MOBILIZING PAYMENTS: BEHIND THE SCREEN OF THE LATEST PAYMENT TREND

Brianna L. Reed*
I. INTRODUCTION

The mobile phone has evolved from a modest 2.2 pound device designed solely for telephonic communication\(^1\) to a five ounce “smartphone” capable of web browsing, utilizing GPS services, taking pictures, streaming video and music media files, text messaging, running complex software applications, and more.\(^2\) On a separate but similar trajectory, payment systems have evolved from simple specie-based and paper currency, to note transfers, deposit-account transfers, and now electronic payment systems.\(^3\) The technologies of mobile telephones and payment systems are still evolving but also merging, creating the phenomenon known as “mobile payments,” or “m-payments.”\(^4\) Mobile payments enable consumers to make purchases via text message or through any number of downloaded applications designed specifically for a mobile phone.\(^5\) The technology of mobile payments will eventually allow consumers to leave behind their traditional leather wallets, enabling a full spectrum of purchases to be made with credit card accounts, bank accounts, gift certificates, and

---


\(^{2}\) See id. at 333 (identifying the key capabilities of the iPhone).


\(^{4}\) See Matthew Gross, Consumers and Mobile Financial Services, FEDERAL RESERVE BOARD DIVISION OF CONSUMER AND COMMUNITY AFFAIRS, 1 (Mar. 2012), archived at www. perma.cc/U26T-4VNU (showing how mobile devices are becoming tools used by consumers for various electronic banking purposes); see also Mobile Payments - A Growing Threat, BUREAU OF INT’L NARCOTICS AND L. ENFORCEMENT AFF. (Mar. 2008), archived at www.perma.cc/K3KT-BXJU (claiming mobile payment development is pushed by the “convergence of the financial and telecommunications sectors”).

\(^{5}\) See Michelle Jun, Mobile Pay or Mobile Mess: Closing the Gap Between Mobile Payment Systems and Consumer Protections, CONSUMERS UNION, 1 (June 2011), archived at www.perma.cc/SWA9-AHP6 (defining what a mobile payment entails).
pre-paid stored value accounts — all accessed through the mobile phone device.\textsuperscript{6}

The creation of the digital wallet through the emergence of mobile payment systems is slated to fundamentally change the way American consumers make daily purchases because of the convenience and efficiency of these systems.\textsuperscript{7} An estimated 87\% of the United States population owns a mobile phone and this population usually carries their mobile phone in their possession, so the ability to pay through a mobile phone would greatly simplify the life of the average American by eliminating the need to carry a wallet.\textsuperscript{8} Mobile payment systems will also create changes for financial institutions, merchants, wireless service providers, and mobile software developers, who will all be working behind the screen to protect their own in-


\textsuperscript{7} See Fost, supra note 6 (examining consumer behavior and positing that the “convenience of whipping out your phone as a payment mechanism” is the driving force behind the implementation of mobile payment systems); Melissa Fox, The Evolution of Alternative Payments: A Look Back, A Look Forward, 13 NO. 5 ELEC. BANKING L. & COM. REP 1, 1 (2008) (showing that the history of payments reveals that consumers like to have choices in payment methods). This Note is focused on mobile payments and not mobile banking, which is the process of using a mobile phone to check bank account balances and perform other online banking functions. Hearing before the Subcommittee on Financial Institutions, supra note 6, at 4 (describing the difference between mobile payments and mobile banking).

\textsuperscript{8} See Aaron Smith, Smartphone Update, PEW RESEARCH CENTER (Mar. 1, 2012), archived at www.perma.cc/D8F-LW3L (detailing smartphone and mobile phone ownership statistics in the U.S.); Assemb. B. 786, 2013-14 Reg. Sess. (Cal. 2013) (describing the Money Transmission Act relating specifically to electronic payment transfers); Don Kohlz & Matt Churchill, Cell Phone Forensics: The New Evidentiary Gold Mine, 34 SEP MONT. LAW. 5 (2009) (claiming the cell phone to be one of the items “most of us” take with us upon leaving our homes); Fost, supra note 6 (predicting that consumers would prefer to take two items with them upon leaving home, their keys and their cell phones, rather than three items, which would include a wallet).
stitutions and their customers against unauthorized payments, fraudulent transactions, mistakes, privacy leaks, and programming bugs and glitches.  

Mobile payments, or “m-payments,” have been successfully implemented in Asia, but have yet to infiltrate the U.S. economy in a real, prevalent way. This Note will examine which current regulations might apply to mobile payment systems, where gaps in the law remain even if these regulations do apply, and what protections mobile payment systems might offer to consumers and financial institutions under the current state of the law. This Note will contend that before m-payment systems achieve proliferation in the United States, legislators need to act to create a regulatory scheme that specifically addresses mobile payment systems because the existing regulatory scheme will be unable to successfully govern the industry. Part Two examines the development of various types of mobile payment systems, as well as the development of the regulations that govern existing payment systems. Part Three discusses the most promising forms of mobile payment systems likely to be adopted in the U.S. and the current regulations that would appear to apply to these systems if

---

9 See Timothy McTaggart & David Freese, Regulation of Mobile Payments, 127 BANKING L. J. 485, 487 (2010) (discussing the different “stakeholders” involved in mobile payment systems); H. Paul Leyva, M-Payment: A Threat To Anti-Money Laundering, 34 VT. B. J. 62, 64-65 (2008) (describing all that can go wrong with mobile payment systems).

10 See McTaggart & Freese, supra note 9, at 485 (stating that m-payments have been prevalent in Asia since “early last decade” and listing reasons for why such payment systems have not been thoroughly developed in the U.S.). Hearing before the Subcommittee on Financial Institutions, supra note 6, at 2 (predicting the size that mobile payments could reach in the near future). This Note is focused on the initiation of mobile payments, where a consumer holds a phone over an access device in order to pay for a purchase; the acceptance of mobile payments, where a mobile phone device is used to accept payment cards, is a separate subject. See Hearing before the Subcommittee on Financial Institutions, supra note 6, at 6 (discussing the differences between initiatives of mobile payments versus acceptance).

11 See infra Part V (concluding that there are still gaps in the existing mobile payment system).

12 See infra Part V (suggesting an update to existing legislation is needed in the field of mobile payment systems).

13 See infra Part II (discussing the background and history of mobile payment systems).
adopted by consumers. Part Four argues that the regulatory framework currently in place is insufficient to properly regulate mobile payments in a manner that protects as well as incentivizes consumers and financial institutions to undertake its adoption, and proposes steps that would adequately address the unique concerns for financial institutions and consumers that are raised by mobile payment systems.

