments and commerce space.[143] With a long history of handling payments and addressing customer authentication and authorization requests, financial institutions may be the best-situated to issue payment credentials and applications on mobile devices, similar to how they would with a physical credit card.[144] In fact, 56% of consumers place the most trust in their financial institution to handle mobile commerce financial data, compared with only 7% who trust retailers and 6% who trust their wireless provider.[145] This trust likely stems from the fact that 90% of consumers are concerned about data privacy and security in mobile transactions, and see financial institutions in the best position to address these concerns.[146]

Wireless providers and handset manufacturers will also play vital roles in the adoption of M-Payments. On November 2010, AT&T Mobility, Verizon Wireless, and T-Mobile USA announced the formation of a joint venture called ISIS in an attempt to create a standard for M-Payments.[147] The three wireless providers have pledged over $100 million to the joint venture, which has partnered with Visa, MasterCard, Discover, and American Express.[148] Handset manufacturers such as Samsung Electronics, Research In Motion and LG Electronics, also have embraced the new technology, making NFC-enabled

---

[143] Ryan Kim, *Mobile Payments: Financial Players Are in the Driver's Seat*, GIGAOM (Jan. 3, 2012), http://commcns.org/JSnzj1 (citing the results of mobile analyst Chetan Sharma's 2012 Mobile Industry Predictions Survey of 150 industry insiders).

[144] DARIN CONTINI ET AL., MOBILE PAYMENTS IN THE UNITED STATES MAPPING OUT THE ROAD AHEAD 7-8 (2011), http://commcns.org/K8AumM.

[145] Press Release, KPMG Int'l, KPMG's 5th Annual Global Consumer & Convergence Survey Confirms Trend of Accelerated Pace of Consumer Adoption of New Digital Business Models (Dec. 5, 2011), *available at* http://commcns.org/KXQ9Bb (citing results of KPMG's online survey of 9,600 consumers ranging in age from 16 to over 65, in 31 countries).

[146] *Id.*

[147] Press Release, T-Mobile USA, AT&T, T-Mobile and Verizon Wireless Announce Joint Venture to Build National Mobile Commerce Network (Nov. 16, 2010), *available at* http://commcns.org/LbllaY.

[148] Olga Kharif, *AT&T-Verizon-T Mobile Sets $100 Million for Google Fight: Tech*, BLOOMBERG BUSINESSWEEK (Aug. 29, 2011), http://commcns.org/JMdhmx; Mark Hachman, *Iris Carrier Venture Signs Payment Deals with Visa, MasterCcard, Others*, PC MAGAZINE (July 19, 2011), http://commcns.org/KZQreK.

phones available for consumer use.[149] However, an important debate between handset manufacturers and wireless providers is whether a consumer's payment data should be stored in the SIM card or on the phone's embedded chip.[150] If stored on the devices' SIM card, wireless providers keep control of the data; alternatively, if handset manufacturers build payment credentials directly in the phone's embedded chip, they can control the payment data.[151] Control of the data is particularly important because it allows the holder to partner directly with financial institutions and receive a larger portion of the revenue.[152]

Successful M-Payment adoption also depends on merchants. One major obstacle facing merchants has been the cost of new, NFC-enabled point-of-sale terminals, which is an estimated $200 per reader.[153] With estimates indicating that only 10% of mobile users will be actively using NFC payments by 2015,[154] and no guarantee that merchants will be able to send rewards or information about promotions to consumers' phones,[155] merchants are understandably reluctant to make such an investment despite pressure from Visa. Recently, however, VeriFone, a major seller of point-of-sale terminals, announced that it would include NFC technology in all of its new point-of-sale hardware, eliminating the need for merchants to make a determination as to whether NFC technology is worth the investment.[156]

---

[149] Mikael Ricknäs, *Visa Certifies Smartphones for NFC Payments*, PCWORLD (Jan. 10, 2012), http://commcns.org/KpKl6b. Google's Android mobile operating system also has NFC functionality built in. Ginny Mies, *Andoird 2.3 (aka "Gingerbread"): Hands-On*, PCWORLD (Dec. 9, 2010), http://commcns.org/KpKqGX. Apple also is expected to introduce NFC capabilities into future generations of the iPhone, which could compete with Isis and GoogleWallet. *See* Nick Bilton, *The Technology Behind Making Mobile Payments a Reality*, N.Y. Times, Mar. 21, 2011, http://commcns.org/LCawa2.

