

WHAT'S IN YOUR WALLET? ADDRESSING THE REGULATORY GREY AREA SURROUNDING MOBILE PAYMENTS

Stephen Congdon

ABSTRACT

Mobile payment applications are poised to replace traditional checks, credit, and debit cards at cash registers around the country. Largely seen as the next step forward for increased convenience in shopping, mobile payments are making it easier for American consumers to make payments simply by having their phone on them at all times. However, until recently, many of the applications that consumers use to make their mobile payments may fall out of the American regulatory system already in place for banks and bank payment sources. The recently formed Consumer Financial Protection Bureau proposed regulatory changes in 2014 that include mobile payment systems and applications in the wheelhouse of services various banking regulations cover. Still, in light of many highly publicized privacy breaches and security hacks in 2014, many consumers are wary of the trustworthiness of mobile payment applications. In order to address these concerns, and ensure that mobile payments have a foothold in the American marketplace, the Consumer Financial Protection Bureau should adopt more regulations than what it proposed in 2014 by using their ability to promulgate rules using informal rulemaking procedures to help establish data security and privacy standards in the mobile payment marketplace.

INTRODUCTION

Of the 87% of the United States Population that owns a mobile phone, 71% have internet-enabled smartphones.¹ Nearly 1/3 of mobile phone owners made purchases with their phones in 2012, and in the same year, consumers spent over \$20 billion on mobile browsers and applications.² The use of mobile devices is poised to take on a major role in the American economy, as consumers can now use their phones not only to make purchases, but also to send money and transfer money between bank accounts.³ Despite the potential for mobile payments to take over as the primary payment method in America, many consumers remain concerned about the privacy of their personal information and the security of their data when using mobile payment applications.⁴

The Federal Reserve Bank (FED) conducts an annual survey to gauge American consumers' use of mobile devices for mobile payments and banking.⁵ In 2015, the FED reported that 62% of consumers do not use mobile payments due to concerns regarding security of the technology,⁶ and only 7% of respondents felt that mobile payment technology was "very safe".⁷

This hesitation is echoed in Congress⁸ and by federal regulatory agencies.⁹ Congress has conducted hearings,¹⁰ regulators have hosted workshops,¹¹ and agencies have proposed rules,¹² looking for ways to make mobile payment technologies safe and reliable for consistent use in the United States. Though banks may appear to be the entities most responsible

-
1. BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, CONSUMER AND MOBILE FINANCIAL SERVICES 2015 1 (2015) [hereinafter *FED REPORT*].
 2. FEDERAL DEPOSIT INSURANCE CORPORATION, MOBILE PAYMENTS: AN EVOLVING LANDSCAPE (2012) [hereinafter FDIC: MOBILE PAYMENTS] (citing JAVELIN STRATEGY & RESEARCH, "MOBILE PAYMENTS HITS \$20 BILLION IN 2012," (2012)).
 3. See generally Meena Aharam Rajan, *The Future of Wallets: A Look at the Privacy Implications of Mobile Payments*, 20 CommLaw Conspectus 445 (2012).
 4. FED REPORT, *supra* note 1, (stating "A preference for other methods of banking and making payments, as well as concerns about security continue to be the main impediments to the adoption of mobile financial services.").
 5. See generally FED REPORT, *supra* note 1.
 6. *Id.* at 2.
 7. *Id.* at 19.
 8. See generally *The Future of Money: Where Do Mobile Payments Fit in The Current Regulatory Structure?: Hearing Before the H. Sub. Comm. on Financial Institutions and Consumer Credit*, 112th Cong. [hereinafter *The Future of Money Hearing*] (2012).
 9. *Id.* See also FDIC: MOBILE PAYMENTS, *supra* note 2, FEDERAL DEPOSIT INSURANCE CORPORATION, MOBILE PAYMENTS: AN EVOLVING LANDSCAPE (2012), FEDERAL TRADE COMMISSION, PAPER, PLASTIC... OR MOBILE? (2013), FED REPORT, *supra* note 1.
 10. See generally *The Future of Money Hearing*, *supra* note 8.
 11. See generally FDIC: MOBILE PAYMENTS, *supra* note 2.
 12. See generally Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 12 CFP Parts 1005 and 1026 [hereinafter CFPB Prepaid Card Rule] (proposed Dec. 23, 2014).

for managing these technologies, new apps are constantly breaking into the mobile payments atmosphere,¹³ threatening to disrupt the industry.¹⁴ The Federal Deposit Insurance Corporation (FDIC) asserts that, “Financial Institutions should not assume their place in the new mobile payments marketplace is assured [just] because they are an integral part of the existing payments infrastructure.”¹⁵ Still, industry leaders are unsure what laws, if any, currently govern mobile payments.¹⁶ An American Bar Association study found that 84% of those banking professionals surveyed ascertain it either very difficult or difficult to identify the laws surrounding mobile payments.¹⁷ With new, non-bank products gaining a foothold in the mobile payments market, the next big questions for legislators and federal regulators moving forward concern which agency should regulate these products, and under what authority.¹⁸