II. HISTORY

A. Models of Mobile Payment Systems

There are two primary models for mobile payment systems. One model is the “remote m-payments” model, in which a cellular phone’s text messaging capability (SMS, or “short messaging service”) is used to send credit or debit card information to the merchant. Under this model, the consumer first creates an account with a mobile payment service provider (MPSP), and links a financial account to the MPSP account. Then, through a series of text messages back and forth between the consumer and the MPSP, the specified dollar amount is transferred to the receiver’s account. Examples of remote m-payment models include systems such as PayPal, Facebook (for purchasing Zynga virtual goods), ringtone purchases made from wireless carriers, and donations made to the American Red Cross for

---

14 See infra Part III (outlining the facts and premises that contribute to the analysis of mobile payment systems).
15 See infra Part IV (identifying the scope of this notes analysis section).
16 See Rajan, supra note 6, at 447 (stating that m-payments come in two “main” forms).
17 See Rajan, supra note 6, at 447 (giving this mobile payment system model its name); Kevin Killoran, How Remote Mobile Payment Works and the Different Options, RETAIL SALES, MARKETING & MGMT. (Aug. 2, 2011), archived at www.perma.cc/GP6P-45DQ (describing how a remote m-payment model works).
18 See McTaggart & Freese, supra note 9, at 488 (outlining the steps involved in utilizing the remote m-payment model).
19 See McTaggart & Freese, supra note 9, at 488 (detailing the back and forth process involved in utilizing an MSPS payment system).
the Haiti earthquake relief by charging an amount to a wireless carrier bill.\textsuperscript{20}

The second mobile payment model, named the “proximity m-payment” model, is the format most attractive for consumers.\textsuperscript{21} This model enables contactless payments for goods and services; the consumer waves the device near a “reader” and account information is wirelessly transmitted to the merchant or receiver.\textsuperscript{22} The proximity m-payment model utilizes near field communication (NFC) technology, which involves an NFC chip installed in the mobile phone that communicates with a point of sale terminal to authorize account transfers from consumer to receiver when the chip is waved in front of the point of sale terminal.\textsuperscript{23} Examples of proximity m-payment models include systems such as the recently launched Google Wallet service as well as Bling Nation.\textsuperscript{24}

The main differences between the remote m-payment model and the proximity m-payment model center on the technologies required for their use, and the conveniences and risks each model poses to the consumer and financial institution.\textsuperscript{25} The choice of which mobile

\textsuperscript{20} See McTaggart & Freese, supra note 9, at 488 (listing ringtone purchases made from wireless carriers as an example of a remote m-payment); Jun, supra note 5, at 3-5 (naming American Red Cross donations and Facebook as examples of remote m-payments); Rajan, supra note 6, at 448 (listing PayPal as an example of an MPSP remote m-payment service).

\textsuperscript{21} See Rajan, supra note 6, at 449-50 (claiming that proximity m-payments have the “most potential to impact consumers”); Hearing before the Subcommittee on Financial Institutions, supra note 6, at 1 (claiming that most consumers believe that making a mobile payment involves waving a smartphone at a cash register).

\textsuperscript{22} See Killoran, supra note 17 (summarizing the process of the proximity model payment model).

\textsuperscript{23} See McTaggart & Freese, supra note 9, at 486-87 (detailing how remote m-payments work through a typical purchase); Rajan, supra note 6, at 450 (simplifying the process of how remote m-payments work).

\textsuperscript{24} See Gross, supra note 4, at 3 (listing Google wallet as an example of a launched NFC technology service); Jun, supra note 5, at 4 (describing Bling Nation as employing similar technology to complete proximity m-payments). Bling Nation is a payment system that employs an RFID-enabled sticker used at point-of-sale terminals by waving the sticker in front of the RFID reader. See Jun, supra note 5, at 4 (detailing the technology that Bling Nation employs).

\textsuperscript{25} See McTaggart & Freese, supra note 9, at 488 (noting one distinction between remote payments and proximity payments as the proximity payments requirement of a POS terminal); Rajan, supra note 6, at 452-53 (pointing to the ease of waving the device to make a payment as being “incredibly attractive”); Jun, supra note 5, at
payment system to use may hinge on the types of technology a consumer has access to; remote m-payment models require no more than a SMS capable phone and a cellular signal (which nearly all mobile phones currently in circulation have), while proximity m-payment models require a point of sale terminal as well as an NFC equipped mobile phone. Remote m-payment system security risks include lack of encryption checks (information is sent in plain text) and lack of authentication protocols, leaving a consumer vulnerable to imposters and hackers. Proximity m-payment system security risks include a heightened vulnerability to identity theft, as stealing a person’s physical phone would now be equivalent to stealing their entire wallet, because there would be no additional authentication procedures other than entering the mobile phone’s own password if the owner has even established one, and the risk of hackers stealing information “out of the air” while account information is transferring.

B. Regulations that Apply to Existing Payment Systems

A variety of laws and regulations designed to protect consumer privacy apply to the traditional existing payment systems in the United States, such as payment by check, credit card, debit card, and online payments. This Note specifically examines the regulations that may have a possible connection to mobile payments. The Federal Reserve Board of Governors regulates the commercial banking

6-14 (listing in descending order of consumer risk the different m-payment models).

26 See Rajan, supra note 6, at 450-52 (enumerating the technological hardware requirements for both the remote m-payment model and proximity m-payment model).

27 See Rajan, supra note 6, at 451 (identifying the security risks associated with remote m-payment systems).

28 See Rajan, supra note 6, at 452-53 (discussing the trauma that would be involved in losing a mobile phone if the phone was also proximity m-payment capable); Marianne Crowe et al., Mobile Payments in the United States at Retail Point of Sale: Current Market and Future Prospects, No. 10-2 FED. RES. BANK OF BOS., at 7 (2010), archived at www.perma.cc/6T8H-2CNE (noting a unique risk associated with proximity m-payment systems that differs from security concerns accompanying traditional payment systems of debit and credit cards).

29 See McTaggart & Freese, supra note 9, at 489 (introducing a discussion of laws and regulations that apply to “traditional” payments).
system of the United States.\textsuperscript{30} The Federal Reserve Board is authorized, implicitly and explicitly, to develop rules that give specificity to federal statutes.\textsuperscript{31} Therefore, the Federal Reserve Board serves as a primary authority in determining the regulation of payment systems, and through decisions and comments the Federal Reserve Board has the power to link and apply specific federal statutes to mobile payment systems.\textsuperscript{32}

Regulations are in place to properly protect consumers who are transferring very sensitive financial information through currently existing payment systems.\textsuperscript{33} The Electronic Funds Transfer Act\textsuperscript{34} and Regulation E\textsuperscript{35} govern fund transfers executed electronically from (and to) a consumer’s financial institution account.\textsuperscript{36} Consumer liability for unauthorized transfers is limited by Regulation E: if the unauthorized transaction is reported within two days, the consumer can only be held liable for up to $50, and if reported within sixty days, maximum consumer liability is $500.\textsuperscript{37} Additionally, the financial institution that holds the consumer’s account is required to disclose the terms and conditions for financial charges.\textsuperscript{38} Financial institu-


\textsuperscript{31} See Norman Silber, Why the U.C.C. Should Not Subordinate Itself to Federal Authority: Imperfect Uniformity, Improper Delegation and Revised Section 3-I02(C), 55 U. PITT. L. REV. 442, 449 (1994) (stating Congress either explicitly or implicitly delegates rulemaking authority to the Federal Reserve Board, which then allows the Board to develop their specific rules and fill gaps).

\textsuperscript{32} See id. at 449 (describing the power of the Board to fill in the details and detailing where this power derives from and how it has been confirmed by the Supreme Court).

\textsuperscript{33} See 15 U.S.C. §§ 1693(a) – (r) (2010) (inferring that the purpose of regulations such as this one are to protect consumers).

\textsuperscript{34} See id. (providing a framework for the rights, liabilities, and responsibilities of all of the players involved in electronic payments systems).


\textsuperscript{36} See McTaggart & Freese, supra note 9, at 490 (describing one piece of the legal landscape surrounding payment systems in the U.S.).

\textsuperscript{37} See 12 C.F.R. § 205.6(b) (2014) (enumerating consumer liabilities for unauthorized electronic fund transfers occurring on an account).