[150] Dan Butcher, *Who Owns the Paying Mobile Consumer: Carriers or Handset-Makers?*, MOBILE COMM. DAILY (Mar. 21, 2011), http://commcns.org/KXQEei.

[151] *Id.*

[152] *Id.*

[153] Peter Eichenbaum & Margaret Collins, *AT&T, Verizon to Target Visa, MasterCard with Smartphones*, BLOOMBERG (Aug. 2, 2010), http://commcns.org/KOuTA1. The incremental cost of manufacturing a mobile phone with NFC technology increases to $10-$15 per phone. *See* Crowe, *supra* note 42, at 7.

[154] Butcher, *supra* note 150.

[155] Eichenbaum & Collins, *supra* note 153. The incremental cost of manufacturing a mobile phone with NFC technology increases to $10-$15 per phone. *See* Crowe, *supra* note 42, at 19.

[156] *C. Wonder Launches with Entirely Mobile POS Service Using VeriFone GlobalBay Mobile and PAYware Mobile Enterprise Solutions*, VERIFONE, http://commcns.org/KEc8P5 (last visited Apr. 21, 2012). VeriFfone CEO Douglas G. Bergeron envisions NFC becoming standard in its POS terminals, "We find ourselves at the epicenter of the mobile payments revolution and the key enabler of the integration of new payment methods with the world's existing payment infrastructure." Christopher Brown, *VeriFfone to Include NFC in All New POS Terminals*, NFC WORLD (Mar. 3, 2011), http://commcns.org/LEfxLo.

Third party developers also are involved in the M-Payment system. Google has led the way with the development of Google Wallet, an application and payment system that allows consumers to pay using NFC and to store credit cards, loyalty cards, and gift cards.[157] Google Wallet works with MasterCard's PayPass system, allowing consumers to tap their phone on the PayPass reader in order to pay.[158] However, there are a number of drawbacks. First, Google Wallet is currently available only on one phone, Sprint's Samsung Nexus S 4G, and supports only two kinds of cards—Citi MasterCard credit cards and the Google Prepaid Card.[159] Additionally, as with other NFC options, merchants have been slow to adopt the PayPass system, making it difficult for consumers to actually use Google Wallet.[160]

In a rapidly evolving technological environment, consumers seek payment methods that are convenient, inexpensive, and secure.[161] A recent study showed that only 1.8% of global consumers are highly likely to adopt NFC payments immediately, while over half of consumers in most markets have no need for mobile payments due to existing alternatives.[162] In the United States, only 0.5% of consumers are highly likely to adopt NFC.[163] With a number of convenient options for payment currently available to consumers, successful NFC implementation in the United States will require some type of added value or incentive for consumers. Efforts to drive NFC payment adoption in other countries have included offering free phones to consumers,[164] adding cash to

---

[157] *Coming Soon: Make Your Phone Your Wallet*, OFFICIAL GOOGLE BLOG (May 26, 2011), http://commcns.org/JKUxIw. Google is just one of several technology companies, including Venmo, Square, and PayPpal, that are competing to replace traditional plastic credit cards with a digital substitute. Nick Bilton & Claire Cain Miller, *Google Wallet Makes Its Debut*, N.Y. TIMES, Sept. 19, 2011, http://commcns.org/JMfy11.

[158] *Get Google Wallet*, GOOGLE, http://commcns.org/KpLoTN (last visited Apr. 21, 2012). *See MasterCard PayPass: A Faster Way To Pay*, MASTERCARD, http://commcns.org/KOvS3e (last visited Apr. 21, 2012).

[159] *Google Wallet: How It Works*, INT'L BUSINESS TIMES (Sept. 20, 2011), http://commcns.org/KEcGoi.

[160] Sean Sposito, *Google Wallet to Require Investments in Terminals*, AM. BANKER (June 2, 2011), http://commcns.org/M2tmcK. Experts project that mobile payments are years away from mainstream use. Fahmida Y. Rashid, *NFC Mobile Payments Gain Momentum With New Partnership, Standards*, EWEEK (Nov. 23, 2011), http://commcns.org/KOwjuC.

[161] DARIN CONTINI ET AL., *supra* note 155, at 9.