The Consumer Financial Protection Bureau (CFPB) aims to answer that question by proposing regulatory changes that will better define the legal and regulatory landscape for mobile payments.¹⁹ The CFPB “Prepaid Card Rules” were proposed in the fall of 2014, though the CFPB has been working with federal regulatory agencies and the financial services industry for years to draft the changes they have put forth so far.²⁰ These rule changes, if adopted, will help to clear up the regulatory grey area surrounding mobile payments, however the next step is to establish an effective agency to take ownership of American consumers’ privacy and data security concerns. In light of these concerns, the CFPB should propose more comprehensive rule changes, and clearly identify itself as the agency responsible for regulating mobile payments from that point forward. As the CFPB has the ability to promulgate rules through informal rulemaking, a capability that some other federal regulators lack, the CFPB that should create the laws and guidelines to properly regulate mobile payments in an efficient, responsive manner as the industry explodes.

This note will focus on the current regulatory gaps within the mobile payments industry, while addressing the CFPB’s proposed rule changes. Part I will examine how the technologies behind mobile payments work, and differentiate mobile payments from mobile banking, which is currently regulated in the United States.²¹ Part II will discuss the existing regulations

13. See generally Eric Ravenscraft, *What's the Best Way to Send Money Online*, LifeHacker (Sept. 20, 2013), <http://lifelifehacker.com/whats-the-best-way-to-send-money-online-1342156640>.

14. See generally FDIC: MOBILE PAYMENTS, *supra* note 2.

15. *Id.*

16. See generally STEPHEN T. MIDDLEBROOK, MOBILE PAYMENTS LEGAL AND REGULATORY SURVEY (2010).

17. *Id.* at 1.

18. See generally *The Future of Money Hearing*, *supra* note 8.

19. See generally CFPB Prepaid Card Rule, *supra* note 12.

20. *Id.*

21. M. MacRae Robinson, *Easing the Burden on Mobile Payments: Resolving Current Deficiencies in Money Transmitter Regulation*, 18 N.C. Banking Inst. 553, 3 (2014).

in the mobile payments marketplace, and where there are gaps. There are currently many laws regulating mobile banking, and no clear precedent for how these laws will affect mobile payments. A critical next step is to establish a leading regulatory agency to determine what laws govern mobile payments. Part III will explore the federal regulatory agencies currently at play in the mobile payments marketplace, and which of these agencies is best poised to take on a larger role in regulating mobile payment applications. Many regulatory agencies are capable of regulating mobile payments, and it has become essential to identify which agency is best poised to regulate mobile payments in the future. Part IV will examine what effect the prepaid card rules proposed by the CFPB will have on mobile payments,²² and how these proposed rules fail to adequately address the privacy and data security concerns of American consumers. Finally, Part V will discuss the best course of action to address privacy and data security concerns surrounding mobile payments, and address which regulatory agency should take the lead in this emerging marketplace.

With new players joining the mobile payments game every day, a dichotomy exists between the benefits to consumers, and risk to their privacy. As noted by the Federal Trade Commission (FTC), “Mobile payments can allow multiple players within the mobile payments ecosystem to gather and consolidate personal and purchase data in a way that was not possible under the traditional payments regime.”²³ Despite these many benefits to consumers, it also creates many privacy and data security risks that are not properly addressed under the current regulatory system in the United States, leaving many mobile payment products users unprotected. As such, this note will argue why one regulatory agency, the CFPB, is the best choice to take ownership of regulating mobile payment privacy and data security in the future

I. EXPLORING HOW MOBILE PAYMENTS WORK, AND THE ISSUES SURROUNDING PRIVACY AND DATA SECURITY

The mobile payments atmosphere is large and diverse,²⁴ with new companies constantly emerging and attempting to stake a claim for the future of the industry.²⁵ It is often unclear where these new mobile payment products fall within the current regulatory structure, if they can be

22. See generally CFPB Prepaid Card Rule, *supra* note 12.

23. FEDERAL TRADE COMMISSION, PAPER, PLASTIC... OR MOBILE? [hereinafter FTC: PAPER, PLASTIC, OR MOBILE] at 13 (2013).

24. See Jason Ankeny, *Financial Execs Survey: Mobile Payments Going Mainstream by 2015*, FierceMobileContent.com, July 13, 2011, <http://www.fiercemobilecontent.com/story/financial-execs-survey-mobile-payments-going-mainstream-2015/2011-07-13>.