\textsuperscript{38} See id. (listing the differences in liability in relation to the time frame of when the unauthorized transaction is reported by the consumer).
tions that are required to comply with Regulation E include “bank[s], savings association[s], credit union[s], or any other person[s] that directly or indirectly [hold] an account belonging to a consumer, or that [issue] an access device… to provide EFT services.” A device that triggers protection by Regulation E can be any “card, code, or other means of access to a consumer’s account…that may be used by the consumer to initiate electronic fund transfers.” In comment 20a-1 to Regulation E, the Federal Reserve Board chose to explicitly apply one section of Regulation E to any “device with a chip or other embedded mechanism that links the device to stored funds, such as a mobile phone.” While this action shows an inclination by the Federal Reserve Board to allow mobile payments to trigger Regulation E protection, the Board has since made no other explicit applications of Regulation E requirements to mobile payments. However, PayPal Mobile voluntarily assumed all of the responsibilities of Regulation E, independent of any specific governmental application of the requirements to the service. This could indicate a willingness of the mobile payment industry to self-identify, but this self-imposed regulation lacks any real consumer enforcement power.

The credit card is now a staple in the field of modern payment systems and fully embraced by consumers as a traditional form of payment. Credit card systems are regulated by the Truth-in-Lending Act and Regulation Z. Credit card companies are re-

39 See 12 C.F.R. § 205.2(i) (2014) (listing the various types of financial institutions that are subject to the Regulation E requirements).

40 See 12 C.F.R. § 205.2(a)(1) (defining the term “access device”).


42 See McTaggart & Freese, supra note 9, at 490-91 (noting the specific application to mobile payments present in comment 20a-1, as well as the lack of specific mention of mobile payments under the rest of Regulation E requirements).

43 See McTaggart & Freese, supra note 9, at 491 (explaining PayPal’s assumption of duties under Regulation E).

44 See Credit Card Ownership Statistics, STATISTIC BRAIN (July 24, 2012), available at www.perma.cc/8NG3-EVRD (noting how widely used credit cards are as a payment system).

required to make initial and continuous disclosures to their customers regarding charges, fees, and terms. Regulation Z’s provisions also govern billing errors and consumer liability for unauthorized transactions. Regulation Z explicitly applies to “each individual or business that offers or extends credit” when that credit is regularly extended to consumers and subject to financing. When a credit card is involved in the transaction, the provisions of Regulation Z will apply even if the credit is not subject to financing. There is currently no explicit application of Regulation Z’s requirements to mobile payment systems by the Federal Reserve Board.

Incidental to effectuating payments is the transfer of the confidential information by consumers; The Gramm-Leach-Bliley Act (GLBA) protects the privacy of non-public customer information held by a financial institution. Protections for consumers under the GLBA include the “financial privacy rule, safeguard rule, and pre-texting protections.” The “Financial Privacy Rule” requires financial institutions to disclose policies regarding the privacy practices of the institution that affect customer non-public information, and also

47 See 12 C.F.R. § 226.1(a) (2011) (explaining the issuance of Regulation Z was designed to implement the Federal Truth-in-Lending Act).
48 See 12 C.F.R. § 226.6 (2011) (listing the initial disclosure requirements of credit issuers); 12 C.F.R. § 226.9 (2011) (listing the subsequent disclosure requirements after the initial disclosure).
51 See 12 C.F.R. § 226.1(c)(2) (2011) (detailing the extensive coverage that applies when a credit card, as opposed to another form of credit, is used for the transaction).
52 See McTaggart & Freese, supra note 9, at 492 (noting the Federal Reserve Board’s silence on whether Regulation Z would apply to the m-payment chain).
55 See Rajan, supra note 6, at 459-61 (listing the consumer protection measures enumerated by the Gramm-Leach-Bliley Act).
requires offering consumers an “opt out” option. The “Safeguard Rule” mandates that financial institutions enact standards to ensure the security of their customers’ personal information. The “Pretexting Protection” obligates financial institutions to train employees in order to better safeguard against security breaches resulting in unauthorized access to customer accounts, including account holder impersonation and scams involving “phishing.” The term “financial institution” is defined as “any institution the business of which is engaging in financial activities.” The Federal Reserve Board has not expressly connected or applied the GLBA to mobile payment systems or the new players involved in mobile payment systems, like wireless service providers or mobile application developers who will likely gain access to sensitive customer information if customers adopt mobile payment systems.

Fluid movement of information related to financial accounts and personal identification will always be accompanied by attempts to access and use this information for illegal purposes. The USA Patriot Act of 2001 requires financial institutions to develop and im-

---

56 See 15 U.S.C. § 6803(a) (2006) (requiring companies to send customers “a clear and conspicuous disclosure” at the time the relationship is established of the institution’s privacy practices).
58 See 15 U.S.C. §§ 6821 – 6827 (1999) (establishing the requirements to protect against fraudulent access to financial information); Lauren L. Sullins, “Phishing” for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft, 20 EMORY INT’L L. REV. 397, 397-98 (2006) (defining phishing as a type of digital identity theft through the use of fraudulent e-mails tricking recipients into revealing personal information of themselves or their customers over the Internet or through other digital means).
59 See 15 U.S.C. § 6809(3)(a) (1999) (defining, in general, financial institution); see also Rajan, supra note 6, at 460 (describing this definition as “open-ended”).
60 See McTaggart & Freese, supra note 9, at 495 (noting that Congress, the Federal Reserve Board, nor the courts have made explicit the GLBA application to mobile payment systems).
61 See Could Online Hackers Steal Your Cash, BANKRATE (Mar. 19, 2014), archived at www.perma.cc/YNL6-GVC8 (stipulating that online accounts need to be protected from hackers and online crooks).
plement a variety of standards and procedures designed to prevent and detect suspicious activity and money laundering. Financial institutions covered by the USA Patriot Act include banks, credit unions, broker-dealers, check cashers, money transmitters, pawnbrokers, casinos, and more. M-payment systems allow for new forms of exploitation and money laundering, yet there are currently no specific requirements regarding regulation of m-payments by financial institutions under the USA Patriot Act, and mobile application developers are under no requirement to implement precautionary mechanisms into their applications. Absence of specific requirements leaves the budding industry particularly vulnerable to attack by criminals.

III. FACTS

The implementation of mobile payment systems in the United States creates two primary concerns for consumers, financial institutions, and legislators; security breaches that may arise 1) when a mobile phone is separated from its true owner, and 2) when sensitive information is transferred from a mobile phone to a merchant. There is no express application of the existing payment system regulations to mobile payment systems by legislators or regulators and there are no laws or regulations that have been created to specifically govern mobile payments; this leaves the primary concerns raised by mobile government’s ability to use electronic surveillance domestically in the name of public safety).