[162] DATA MONITOR, NFC PAYMENTS: TAPPING THE FUTURE 2, 4 (2011). *See* Dan Balaban, *Report: Vast Majority of Consumers Will Need Push to Use NFC Payment*, NFC TIMES (July 6, 2011), http://commcns.org/JSq7xA. Although mobile payments may serve as a convenient alternative for consumers, they come at a higher cost than traditional payment systems. *See also* Sarah Bloom Raskin, Governor, Fed. Reserve Board, Remarks at the New America Foundation Forum: Economic and Financial Inclusion in 2011: What it Means for Americans and Our Economic Recovery (June 29, 2011).

[163] Dan Balaban, *supra* note 162.

[164] Sarah Clark, *Citi's Bangalore trial: Offering cardholders phone subsidies can kickstart NFC transaction volumes*, NFC WORLD (Mar. 11, 2010),

prepaid M-Payment accounts,[165] and introducing contactless-mobile couponing.[166] New features, as simple as integration of rewards points, coupons, and cards on the mobile device, as is possible with Google Wallet, may be enough to drive adoption among U.S. consumers. [167]

B. Execution Scenarios

Several business models have been proposed regarding the implementation of contactless M-Payments, each of which will require stakeholders to have a different role and therefore be affected by privacy and consumer protection laws differently.[168] The simplest model from a regulatory standpoint would have financial institutions, which already must adhere to the majority of the applicable law, leading M-Payment execution. Visa has been the leading financial institution in the M-Payment market with its payWave application.[169] Recently, Visa certified a number of new phones from Samsung Electronics, LG Electronics and Research In Motion, for use with payWave.[170] These phones "host the Visa payWave application on a secure SIM card and feature NFC (Near Field Communication) technology."[171] American Express has also forayed into the M-Payment space by partnering with both Sprint and Verizon Wireless to support its mobile digital wallet application, Serve.[172] Serve combines payment options into a single account, funded from a bank account, debit card, credit card, or another Serve account.[173] Customers can use Serve to make purchases at American Express participating merchants, paying their mobile bill, and redeem offers on goods and services.

The issue with this model is the level of cooperation between financial institutions and wireless providers. At the very least, financial institutions will

---

http://commcns.org/Kq62TV.

[165] Sarah Clark, *UK gets first commercial NFC service with Quick Tap from Orange and Barclaycard*, NFC WORLD (May 20, 2011), http://commcns.org/LBRqgJ.

[166] Sarah Clark, *NTT Docomo partners with Korea's KT to switch to NFC at end of 2012*, NFC WORLD (Feb. 9, 2011), http://commcns.org/KCCsJj.

[167] Joe Casabona, *Google Wallet Makes Payments Truly Mobile*, APP STORM ANDROID (Jan. 20. 2012), http://commcns.org/LbpDEM.

[168] CYNTHIA MERRITT, FED. RESERVE BANK OF ATLANTA, MOBILE MONEY TRANSFER SERVICES: THE NEXT PHASE IN THE EVOLUTION IN PERSON-TO-PERSON PAYMENTS 9-11 (2010), http://commcns.org/KToqju.

[169] *Frequently Asked Questions*, VISA, http://commcns.org/LEh7N5 (last visited Apr. 21, 2012).

[170] Press Release, Visa Inc., Visa Certifies Smartphones for Use as Visa Mobile Payment Devices (Jan. 10, 2012), http://commcns.org/KToEa8.

[171] *Id.*

[172] *American Express and Sprint Collaborate to Promote Serve*, Bus. WIRE (July 18, 2011), http://commcns.org/KZTFz4.

[173] *How Serve Works*, SERVE, http://commcns.org/K9NlG2 (last visited Apr. 21, 2012).

require wireless provider to assist them in reaching out to potential M-Payment customers. Moreover, consumers likely will look to their specific wireless provider if there are any issues making M-Payments. As the ISIS joint venture indicates, providers are investing heavily in NFC technology and rollout, making it likely that they will be reluctant to cede so much control over the process—and the revenues—to financial institutions.