25. FTC: PAPER, PLASTIC, OR MOBILE, *supra* note 23, at 13 (2013) (stating “several of the country’s largest and most well known companies – including Goggle, Intuit, AT&T, Verizon, T-Mobile, Visa, MasterCard and VeriFone – have entered or increased their presence in the mobile payments market. Small start-ups such as Dwolla, LevelUp, and Boku are also vying for a seat at the table.”).

regulated at all, and different forms of mobile payments are driven by very different technologies.²⁶ The FDIC stated in its “Mobile Payments” working paper,

Mobile payments require the coordinated and secure exchange of payment information among several unrelated entities... Depending on the type of mobile payment, financial institutions may find that the effective management of risks involves partnering with application developers, mobile network operators, handset manufacturer, specialized security firms and others.²⁷

As new players break into the industry, understanding how these various mobile payment technologies work is key in understanding how they should be regulated.

A. Differentiating Mobile Payments from Mobile Banking

To a casual observer, mobile payments and mobile banking may appear to be the same, but, the two systems are actually separate entities that fall into different regulatory spheres.²⁸ Mobile payments are typically businesses and nonbank entities that use either mobile devices or internet-enabled devices to provide payment services between peers.²⁹ These payments can occur between friends, strangers, or merchants and customers.³⁰ Typically, mobile payments use funds taken from a prepaid card or pooled bank accounts held by third parties to make a purchase or transaction.³¹ Mobile payment systems utilize a customer-nonbank relationship where electronic value is issued in exchange for cash when a third party matches the value for those assets through a pooled account in a licensed bank.³²

Mobile banking, on the other hand, revolves around a customer relationship with their financial institutions or banks.³³ Typically, mobile banking involves accessing an individual's financial accounts through a mobile device, rather than the transaction of funds to or through a third

26. See generally FTC: PAPER, PLASTIC, OR MOBILE, *supra* note 23.

27. FDIC: MOBILE PAYMENTS, *supra* note 2.

28. See generally *The Future of Money Hearing*, *supra* note 8.

29. Robinson, *supra* note 21, at 1-2.

30. *Id.*

31. *Id.*

32. TANAI KHIAONARONG, OVERSIGHT ISSUES IN MOBILE PAYMENTS, 8 (Ghiath Shabsigh, 2014).

33. *Id.*

party.³⁴ Mobile banking technologies use intra-bank and inter-bank payment networks, and simply rely on existing bank-customer relationships, facilitated through electronic channels.³⁵ Many of the technologies surrounding mobile banking are already regulated as these technologies are considered an extension of the bank account.³⁶ As such, questions largely revolve around how to best regulate mobile payments, as some mobile payment technologies are yet to be firmly established within the current regulatory system.³⁷

B. Various Forms of Mobile Payments

There are many different technologies that drive the mobile payments industry. Beyond the organizations present in traditional transactions: banks, merchants, and payment card networks,³⁸ the FTC states that new parties, including “operating system manufacturers, hardware manufacturers, mobile phone carriers, application developers, and coupon and loyalty program administrators” are taking a larger role in the mobile payments industry.³⁹ Understanding the roles these organizations aim to take in the mobile payments atmosphere, and the technologies used in each consumer experience will give a better understanding on how to regulate mobile payment systems moving forward.

1. Carrier Based Mobile Payments

One form of mobile payment is mobile carrier based billing. In this system, a third party bills a consumer’s mobile service provider, and then the charge for the transaction is found on the consumer’s monthly phone bill.⁴⁰ This type of billing is problematic because currently, there are no federal regulations in place to monitor mobile carrier billing.⁴¹ Instead, consumers are left to rely on voluntary safeguards and privacy provisions enacted by individual mobile carrier companies.⁴²

Regulating these types of payments is difficult, and not covered under the current banking regulatory structure. This is largely because mobile phone networks are regulated by the Federal Communications Commission (FCC)⁴³ and the FCC has oversight over mobile carrier companies.⁴⁴ As stated by the Clearing House, LLC,

34. Robinson, *supra* note 21, at 2.

35. KHIAONARONG, *supra* note 32, at 5.

36. *Id.*

37. *See generally The Future of Money Hearing, supra* note 8.

38. *Id.*

39. FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23, at 2.

40. Robinson, *supra* note 21, at 4.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*

Although in some cases federal consumer protection laws that also apply to bank payment services may apply, the bank supervisory regime does not, making enforcement of these laws, as well as the security and integrity of the payments process, less certain.⁴⁵

In other words, some regulatory agencies may be able to regulate these payments through consumer protection laws, but these laws may only cover specific infractions by a mobile carrier company. However, mobile carrier based payment systems fall into a different regulatory atmosphere than most mobile payments, and will not be covered further in this note.