64 See McTaggart & Freese, supra note9, at 495 (listing the institutions included in the financial institution definition of the USA Patriot Act).
65 See Leyva, supra note 9, at 64 (discussing the criminal possibilities resulting from mobile payment systems); Patriot Act of 2001, 115 Stat. 272 (lacking any mention of mobile payment systems or mobile payment application developer responsibilities).
66 See Leyva, supra note 9, at 64 (positing that if m-payments remain unregulated criminals will have new means of laundering money and funding terrorist schemes).
67 See McTaggart & Freese, supra note9, at 489 (stating the two primary security concerns of mobile payment system models).
payment systems unresolved.\textsuperscript{68} However, if mobile payments are analyzed as a traditional payment effected with a new form of technology through a new access device, some of the existing regulations surrounding other payment systems could possibly be applicable to m-payments.\textsuperscript{69} The following discussion examines which current regulations would most likely apply to mobile payment systems and what protections mobile payment systems offer to consumers and financial institutions under the current state of the law.\textsuperscript{70}

If Regulation E were found to be applicable to mobile payment systems, consumers would benefit from protection for mobile payments made through linkage to debit cards or bank accounts.\textsuperscript{71} In the event of a stolen phone or the interception or manipulation of financial information, consumer liability would be limited to $50 for unauthorized transactions reported within two days, and $500 for transactions reported after two days.\textsuperscript{72} However, adding a new form of payment technology covered by Regulation E also means that banks and financial institutions take on additional liabilities.\textsuperscript{73} While consumers would benefit from the application of Regulation E to mobile payments, banks would become increasingly exposed to losses, as consumers would now have multiple access devices linked to the same account, doubling the opportunities for unauthorized transactions.\textsuperscript{74}

\textsuperscript{68} See McTaggart & Freese, supra note 9, at 489 (noting that legislators have remained silent on the applicability of regulations to mobile payments).

\textsuperscript{69} See McTaggart & Freese, supra note 9, at 489 (positing that come current regulations will likely extend to m-payments, even though the application has not been expressly made).

\textsuperscript{70} See infra pp. 11-16 (discussing current protections offered to customers from mobile payment systems).

\textsuperscript{71} See Jun, supra note 5, at 7 (claiming that mobile payments linked to debit cards or bank accounts would offer the second best protections to consumers).

\textsuperscript{72} See Jun, supra note 5, at 7 (outlining consumer liability in worst-case-scenarios relating to mobile payments linked to a debit card account).

\textsuperscript{73} See Jongho Kim Ph. D, Ubiquitous Money and Walking Banks: Environment, Technology, and Competition in Mobile Banking, 8 RICH. J. GLOBAL L. & BUS. 37, 79-80 (2008) (discussing the risks to banks that will arrive along with the mobile banking industry).

\textsuperscript{74} See id. at 79-80 (noting that risks to banks will largely depend on how long mobile payment services go unregulated, and that the distribution of risk is a primary issue for financial institutions regarding m-payment services). According to recent statistics, financial institutions incurred $995 million in losses due to debit card
If Regulation Z were found applicable to mobile payment systems, consumers with mobile payments linked to credit cards would be offered the best form of protection considering the current state of the law. As previously noted, consumer liability is limited to $50 for unauthorized transactions, and consumers are not liable for billing errors if they are reported within 60 days. However, applying Regulation Z to mobile payment systems would expose credit companies to additional risk and liability. Additional devices linked to the same credit account allow for superfluous opportunities for unauthorized transactions, which the credit institution must then absorb.

Consumers whose mobile payment systems are linked to prepaid cards, gift cards, or to phone bills currently receive little to no protection under the existing regulatory framework. The only consumer protection regulations that currently apply to prepaid cards are voluntary regulations that are self-imposed by the financial institutions that issue the prepaid cards. There is an absence of federal regulation that governs liability for unauthorized transactions effectuated with gift cards. The Federal Communications Commission (FCC) is responsible for regulating interstate telephone services, but the FCC has not yet issued any regulations regarding mobile payments. This fraud in 2010 alone. See Credit Card and Debit Card Fraud Statistics, CARDHUB (Mar. 19, 2014), archived at www.perma.cc/V844-AB4P (listing various statistics regarding the costs of fraud to financial institutions and merchants, gathered from an August 2013 Nilson Report).

75 See Jun, supra note 5, at 6 (claiming that m-payments linked to credit cards offer the best consumer protection).
76 See Jun, supra note 5, at 6 (outlining consumer liability if a mobile phone linked to a credit card is lost or stolen or involved in unauthorized transactions).
77 See Kim, supra note 73, at 79-80 (emphasizing that distribution of liability risk will pose a large problem for financial institutions when offering m-payment services).
78 See Kim, supra note 73, at 79-80 (noting the increased risks banks will face if proper and strategic risk management is not addressed before the large-scale adoption of mobile payment services).
79 See Jun, supra note 5, at 8-10 (describing m-payments linked to these types of accounts as offering the least amount of protection and unclear protection).
80 See Jun, supra note 5, at 8-9 (detailing the regulation landscape relating to prepaid card accounts).
81 See Jun, supra note 5, at 9-10 (detailing the regulation landscape relating to gift card accounts).
82 See Jun, supra note 5, at 10 (stating the regulatory landscape relating to mobile carrier accounts).
means that consumers are currently not protected from unauthorized transactions that are effectuated through an account held with their wireless carriers. \(^8^3\)

The Federal Communications Commission (“FCC”) supervises mobile carrier standards and oversees competition within the industry but does not have authority over payments made with a mobile phone.\(^8^4\) The existing statutory obligations of wireless carriers starkly contrast with those obligations of financial institutions; wireless carriers have no obligations as to customer authentication, and their obligations as to verifying the origination and termination of a mobile transmission is legally limited to ensuring that a call is completed and that customers are billed for the service properly.\(^8^5\) The wireless carrier industry has developed an independent set of best practices, recommending that carriers hold themselves responsible for implementing best practices to authenticate a user’s identity and to cap consumer liability for any unauthorized transactions.\(^8^6\) It is currently unclear as to whether these best practice recommendations will have a practical influence on wireless carriers given the doctrine of limited liability and the lack of actual statutory obligations regarding mobile payment transactions that apply to wireless carriers.\(^8^7\)

---

\(^8^3\) See Jun, supra note 5, at 10 (noting the lack of consumer protection for customer accounts linked to mobile carriers).


\(^8^5\) See Frederick Joyce, Mobile Banking Liability: The Elephant in the Parlor, 3 THE INNOVATOR 3 (2010) (outlining the statutory regulations that apply to wireless communications carriers and noting the contrast in the obligations of financial institutions and the limited obligations of the wireless carriers).

\(^8^6\) See id. at 31 (discussing the “CTIA,” the wireless carrier industry’s primary trade association, and the adoption of their “Best Practices and Guidelines for Mobile Financial Services” and noting examples of particular best practices); see also Cellular Telephone & Internet Association, Best Practices and Guidelines for Mobile Financial Services (Jan. 28 2009), archived at www.perma.cc/GUK7-SJDX (listing of the wireless industry’s best practices and guidelines).