Wireless providers would lead another possible business model, which has achieved success in Japan. Thus far, ISIS has partnered with handset manufacturers such as HTC, LG Electronics, Motorola Mobility, Research In Motion, Samsung Electronics, and Sony Ericsson to develop devices using the joint venture's NFC technology standard.[174] The joint venture has also partnered with the four major credit card companies—American Express, Discover, MasterCard, and Visa—to give consumers ubiquitous payment options, as well as digital security company Gemalto to oversee the transfer of payment credentials from banks and payment services to the ISIS application.[175]

ISIS has been successful in joining together the competing entities—wireless providers, handset manufacturers, and financial institutions—on the provider side, but a number of roadblocks remain before the venture can achieve success in the United States. The provider-led model has been adopted in Japan in large part because communications giant DoCoMo acquired a bank, which allowed it to vertically integrate the M-Payment process.[176] Putting aside the antitrust issues associated with a wireless provider acquiring a financial institution, the strict regulatory barriers that providers would face as a financial institution would make such an acquisition impractical.[177] While ISIS offers a more realistic partnership approach, issues such as regulatory burdens, the division of responsibilities, and the sharing of profits remain unsettled.[178] With each of these groups attempting to take advantage of the revenue potential that comes from enabling CM-Payments, it is hard to imagine any of them relinquishing a large share of the profits.

---

[174] Roger Cheng, *Isis Mobile-Payment Group Lines Up Handset Backers*, CNET NEWS (Sept. 27, 2011), http://commcns.org/K9Nrxh.

[175] *Isis Forms Relationships with Visa, MasterCard, Discover and American Express*, BUS. WIRE (July 19, 2011), http://commcns.org/K9NAkh.

[176] *See* Crowe, *supra* 42, at 9-11.

[177] *Id.* at 10.

[178] Erin F. Fonté, COX SMITH MATTHEWS INC., MOBILE BANKING/MOBILE PAYMENTS 2012: HOT TOPICS FOR FINANCIAL INSTITUTIONS, VENDORS AND THIRD-PARTY PAYMENT PROVIDERS (Jan. 23, 2012), http://commcns.org/K8EyTX.

VI. LEGISLATIVE AND REGULATORY RECOMMENDATIONS FOR M-PAYMENT IMPLEMENTATION

There is no clear answer on who will be responsible for regulatory oversight of M-Payments given the numerous industries required to work together. Currently, the Federal Deposit Insurance Corporation ("FDIC"), Federal Reserve Board, and Office of Comptroller of the Currency ("OCC") regulate financial institutions, while the Federal Trade Commission ("FTC") and the Federal Communication Commission ("FCC") are the main regulators of wireless providers.[179] The newly created Consumer Financial Protection Bureau ("CFPB") has also committed to filling the gaps in legislation and regulatory oversight to ensure widespread adoption of M-Payments.[180]

Some industry leaders have argued that it is incumbent upon all stakeholders in the M-Payment system to ensure the privacy of customer data and that market forces should be allowed to work freely.[181] However, consumer trust is essential to the success of this system; given the financial market failures of the last few years and the continual complaints of wireless bill shock, it is unlikely that consumers will all of a sudden trust the players in the M-Payment system.

As a result, amendments to existing financial protection acts, such as Regulation E and TILA, should be made to include M-Payment transactions. Doing so would be an important step in creating consumer confidence in the payment form, which will in turn lead to a greater level of adoption. Additionally, these amendments will provide a clearer framework for mobile-payment implementation amongst key stakeholders such as wireless providers and financial institutions.

VII. CONCLUSION

The future growth of M-Payments in the United States appears promising, given technological advances and the potential value added to customers. In order for customers to adopt m-payments it will be important for the government to "fill-in gaps" relating to privacy and consumer protection laws. The best way to do this would be to amend statute language to include M-Payments within the statutory scope.

Furthermore, the M-Payment business model must be solidified in order for stakeholders, such as merchants, customers, and financial institutions to fully support m-payment adoption. The best business model would allow for

---

[179] *See* Crowe, *supra* 42, at 29.

[180] *Consumer Financial Protection Bureau Launches Nonbank Supervision Program*, PYMNTS.COM (Jan. 5, 2012), http://commcns.org/L1hHGm.

[181] *See* discussion, *supra* Part V.A.

wireless providers to act as an intermediary between customers, financial institutions, and the card issuer. The reason why this would be the best method is because financial regulations are extremely onerous and would be timely and costly for wireless providers adhere to. Wireless providers are already required to be compliant to several provisions of GLBA relating to protection of customer personal data.

The potential of M-Payments to add value to customers seeking to eliminate their wallets and increased revenue to merchants and other stakeholders is driving the U.S. towards adopting m-payments. Even more important is that this payment method can be adopted smoothly and with little effect to consumers' protection and privacy protection if proper legislative holes are preemptively addressed.