2. Remote & Proximity Mobile Payments

The two major subdivisions of mobile payments most commonly used are classified as remote and proximity mobile payments.⁴⁶ Companies such as Amazon, Google, PayPal, Square, and Venmo are involved in each of these spaces.⁴⁷ Though remote and proximity payments may be regulated similarly in the future, how the technology driving each segment of mobile payments operate in very different ways.

In proximity mobile payments, a consumer typically puts his mobile device on or around a point of sale terminal, which in turn will read a unique Near Field Communication (NFC) chip embedded in the phone.⁴⁸ The phone then sends transactional data either to the consumer's bank or a third party, which approves or declines the funds for the purchase.⁴⁹

In a remote mobile payment, a customer does not need a point of sale terminal to interact with, and instead can use their phone's data, either through the internet or a text messaging service, to engage in the transaction.⁵⁰ Typically, the consumer will set up an account with a mobile payment service provider such as PayPal, which will then facilitate a transaction through text based messaging between the customer and the application, which is tied to a consumer's bank account.⁵¹

45. *The Future of Money Hearing*, *supra* note 8, at 41 (statement of The Clearing House Association L.L.C.).

46. David W. Freese & Timothy R. McTaggart, *Regulation of Mobile Payments*, 127 *The Banking L.J.* 485, 486-487 (2010).

47. Robinson, *supra* note 21, at 2 (stating "Mobile payment businesses such as Google, PayPal, Amazon, and Square offer a variety of mobile payment services.") *see also* Alison Griswold, *Venmo Money, Venmo Problems*, *Slate* (Apr. 5, 2015), http://www.slate.com/articles/technology/safety_net/2015/02/venmo_security_it_s_not_as_strong_as_the_company_wants_you_to_think.single.html.

48. Freese & McTaggart, *supra* note 46, at 486-489.

49. *Id.*

50. *Id.*

51. *Id.*

Some applications, such as Google's mobile payment system, Google Wallet,⁵² are creating a major concern for regulators.⁵³ Instead of working directly with a bank account, or acting as an extension of one's bank account on their phone, which is already covered in existing regulation,⁵⁴ Google Wallet uses a company called The Bancorp, Inc. to facilitate its transactions.⁵⁵ When a consumer purchases a product from a merchant, either through a remote or proximity payment, The Bancorp, Inc. issues a prepaid MasterCard debit card for the exact amount of the transaction.⁵⁶ Google Wallet then debits the prepaid card towards the merchant in the particular sale, and then also debits the same amount from one of the customer bank accounts that is stored in Google Wallet.⁵⁷ This payment system uses what is referred to as "prepaid cards" and "pooled accounts". The pooled account is made up of many consumers' funds, pooled together in The Bancorp Inc., and the prepaid card issued by MasterCard facilitates the transaction from this account.⁵⁸ Other mobile payment applications, such as Venmo,⁵⁹ maintain stored balances in the application that can be used to transact with merchants and peers.⁶⁰ In addition to the existing regulatory gaps surrounding these stored balances discussed below, these stored balances create concerns for consumers, as they are not insured by the FDIC, and often funds from these accounts are pooled and invested for the benefit of the mobile payment company.⁶¹

Companies using prepaid cards and pooled bank accounts are not clearly and effectively regulated by the current federal regulatory scheme, leaving consumers' privacy and data security at risk. The Consumer Financial Protection Bureau (CFPB) aims to address these risks through changes to existing regulations,⁶² however, the changes proposed by the CFPB may still not be comprehensive enough. To fully understand the effect any proposed rule changes may have, examining the current regulatory structure and what changes need to be made to better protect consumers is vital.⁶³

52. Robinson, *supra* note 21, at 2.

53. *See generally* *The Future of Money Hearing*, *supra* note 8.

54. *See generally* Rajan, *supra* note 3.

55. Robinson, *supra* note 21, at 2.

56. *Id.*

57. *Id.*

58. *Id.*

59. Alison Griswold, *Venmo Money, Venmo Problems*, Slate (Apr. 5, 2015), http://www.slate.com/articles/technology/safety_net/2015/02/venmo_security_it_s_not_as_strong_as_the_company_wants_you_to_think.single.html.

60. *See generally* Robinson, *supra* note 21.

61. *Id.*

62. *See generally* CFPB Prepaid Card Rule *supra* note 12.

63. *See generally* *The Future of Money Hearing*, *supra* note 8.

C. Data Security and Privacy Issues

With new, diverse technologies driving mobile payments forward, it is no surprise that many consumers are anxious about the security of their data and private information.⁶⁴ Mobile payment companies have begun to address these concerns by installing security provisions for their customers. Some mobile payment systems allow for “end-to-end encryption”,⁶⁵ or encryption throughout the entire payments process, and store payment information separately from the rest of a mobile device’s memory.⁶⁶ However, not every mobile payment company uses these security provisions,⁶⁷ and there are no laws currently that explicitly force mobile payment companies to provide these security provisions.