\(^8^7\) See Joyce, supra note 85, at 31 (analyzing the practical effect that these best practices guidelines may or may not have on the wireless carrier industry, as the guidelines are recommendations and compliance is not mandatory).
Merchants are not statutorily allocated liability for fraudulent or unauthorized transactions. Payment card networks (such as Visa, MasterCard, Discover, American Express) develop rules to bind issuer and acquirer banks for liabilities, and these banks in turn contractually pass on some of this liability to merchants. Merchant liability depends on the type of transaction being performed by the consumer. Card-not-present transactions, such as mail order, telephone order, or Internet transactions, typically distribute liability to the merchant. However, contactless and proximity payment systems, including m-payment systems, fall under the card-present transactions category in which the merchant has the opportunity to physically observe the card or other account access device and can attain a customer signature or pin number. Under the card-present transaction category, the card issuer (the financial institution) assumes all liability for unauthorized transactions, as long as the merchant follows basic security steps. The basic nature of these security steps, which vary but typically include physically viewing the card, obtaining authorization from the card issuer for the transaction, or procuring the customer’s signature, essentially means that the liability for card-present transactions remains with the issuer. Because of a merchant’s relative inability to detect impersonation, forgery, or counterfeit access devices, allocation of liability for m-payment transactions

89 See id. (illustrating the development and implementation of the payment card liability rules in the United States through statute and private ordering).
90 See id. (noting that there could be considerable variability in liability allocation depending upon the payment card network, but generally all payment card networks follow this formula, changing liability allocation depending upon whether the transaction was card-not-present or card-present).
91 See id. at 20 (describing the typical liability allocation for card-not-present transactions and defining card-not-present transactions).
92 See id. at 15 (listing contactless and proximity payment systems, employed by RFID technology, as a form of card-present transaction).
93 See id. at 16 (discussing the liability allocation used by most payment card networks for card-present transactions).
94 See Levtin, supra note 88, at 15 (listing the basic security steps that a merchant is required to take in order to avoid liability for unauthorized card-present transactions, and then noting the limited expectations that these requirements actually entail).
gone awry to merchants does not appear sensible and this allocation system will likely not change.95

Mobile payments create new issues for institutions subject to the GLBA and USA PATRIOT Act.96 Financial institutions that are currently subject to the GLBA will now be interacting with and transferring information to mobile carriers and mobile application developers that are not subject to the GLBA, which will likely mute the efficacy of financial institutions' privacy policies.97 Current anti-money laundering provisions set up to comply with the USA PATRIOT Act do not account for the new risks posed by the transfer of funds through mobile phones.98 Mobile payments offer criminals a new means through which they can achieve their illegal ends, with increased speed and efficiency, and involving less risk than the movement of physical cash.99

Additionally, the phenomenon of “smurfing” could evolve into “digital value smurfing” with the proliferation of mobile payment systems.100 Smurfing involves using multiple criminals, called the “smurfs,” to each open or access individual accounts for under $10,000, in order to bypass financial reporting requirements.101 With mobile payment capabilities, however, one smurf would be able to establish numerous m-payment accounts, all belonging to the same smurf, and keep the amount of transactions per account under

---

95 See Levtin, supra note 88, at 19-20 (describing the current arrangement of loss allocation for card-present rules as sensible and describing the issuer as the least cost avoider in card-present transaction situations).
96 See McTaggart & Freese, supra note 9, at 494-95 (stating the problems regarding mobile payments and how these systems would or would not fit under the GLBA and Patriot Act).
97 See McTaggart & Freese, supra note 9, at 495 (observing that banks will now be in contact with mobile carriers and mobile application developers, to whom the GLBA does not yet expressly apply).
98 See McTaggart & Freese, supra note 9, at 495-96 (noting the lack of mobile payment related measures currently adopted by anti-money laundering regulators).
99 See Mobile Payments - A Growing Threat, supra note 4 (discussing the new avenues available to terrorist organizations with the proliferation of mobile payment systems).
100 See Leyva, supra note 9, at 64 (postulating the growth of digital value smurfing concurrent with the growth of mobile payments, because of the unchecked, limitless number of accounts accessible to criminals through m-payments).
101 See Leyva, supra note 9, at 64 (defining the process of “smurfing” and the term “smurfs.”)
$10,000. Essentially, one smurf with mobile payment account capabilities could accomplish the illicit transactions of what ten smurfs with traditional payment accounts could accomplish. The propagation of unregulated mobile payment systems allows criminals the opportunity to find ways to exploit the new technology, rendering the existing USA PATRIOT Act much less effective and comprehensive.

IV. ANALYSIS

Viewing mobile payments as a novel channel to access traditional payment methods rather than classifying mobile payments as an entirely separate system would seem to indicate that the regulations currently governing electronic payments might be able to properly regulate mobile payments. This is the approach that some parties advocate taking. However, deeming the existing regulatory scheme as one size fits all that can adequately address mobile payments creates new uncertainty and tension between the different stakeholders involved: financial institutions, wireless carriers, mobile application developers, and the consumer. The current regulatory landscape lacks appropriate limitations on financial institution liability for unauthorized and fraudulent transactions effected through mobile payment systems, does not properly account for the additional responsibilities that mobile payment systems would impose on financial institutions to remain in compliance with the current regulatory scheme, and offers unchecked opportunities for criminals to quietly

102 See Leyva, supra note 9, at 64 (inferring the outcome of a possible m-payment situation).
103 See Leyva, supra note 9, at 64 (outlining the limitless possibilities for smurfing with m-payment accounts and describing the precise possibilities for criminal activity).
104 See Leyva, supra note 9, at 64 (noting the “dark side” of m-payment services if the services are adopted and propagated before they are regulated properly).
105 See Kepler, supra note 84, at 4 (noting the common elements between mobile payments and payment transactions that occur over the Internet).
106 See Hearing before the Subcommittee on Financial Institutions, supra note 6, at 9 (claiming that the existing regulations cover mobile payments systems).
107 See Kepler, supra note 84 at 7 (asserting that the diversity of mobile payment system models and the developing nature of mobile payment systems indicates that regulation that is one size fits all will not be adequate).
and unobtrusively exploit the new mobile payment technology. Consumers end up paying the ultimate price as the costs imposed on financial institutions are spread to the customers of the financial institution. The existing regulatory scheme is therefore insufficient and should be supplemented by new regulations specifically directed at governing the nuances of mobile payment systems.

A. Increased Strain on Institutional Resources

Financial institutions expend a large volume of resources complying with federal regulations designed to protect sensitive consumer information and minimize successful fraudulent transactions. Complying with the Gramm-Leach-Bliley Act and the USA Patriot Act of 2001 requires expending money to develop quality control technologies, maintain privacy measures, keep sensitive information confidential, and train employees to spot and stop criminal transactions. The arrival of mobile payment technology would pose new and unique problems for the institutions required to comply with the USA Patriot Act and the GLBA.
Because financial institutions are subject to the requirements of the GLBA, the institutions would already be providing their privacy disclosure policies to their customers that hold debit or credit accounts through them.\textsuperscript{114} There would appear to be no additional strain upon financial institutions in continuing to supply the privacy disclosure policies to customers now using m-payment services to access the same accounts.\textsuperscript{115} However, under an m-payment system model, financial institutions must interact with third parties that are not currently subject to the GLBA that will have access to sensitive customer information, such as mobile application developers and wireless carriers.\textsuperscript{116} If these parties are not brought under the GLBA, financial institutions will have to contract with them individually to ensure these parties do not breach the financial institution’s obligations.\textsuperscript{117} The fault of a breach caused by a mobile carrier or mobile application developer could ultimately fall upon an institution.\textsuperscript{118}

Mobile payment technology would allow criminals to avoid the detection risks of physically moving paper money, to circumvent reporting requirements, and to quickly transfer funds across long distances.\textsuperscript{119} Anti-money laundering regulators under the USA Patriot Act would be required to watch out for and prevent criminals and terrorists transferring proceeds from illegal operations through mobile

\textsuperscript{114} See McTaggart & Freese, supra note 9, at 495 (asserting that on the surface, it would appear that financial institution’s obligations under the GLBA would not be changed with the arrival of mobile payment services).

\textsuperscript{115} See McTaggart & Freese, supra note 9, at 495 (explaining that regardless of how an account is accessed, the same account is being accessed, and only one set of privacy disclosure policies is necessary for each account).

\textsuperscript{116} See McTaggart & Freese, supra note 9, at 495 (noting the additional stakeholders that will be involved in administering mobile payment services and explaining that these additional parties are not currently subject to the GLBA).