Privacy remains another major concern for consumers using mobile payment systems.⁶⁸ The FTC stated,

In addition to the banks, merchants, and payment card networks present in traditional payment systems, mobile payments often involve new actors such as operating system manufacturers, mobile phone carriers, application developers, and coupon and loyalty program administrators. When a consumer makes a mobile payment, any or all of these parties may have access to more detailed data about a consumer and the consumer’s purchasing habits as compared to data collected when making a traditional payment.⁶⁹

Consumers using mobile payment systems may find that merchants are able to gain access to enough data to put together a financial profile for a consumer from just one transaction.⁷⁰ Though the FTC has urged companies to adopt privacy and data security provisions to address issues such as these,⁷¹ no law explicitly requires mobile payment companies to adopt any specific data security or privacy provisions.

64. FTC: PAPER, PLASTIC, OR MOBILE, *supra* note 23, at 12.

65. *Id.*

66. *Id.*

67. *Id.*

68. *Id.*

69. FTC: PAPER, PLASTIC, OR MOBILE, *supra* note 23, at 13.

70. *Id.*

71. *Id.*

II. CURRENT REGULATIONS AT PLAY

While banking is a heavily regulated industry, mobile payments exist in a regulatory grey area. As stated by Stephanie Martin, Associate General Counsel for the Federal Reserve Board of Governors in Congress' Future of Money Hearing,

It is difficult to make broad generalizations about the applicability of existing statutes and rules to mobile payments...due to the different types of service providers, bank and nonbank, the wide variety of payment arrangements and the potential applicability of both banking and nonbanking laws to any given arrangement.⁷²

Still, some mobile payment issues are currently being covered by the existing regulatory system. If an application simply acts as a platform for a bank to facilitate a transaction, it will fall under existing banking regulations.⁷³ Currently, there is a statutory framework in place that addresses many traditional payment activities used by banks.⁷⁴ Under these existing laws, using a new mechanism to connect consumers to their financial accounts, such as a smartphone, does not generally result in changes to financial institution's responsibility to the consumer, or a bank customer's basic user rights.⁷⁵ Depending on the method used to facilitate a payment when a nonbank is involved, the current laws may not be properly tailored to address a mobile payment.⁷⁶ As such, many nonbank payment processors operating in the mobile payments space operate as what The Clearing House refers to as "shadow payment processors," as they fall outside of the existing regulatory structure for financial institutions.⁷⁷ Currently, these "shadow payment processors" and other companies that use prepaid debit cards and pooled bank accounts to facilitate transactions fall outside of the existing regulatory scheme.⁷⁸ Not being covered by the current regulatory structure may allow some mobile payment processors to slack on anti-money laundering and customer privacy provisions.

As the Clearing House stated, "the patchwork of regulatory and supervisory regimes applicable to shadow payment providers leaves

72. *The Future of Money Hearing*, *supra* note 8, at 6 (statement of Stephanie Martin, Associate General Counsel, Board of Governors of the Federal Reserve System).

73. *Id.* at 32.

74. *Id.*

75. *Id.* at 35.

76. *Id.*

77. *Id.* at 39

78. *See generally* FTC: PAPER, PLASTIC, OR MOBILE, *supra* note 23.

consumers with varied and often uncertain protections.”⁷⁹ In an effort to address these concerns, some companies have addressed gaps in the regulations through their terms and conditions and contracts with their customers.⁸⁰ Though this is an admirable effort by some companies, consistent regulation is still necessary to establish a consistent precedent across the industry to protect consumers.⁸¹ While the current regulatory structure is vast in scope, it still leaves some gaps in coverage for payment methods that could not have been conceived when many of the existing statutes were written.⁸²

A. Electronic Funds Transfer Act/Regulation E

The Electronic Funds Transfer Act⁸³ (EFTA) was passed in 1978, and codified into law through the FED’s Regulation E.⁸⁴ The EFTA contains rules for electronic fund transfers (EFT)’s, which can include any transaction initiated through a computer, telephone, magnetic tape, or electronic terminal.⁸⁵ These types of transactions can be initiated through automated teller machines (ATM’s), debit card transactions, and direct deposits and withdrawals from a bank account.⁸⁶

While the EFTA generally applies to financial institutions, certain provisions in the EFTA can apply to “any person”⁸⁷ in mobile payment situations where a payment is made from a consumer’s account through an electronic funds transfer.⁸⁸ Specifically, the EFTA applies to “any bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide an EFT service.”⁸⁹ Though currently, who qualifies as “any other person” and whether or not mobile phones count as an “access device” is unclear.