\textsuperscript{117} See McTaggart & Freese, supra note 9, at 495 (illustrating the solutions to the problem of the additional stakeholders not being subject to the GLBA, and how these solutions fall upon the financial institution to take).

\textsuperscript{118} See McTaggart & Freese, supra note 9, at 495 (suggesting that since the financial institutions need to take these steps, they will be the party that faces liability if their obligations under the GLBA are compromised by an outside party).

\textsuperscript{119} See McTaggart & Freese, supra note 9, at 495-96 (discussing the new methods of performing criminal transactions and committing fraud that will be available to criminals with the arrival of mobile payment technology); Mobile Payments - A Growing Threat, supra note 4 (outlining the new avenues for criminal activity that are introduced along with the implementation of mobile payment services).
If mobile payments were introduced successfully to the U.S., financial institutions would need to update their internal controls to scrutinize m-payments, train employees to recognize signs of laundering through mobile payment technology, allow their m-payments services to be independently audited, and alter their suspicious activity reporting procedures. All of these additional measures taken to ensure compliance with the existing regulatory scheme would cost financial institutions further resources, with only indirect benefits to the financial institutions. Mobile application developers and wireless carriers should be responsible for some of these statutory obligations as well, in order to reduce the burden on financial institutions, incentivize these parties to act appropriately, and to ensure that the party with the best ability to implement the obligations is doing so, and new m-payment regulations that equally apportion the obligations between all three stakeholders would accomplish these goals.

B. Criminal Manipulation Of New Mobile Technology

New technology attracts criminals because it allows them to find new ways to exploit it until the technology is fully understood and preventative measures can be taken. Consumers are already wary of the security of mobile payment transactions, whether or not their concerns are well founded. Once mobile payment technology

---

120 See McTaggart & Freese, supra note 9, at 496 (asserting that if mobile payment technology is introduced, these services will also come under the required supervision of financial institutions because of their obligations under the USA Patriot Act).

121 See McTaggart & Freese, supra note 9, at 495-96 (listing the changes that would need to be made by financial institutions in order to remain in compliance with anti-money laundering requirements of the USA Patriot Act).

122 See Arnab Datta, Mehmet Pasa & Tom Schnitker, Emerging Markets: Could Mobile Banking Go Global?, 4 THE MCKINSEY QUARTERLY, 71 (2001) archived at www.perma.cc/X7XE-NDSK (claiming that mobile payment services only provide financial institutions that implement them with indirect benefits, which are only worth the trouble if the benefits can be retained for long enough to justify the investment).

123 See supra Part A (summarizing the responsibilities of the wireless carriers and developers in regards to m-payments).

124 See Leyva, supra note 9, at 65 (describing the reasons that mobile payment technology will attract criminals: its novelty).

125 See Joyce, supra note 85, at 29 (asserting that regardless of empirical evidence that mobile payment transactions may at least currently be safer than online bank-
achieves proliferation, it will attract criminal manipulation because manipulating these services will be beneficial to criminals, and in its early stages the technology will be most vulnerable to attack. Preventative measures and curative legislation should be implemented prior to the arrival of mobile payment services, or else criminal manipulation could prove extraordinarily and unprecedentedly costly for financial institutions, and consumers could become permanently scared away from mobile transactions.

The U.S. currently has minimal safeguards against the exploitation of mobile payment technology. New legislation could unburden financial institutions of the risks of hosting mobile services that are unregulated by lowering the maximum transaction limits, requiring the registration of pre-paid mobile phones equipped with mobile payment technology (so that the technology could not be used with disposable mobile phones), and spurring the development of new software that is specific to mobile payments that can accurately detect dubious activity. All of these mechanisms, if required by legislature, could reduce the costs on financial institutions that would otherwise have to absorb the losses caused by criminal or fraudulent activity. Initial legislative changes should not be focused on creating

\[126\] See Kim, supra note 73, at 72-73 (stating that a strong firewall needs to be implemented in order to prevent hacking into and intervening in transactions); Kim, supra note 73, at 64 (claiming that technologies as a general rule become more secure over time, not less secure over time); Leyva, supra note 9, at 64-65 (discussing all of the possibilities criminals have to manipulate mobile payment technologies for their own benefit).

\[127\] See Rajan, supra note 6, at 468-69 (suggesting that adoption of mobile payment technology will be much swifter if gaps are filled in the current regulatory landscape, as consumer and financial institution fears will be calmed).

\[128\] See Leyva, supra note 9, at 65 (stating that the US currently is not well prepared to handle the darker side of mobile payment systems technology; Mobile Payments - A Growing Threat, supra note 4 (asserting that the U.S. has very few safeguards against m-payment system abuse by criminals).

\[129\] See Leyva, supra note 9, at 65 (suggesting a variety of legislative remedial measures that would lessen the burden on financial institutions of having to absorb the costs of successful criminal attacks on mobile payment transactions).

\[130\] See Leyva, supra note 9, at 65 (suggesting that if preventative legislative action is not taken, then financial institutions will be fiscally harmed by the criminal action as institutions are the parties primarily held responsible under Regulations E and Z if a transaction is fraudulent or unauthorized).
additional burdens for financial institutions to comply with, as the institutions are already taking on additional burdens if mobile payment systems are introduced, and added encumbrances would only further dissuade institutions from implementing mobile payment services in the first place.\textsuperscript{131} Failing to defend against criminal infiltration of mobile payment technology puts financial institutions at too high of a risk since these parties will have to absorb the losses and will suffer from consumer dissatisfaction.\textsuperscript{132}

\textbf{C. Increased Liability Exposure for Financial Institutions}

Financial institutions are the parties at the greatest risk if mobile payment systems are successfully implemented in the U.S before further legislation is enacted.\textsuperscript{133} Although consumers are tentative to embrace mobile payment technology, they are not the party most exposed to liability under the existing regulations.\textsuperscript{134} As discussed above, if the current electronic fund transfer regulations are interpreted to apply to mobile payment systems, then consumer liability for transactions gone awry will, in most cases, be limited to a nominal monetary amount, pending reporting by the customer.\textsuperscript{135} The wireless carrier is not responsible for authenticating the mobile phone user’s identity, and the carrier has no legally binding obligations relating to mobile payment transactions that would lead to liability.\textsuperscript{136}

\textsuperscript{131} See Kim, supra note 73, at 72-73 (discussing the costs for financial institutions in implementing mobile payment services for their customers, and noting that these institutions already must weigh the costs against the benefits when deciding whether or not to offer mobile payment services); Leyva, supra note 9, at 65 (outlining possible legislative remedies that do not involve additional resources to be expended by financial institutions).

\textsuperscript{132} See Leyva, supra note 9, at 65 (inferring the risks that financial institutions undergo by trying to reduce costs).

\textsuperscript{133} See Joyce, supra note 85, at 31 (stating that since financial institutions are the parties at a greater risk for liability would benefit from an industry-wide adoption of uniform best practices standards).

\textsuperscript{134} See Joyce, supra note 85, at 29 (noting the research statistics which indicate that consumers believe mobile banking is less secure than online payment transactions and stating that financial institutions are at the greatest risk in mobile banking transactions).

\textsuperscript{135} See Jun, supra note 5, at 7 (claiming that consumers are well protected when transacting mobile payments linked to debit cards or bank accounts as well as credit card accounts and gift certificate or prepaid card accounts).

\textsuperscript{136} See Joyce, supra note 85, at 31 (detailing the minimal statutory obligations of wireless carriers in relation to mobile payment transaction liability).
Therefore, the financial institutions holding the consumer accounts are the party left to absorb the loss that is incurred by any fraudulent, unauthorized, or incorrect mobile payment transactions, until and unless the issue is specifically addressed by government authorities. 137

The potentially sizeable risk that currently lies with the financial institutions may initially appear to be a sensible allocation of liability. 138 With consumers remaining tentative about embracing the new mobile payment technology, a further obstacle in the technology achieving propagation would be raised if consumers were saddled directly with the liability for mobile payment transactions gone awry. 139 Financial institutions have the ability to spread a monetary loss to its wide base of customers, resulting in a smaller actual loss to the institution and a miniscule, almost unnoticeable loss to each individual consumer. 140 In comparison, individual consumers do not have the ability to spread the cost of a loss through various resources, and therefore a loss “costs” an individual consumer more. 141 The loss

137 See Joyce, supra note 85, at 32 (concluding that the “elephant in the parlor” will either lead to statutory changes initiated by government authorities or will result in a financial institution unhappily reading in a newspaper about a very large mobile payment transaction going wrong in a major way).

138 See Cooter & Rubin, supra note 108, at 71-72 (viewing loss allocation through an economic lens, the loss spreading principle, loss reduction principle, and loss imposition principle all tend to favor allocating the loss to the financial institution, because the institution has greater economic resources to more easily absorb the loss by spreading the costs to its entire consumer base). Even when both the consumer and the institution have the ability to take precautions that reduce costs of losses, the principles suggest that consumer liability remain limited. See Cooter & Rubin, supra note 108, at 123-24 (discussing the allocation of loss that the principles suggest).

139 See Joyce, supra note 85, at 29 (noting the “skittish” attitude of consumers toward mobile payment transactions, and suggesting the reasons behind the attitude being lack of consumer knowledge of the security of mobile payment transactions and lack of consumer knowledge regarding the liability of fraudulent or inaccurate transactions).

140 See Cooter & Rubin, supra note 108, at 71-72 (explaining the theory behind the loss spreading principle and contrasting the desirability of allocating loss to the institution versus the consumer on the basis of the relative size of the loss and the party’s ability to spread it).

141 See Cooter & Rubin, supra note 108, at 71-72 (listing the reasons why the loss spreading principle suggests that loss is better allocated to a large financial institution rather than an individual consumer, and explaining how the loss from one transaction may be significant to an individual but very insignificant to a large financial institution).
spreading principle suggests that the party with the ability to spread
the loss to minimize the costs of the loss should be the party to absorb
the loss, and in the context of mobile payment systems, a party with
this ability is the financial institution. The loss reduction principle
dictates that the party with the ability to prevent or reduce losses
should be the party to which the law assigns liability. In the mo-
bile payment context, both the individual consumer and the financial
institution have the ability to take certain precautions to prevent
fraudulent or inaccurate transactions. The consumer can password
protect their mobile phone, keep close track of his or her phone, and
be diligent in reporting a lost or stolen phone to their wireless carrier
and the financial institution holding the accounts linked to the mobile
phone. The financial institution can institute internal policies, pro-
cedures, and mechanisms to ensure authentication, quality control,
and minimize fraud. But the institution also has the resources and
ability to invent new technology that can reduce loss, and respond to
and learn the legal incentives surrounding loss allocation. Therefore,
the loss reduction principle again suggests that while both the
consumer and the institution should assume some degree of liability,
the financial institution should be the party with the greater amount
of loss allocated to it. The economic theory of loss spreading and

142 See Cooter & Rubin, supra note 108, at 71-72 (discussing the loss spreading
principle in the context of payment systems); Joyce, supra note 85, at 29 (extrapo-
lating liability allocation theories to the mobile payment context).
143 See Cooter & Rubin, supra note 108, at 73 (explaining the loss reduction prin-
ciple as an economic theory of loss allocation).
144 See Cooter & Rubin, supra note 108, at 73-74 (noting the ability of both parties
to engage in equally effective loss reducing activities).
145 See Cooter & Rubin, supra note 108, at 73 (listing the types of precautions con-
sumers can take, namely being diligent in making their payments and handling their
account access devices carefully).
146 See Cooter & Rubin, supra note 108, at 73 (comparing the precautionary
measures that institutions can take to quality control mechanisms similar to those
implemented in manufacturing processes).
147 See Cooter & Rubin, supra note 108, at 74-76 (describing the deeper complexi-
ties involved with the loss reduction principle, complicated by the elements of pre-
caution, innovation, responsiveness, and learning, which all contribute to a party’s
ability and desirability to reduce losses).
148 See Cooter & Rubin, supra note 108, at 124 (concluding that although under the
loss reduction principle it is desirable for both parties to bear some loss, the con-
sumer loss allocation should still remain very limited with the financial institution
absorbing most of the loss, because the institution usurps consumer ability in the
innovative, responsiveness, and learning elements).
loss reduction reasons that financial institutions should be the party absorbing the loss when a mobile transaction goes awry.\textsuperscript{149} Looking beyond classic economic theories of loss allocation, loss allocation in the mobile payment transaction context differs from loss allocation in other more traditional payment systems.\textsuperscript{150} Consumers are likely to be reluctant to abandon their credit and debit cards at first, even if mobile transactions are proven to be reliable and secure.\textsuperscript{151} With consumers tentatively embracing the new mobile technology while still clutching to the traditional payment technology at the very least as a back-up, the number of access devices to any one particular account should double at least initially, if not long-term.\textsuperscript{152} The sheer increase in number of access devices linked to a single account increases the chances for unauthorized, fraudulent, or inaccurate transactions made through the account and doubles the opportunity for loss of or criminal interception of one of the access devices.\textsuperscript{153} A landscape comprised of double the access devices to

\textsuperscript{149} See Cooter & Rubin, supra note 108, at 124 (stating the total effect of the conclusion reached by the loss reduction and loss spreading principles).

\textsuperscript{150} See Joyce, supra note 85, at 29 (asserting that in the mobile payment context, the additional stakeholder of the wireless carrier affects the liabilities involved in transactions).

\textsuperscript{151} See Jane Kaufman Winn, Clash of the Titans: Regulating the Competition Between Established and Emerging Electronic Payment Systems, 14 BERKELEY TECH. L.J. 675, 677 (1999) (analogizing the adoption of new payment systems and payment technologies versus the commitment to tried and true payment technologies to a war between the Titans and the Olympians). Consumers in the U.S. still continue to primarily use traditional payment systems, despite the availability of newer and more advanced payment systems. See id. at 682 (describing the traditional payment systems and their foothold in the consumer payment landscape as the “Titans”).

\textsuperscript{152} See id. (reiterating the hold that traditional payment technology has over consumers and their reluctance to whole-heartedly embrace new technology); Joyce, supra note 85, at 29 (noting the slow and hesitant attitude of consumers towards mobile payment technology and possible reasons behind it); Darcy Travlos, All Eyes on Mobile Commerce, FORBES (Nov. 10, 2009), archived at www.perma.cc/6KHS-5CWV (noting the increased consumer acceptance of mobile transactions, although it still remains at less than 45% acceptance).