The CFPB aims to address these issues in their pending prepaid card rule,⁹⁰ as the CFPB has interpretive rulemaking authority over the EFTA.⁹¹ The EFTA defines an “access device” as “something used to initiate debit card transactions processed over existing payment card networks.”⁹² The largest ambiguity existing around “access devices” is in situations where a

79. *The Future of Money Hearing*, *supra* note 8, at 41 (statement of The Clearing House Association L.L.C.).

80. FTC: PAPER, PLASTIC, OR MOBILE, *supra* note 23, at 7.

81. *Id.*

82. *See generally The Future of Money Hearing*, *supra* note 8.

83. *See generally* Electronic Fund Transfer Act, 15 U.S.C. § 205 (1978).

84. *See generally* Regulation E, Electronic Fund Transfer Act, 12 C.F.R. 1005 (2009).

85. Electronic Fund Transfer Act § 205.2.

86. *Id.*

87. *Id.* at 205.2(b)(1).

88. FDIC: MOBILE PAYMENTS, *supra* note 2.

89. Freese & McTaggart, *supra* note 46, at 490 (citing Regulation E § 205.2(i)).

90. *See generally* CFPB Prepaid Card Rule *supra* note 12.

91. *The Future of Money Hearing*, *supra* note 8, at 6 (statement of Stephanie Martin, Associate General Counsel, Board of Governors of the Federal Reserve System).

92. Electronic Fund Transfer Act § 205.2.

nonbank initiates a transaction, but does not own the consumer's account being charged for the transaction.⁹³ Until "access devices" are further defined by the CFPB, ambiguity in the statutes results in potential harm to consumers, and the growth of the mobile payments industry. However, it is largely regarded that wireless carriers, even those that engage in mobile carrier billing, are likely not included under this provision, and not subject to the regulations of the EFTA.⁹⁴ Additionally, if a consumer uses a debit card stored on their mobile device to make a payment, the bank issuing the debit card is still required to comply with the EFTA.⁹⁵

One of the main purposes of the EFTA is to establish consumer rights for various required disclosures and error resolution procedures surrounding fraudulent or unauthorized charges.⁹⁶ These disclosures require a terms and conditions for any EFT service offered by the company and information on error resolution procedures.⁹⁷ Additionally, institutions regulated by the EFTA must limit consumer liability to \$50 for unauthorized charges if the charge is reported within two days, and \$500 to any charge coming after two days.⁹⁸ The CFPB has interpretive rulemaking authority over the EFTA,⁹⁹ and as such, will decide what types of disclosures and error-resolution processes are necessary when dealing with an EFT.¹⁰⁰

B. Truth in Lending Act/Regulation Z

The Truth in Lending Act (TILA),¹⁰¹ which was codified under FED Regulation Z,¹⁰² establishes the rules surrounding consumer credit.¹⁰³ TILA was written to give consumers a better sense of the available credit options and to better understand the costs of various credit lines.¹⁰⁴ TILA is meant to apply to creditors that offer credit products such as credit cards, but may apply to mobile payment systems when a mobile payment is funded by a credit card or other TILA covered credit account.¹⁰⁵

Under TILA, creditors must provide consumers with disclosures that describe various credit costs, including interest rates, billing rights, and

93. SUSAN PANDY, UPDATE ON THE U.S. REGULATORY LANDSCAPE FOR MOBILE PAYMENTS 11 (2014).

94. Freese & McTaggart, *supra* note 46, at 490-492, *see also* Regulation E § 205.14.

95. Rajan, *supra* note 3, at 456-458.

96. *Id.*

97. *The Future of Money Hearing*, *supra* note 8, at 12 (2012) (statement of Stephanie Martin, Associate General Counsel, Board of Governors of the Federal Reserve System).

98. Regulation E § 205.6, *see also* Rajan, *supra* note 3, at 456-458.

99. Rajan, *supra* note 3, at 456-458.

100. *See generally* CFPB Prepaid Card Rule, *supra* note 12.

101. Truth in Lending Act, 15 U.S.C. § 1026 (1968)

102. Regulation Z, Truth in Lending Act, 12 C.F.R. §1026 (1969).

103. FDIC: MOBILE PAYMENTS, *supra* note 2.

104. *Id.*

105. *Id.* *see also* Truth in Lending Act § 1026.

dispute resolution procedures.¹⁰⁶ However, as is the case with the EFTA, no federal regulatory agency has yet established what entities must abide by TILA disclosures when mobile payments are involved.¹⁰⁷

C. Federal Trade Commission Act/Unfair, Deceptive, or Abusive Acts and Practices

The FTC Act and the Unfair, Deceptive, or Abusive Acts and Practices (UDAAP) provision of the Dodd Frank Act¹⁰⁸ give the FTC and CFPB powers to prohibit any unfair or deceptive (and abusive in UDAAP) acts or practices used by a company.¹⁰⁹ The acts allow the FTC and CFPB to go after “any person or entity engaged in commerce”;¹¹⁰ giving both agencies a wide net to cast over what companies they can prosecute under each act. Under Section 8 of the Federal Deposit Insurance Act,¹¹¹ the FTC Act and UDAAP also apply to banks and other financial institutions.¹¹² Both acts will apply to mobile payment transactions, regardless of the underlying payment source,¹¹³ and prohibit “unfair or deceptive acts or practices in or affecting commerce”.¹¹⁴ This gives both agencies immense power to regulate wrongdoing in the mobile payments space. However, neither the FTC Act nor UDAAP sets guidelines on how companies “in or affecting commerce”¹¹⁵ should act towards privacy and data security, or the minimum requirements the mobile payments industry must abide by. Both acts are largely reactive to existing problems, and do not do enough to establish a status quo of safe and responsible behavior by mobile payment companies who deal with consumers private data.

D. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) was enacted in 1999 to repeal a section of the Glass-Steagall Act, and allowed for banks, securities companies, and investment companies to consolidate into one institution.¹¹⁶ Additionally, the GLBA set up data security guidelines and privacy rules for depository institutions and any nonbank engaged in financial activity.¹¹⁷ The GLBA applies when a financial institution (or nonbank engaged in

106. Truth in Lending Act § 1026.

107. *See generally* Freese & McTaggart, *supra* note 46.

108. *See generally* Dodd Frank Act, 12 U.S.C. § 5511 (2011).

109. *See* 15 U.S.C. § 45(a), *see also* 12 U.S.C. §5536(a)(1)(B).

110. *See* 15 U.S.C. § 45(a), *see also* 12 U.S.C. §5536(a)(1)(B).

111. 15 U.S.C. § 45(a).

112. *Id.*

113. FDIC: MOBILE PAYMENTS, *supra* note 2.

114. 15 U.S.C. § 45(a).

115. *Id.*

116. LISSA LAMKIN BROOME & JERRY W. MARKHAM, THE GRAMM-LEACH-BLILEY ACT: AN OVERVIEW (2001).

117. Gramm-Leach-Bliley Act, 15 U.S.C. §6801 et seq. (1999).

financial activity) handles the personal information of a customer.¹¹⁸ The GLBA requires financial institutions to provide notices regarding a customer's nonpublic information to its customers, and allow customers to opt out of certain types of information sharing.¹¹⁹ Data security provisions in the GLBA set up guidelines for appropriate safeguards of customer nonpublic information, specifically customer addresses, phone numbers, bank account numbers, social security numbers, income, and credit histories.¹²⁰

To comply with the provisions set forth by the GLBA safeguard rule, a company must "assess risks to customer information, create and monitor a safeguard program, and adjust the program as necessary."¹²¹ This can include specific employee training programs, disciplinary actions for company safeguarding policy violations, and ensuring customer data security.¹²² The GLBA also contains a "Pretexting Protection"¹²³ which requires financial institutions to safeguard unauthorized access to personal accounts and information.¹²⁴

The FTC enforces the GLBA,¹²⁵ and to date, the FTC's definition of what constitutes a financial institution or nonbank engaged in financial activity has been broad.¹²⁶ The FTC's broad definition has led them to expose the GLBA's safeguarding provisions to many institutions, including "banks, check cashing businesses, real estate appraisers, professional tax preparers, and courier services."¹²⁷ Given how broad of a net the FTC has cast over various nonbanks engaging in financial activity, it follows that mobile payment providers may also get roped in to the safeguarding provisions if they become substantially involved financial activity.¹²⁸ However, no mobile payment companies have yet been brought to court under the provisions of the GLBA, and it has not yet been established if mobile payment companies will be subject to the provisions of the GLBA.

E. FDIC Insurance

FDIC insurance insures the funds in an individual customer account at a financial institution in case of the institution's failure.¹²⁹ FDIC insurance applies to all deposits and accounts defined in the FDIC Act and National Credit Union Act,¹³⁰ including savings and checking accounts, and shared

118. *Id.*

119. *Id.*

120. Freese & McTaggart, *supra* note 46, at 494-495

121. Rajan, *supra* note 3, at 459-463.

122. *Id.*

123. 15 U.S.C. §6801 et seq.

124. Rajan, *supra* note 3, at 459-463.

125. 15 U.S.C. §6801 et seq.

126. *See generally* Freese & McTaggart, *supra* note 46.