\textsuperscript{153} See Michael Ena, Securing Online Transactions: Crime Prevention is the Key, 35 FORDHAM URB. L.J. 147, 160-61 (2008) (discussing the increasing attraction of criminals to mobile phones because of the increasing number of uses for mobile phones, and noting that mobile phones are more vulnerable than personal computers); Kim, supra note 73, at 56-57 (noting that in the case of lost mobile phones,
consumer accounts creates a disproportionate amount of liabilities that financial institutions are not currently prepared for. Maintaining the existing regulatory scheme with its current allocation of liability solely upon financial institutions would lead to a spike in costs that would either cripple institutions if they absorbed the cost themselves or force the financial institutions to pass the new higher costs on to the consumer. Faced with these two possibilities, financial institutions might use their resources to deter the adoption of mobile payment systems so as to avoid the new increase in liabilities, and consumers will continue to feel hesitant about using mobile phones to transact due to the risk that the new disproportionately high costs from mobile payment technologies will ultimately be dumped onto them. Potential pushback from the financial institutions combined with consumer trepidation means that mobile payment technology is facing an uphill battle for proliferation and permanent success in the existing payment system landscape.

D. Steps That Should be Taken Before Mobile Payments Take Over

Explicitly applying Regulations E and Z to mobile payment systems would be a good first step to provide a baseline level of protection to consumers, but the legislation cannot stop there due to the security, safety, privacy, protection, and crime prevention all become issues, as in the case of a lost credit or debit card).

154 See Joyce, supra note 85, at 32 (describing the new liabilities that come along with mobile banking technology as dangerous elephants that need to be addressed before they cause chaos).

155 See Kim, supra note 73, at 57 n.116 (suggestion that the same rule would apply in the case of a lost mobile phone as in the case of a lost debit card, where the financial institution assumes nearly sole liability, with the consumer paying only a limited $50 for the fraudulent transaction); Cooter & Rubin, supra note 108, at 71 (describing the process of a financial institution passing its costs of liabilities on to its customers as one of the reasons institutions are straddled with the liabilities in the first place).

156 See Ena, supra note 153, at 160 (stating that many consumers doubt the security of mobile payment technology for many reasons); Cooter & Rubin, supra note 108, at 71-72 (discussing the process of risk costs being passed on to consumers by financial institutions).

157 See Ena, supra note 153, at 160 (asserting that reliable sources believe that mobile payments in the U.S. are at least five years away from becoming a reality).
problems discussed above. There are additional parties involved in mobile payment transactions that are not involved in alternative electronic payment systems: the wireless carrier and the mobile application developer. The wireless carrier is more akin to the financial institution because of its wide customer base and the ability to spread losses and large resource pool that has the ability to create better innovative technology and respond to and learn legal rules and incentives. A wireless carrier has the ability and responsibility to shut off a mobile phone’s service, which could mean the difference between a harmless misplaced phone and a lost phone successfully used to make numerous expensive transactions before service is cut off. Mobile application developers also will have a large customer base and will have strong incentives to ensure that their particular application is the most secure, in order to attract consumers, and to develop strong relationships with the other stakeholders in order to secure a foothold in the competition.

These two additional parties should more fairly share in liability along with financial institutions, as they have similar access to sizeable resources and should be similarly incentivized to develop better quality control and safety mechanisms. If these additional stake-

\[158\] See McTaggart & Freese, supra note 9, at 489 (explaining the logic of applying the current regulations to m-payments).

\[159\] See McTaggart & Freese, supra note 9, at 487 (claiming the stakeholders involved in completing an m-payment transaction differ from the stakeholders involved in traditional payment model transactions, and there is also some variety within the different m-payment models as well).

\[160\] See Cooter & Rubin, supra note 108, at 71-72 (discussing the aspects of a stakeholder that favor an allocation of liability to it, such as the ability to spread and absorb the losses because of a large resource pool and the incentive and ability to innovate new technologies to better prevent the losses in the first place).

\[161\] See Joyce, supra note 85, at 31 (noting that the wireless carrier has the ability to locate or shut off service of a wireless phone, and this technical tool could be a powerful method of preventing mobile banking fraud).

\[162\] See Alex Krouse, iPads, iPhones, Androids, and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices, 9 IND. HEALTH L. REV. 731, 733-34 (defining mobile applications and discussing the history of mobile applications). The number of consumers that mobile applications reach is extensive and growing, but varies based on which mobile platform the application works on. See id. (suggesting the ability to attain a wide consumer base for mobile application developers and the competition in the market).

\[163\] See Joyce, supra note 85, at 31 (stating that a more fair allocation of liability between wireless carriers and financial institutions should be worked towards to
holders were to share in the liability along with financial institutions, less of a strain would be placed on the institutions and the institutions therefore might be more amenable to convincing consumers to embrace the new technology.\textsuperscript{164} In addition, consumer knowledge of a more evenly spread allocation of liability might be less intimidating to individual consumers.\textsuperscript{165} Consumer knowledge that the financial institutions holding their bank accounts will be held solely liable might scare the consumers because they might anticipate that these costs will be passed on to them directly through their bank accounts.\textsuperscript{166} If wireless carriers and mobile application developers are allocated more of the responsibility, consumers have a choice of whether or not to engage in mobile payment transactions at all, thus circumventing charges if the costs are passed on through these parties.\textsuperscript{167} Costs passed to consumers through a financial institution will be passed regardless of whether one individual consumer chooses to utilize the mobile payment technology services.\textsuperscript{168} Requiring liability
costs to be spread to wireless carriers and mobile payment application developers promotes fairness, saves financial institutions from drowning in costs from fraudulent transactions and passing these costs to all of their customers, and ultimately will help to eliminate consumer hesitation to embrace this new payment technology.169

V. CONCLUSION

Mobile payment technology is an emerging, convenient, and efficient payment method that has the ability to positively change the existing payment system landscape. However, in order for this change to be positive for all parties involved in the mobile payment model, including consumers, financial institutions, wireless carriers, and mobile application developers, adequate preparation should be taken before the technology prevalently arrives and consumers bite. The existing regulatory scheme controlling payment systems in the U.S. is not extensive enough to protect both consumers and financial institutions if mobile payment systems are introduced before it is reworked. The first step is for Regulations E and Z to be made explicitly applicable to mobile payments to safeguard vulnerable consumers, and then the current regulations must be further supplemented in order to more fairly spread liability for transactions gone awry to wireless carriers and mobile payment application developers in addition to financial institutions, in order to avoid devastating costs for financial institutions. Compliance with existing consumer protection regulations in a new mobile context would drain financial institutions of their resources if these responsibilities are not shared with these other parties, and the consumer suffers if these responsibilities are legislatively lessened. The existing payment system regulations were developed prior to the introduction of mobile payment technology, and therefore the scheme is not comprehensive enough to make illegal all of the methods criminals may utilize to take advantage of the new technology, which also puts financial institutions and consumers at risk. Sup-

See Cooter & Rubin, supra note 108, at 71-72 (opining that consumers will end up bearing costs if other consumers are forced to use m-payments). See Joyce, supra note 85, at 29, 31 (claiming that a fairer and less hazardous result would be reached if liability costs were spread between financial institutions, mobile application developers, and mobile carriers, and noting lack of knowledge about liability as a primary reason along with security concerns of why consumers are hesitant to embrace m-payment services).
lemental regulations specifically designed to prevent crimes perpetrated through mobile payment technology are essential to ensure fraud cannot slip through the legislative cracks left by haphazard gap-filling. In order for financial institutions to be properly protected and incentivized to implement mobile payment services, wireless carriers and mobile application developers need to be regulated through new legislation in order to properly address the nuances that mobile payment technology generates.