127. Rajan, *supra* note 3, at 456.

128. *Id.*

129. FDIC: MOBILE PAYMENTS, *supra* note 2.

130. *Id.*

draft accounts at credit unions.¹³¹ Though a mobile payment user's funds will be protected if the underlying paying source is an FDIC insured institution, the funds will not be protected if a nonbank mobile payments provider goes out of business or files for bankruptcy, or if the funds are held in any pooled or prepaid account held by a nonbank.¹³² As many mobile payment systems use pooled accounts when loading consumer funds to a mobile wallet, FDIC insurance will not apply many customers using mobile payments, leaving consumers completely unprotected.¹³³

F. Credit Card Accountability, Responsibility, and Disclosure Act

The Credit Card Accountability, Responsibility, and Disclosure Act (CARD Act) was enacted in 2009, and directs the Financial Crimes Enforcement Network (FinCEN), to issue regulations regarding the

[s]ale, insurance, redemption, or international transport of stored value, including prepaid devices such as plastic cards, mobile phones, electronic serial numbers, key fobs, and or other mechanisms that provide access to funds that have been paid for in advance and are retrievable and transferable.¹³⁴

This act gives FinCEN the ability to set up anti-money laundering and terrorist funding provisions for prepaid cards and mobile phones.¹³⁵

III. FEDERAL REGULATORS AT PLAY

With such a wide array of regulations with potential implications on the mobile payments space, it follows that there is an overload of federal regulatory agencies in the space. With so many regulators at play, a grey area exists over who has oversight of the mobile payments business.¹³⁶ Understanding the roles current agencies play when regulating mobile payment systems will help determine the best methods to regulate the industry moving forward.

131. *Id.*

132. *Id.*

133. See Robinson, *supra* note 21, at 2-3.

134. *The Future of Money Hearing*, *supra* note 8, at 18-31 (2012) (statement of James H. Freis Jr., Director, Financial Crimes Enforcement Network).

135. *Id.*

136. See generally Robinson, *supra* note 21.

*A. Federal Reserve System/ Office of the Comptroller of the Currency/
Federal Deposit Insurance Corporation*

The Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC) are the three primary bank regulators, responsible for ensuring financial institutions across the country comply with various banking laws and regulations. However, congruent to the Dodd Frank Act, consumer protection duties were delegated from these regulators to the CFPB.¹³⁷ Still, the FDIC insures funds held in a bank account tied to a mobile payments account, and all three regulators will continue to regulate the banks underlying mobile payment products.¹³⁸ Despite the FED, OCC, and FDIC's role in regulating banks, these agencies will not have a large role in protecting consumer privacy and data security used by mobile payment systems moving forward.

B. Federal Communications Commission

The Federal Communications Commission (FCC) is in charge of regulating many industries, including wireless service providers.¹³⁹ Though the FCC has yet to propose any laws or rules regulating mobile carrier billing, it is quite possible that they could ultimately end up responsible for such services.¹⁴⁰ As the primary regulator for wireless providers, it follows that the FCC may be the most appropriate authority to manage wireless carrier billing, and the privacy and data security provisions that are included in such a responsibility. However, the FCC will not likely have any authority or responsibility if mobile payments are made using prepaid cards or pooled bank accounts.

C. Financial Crimes Enforcement Network

In 1990, the Department of the Treasury created the Financial Crimes Enforcement Network (FinCEN) to regulate money transmitters, including those products listed in the CARD Act, for criminal activity monitoring purposes.¹⁴¹ All "money service businesses"¹⁴² must register with FinCEN, maintain various financial records, meet reporting requirements, and

137. See Dodd Frank Act § 5511.

138. See generally FDIC: MOBILE PAYMENTS, *supra* note 2.

139. The Federal Communications Commission, *What We Do*, (Apr. 5, 2015), <http://www.fcc.gov/what-we-do>.

140. See generally Electronic Fund Transfers (Regulation E) ANPR, 77 Fed. Reg. 30923 (May 24, 2012).

141. Robinson, *supra* note 21, at 2-3 (2014).

142. 31 C.F.R. § 1010.100(ff)(5) (stating "Money service business. A person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States...This includes but is not limited to maintenance of any agent, agency, branch, or office within the United States.").

establish anti-money laundering programs.¹⁴³ FinCEN may require mobile payment companies to abide by these provisions, but largely to defend against money laundering and terrorist funding, not to protect consumer privacy and data security.

D. Federal Trade Commission

The Federal Trade Commission (FTC) is one of America's oldest consumer protection agencies, recently celebrating 100 years as an institution.¹⁴⁴ The FTC can prosecute companies for violating the FTC Act if the FTC determines the company is engaged in unfair or deceptive acts or practices.¹⁴⁵ Through the FTC Act, the FTC can prosecute mobile payment processors.¹⁴⁶ To date, the FTC has brought cases against tech giants such as Google¹⁴⁷ and Facebook¹⁴⁸, specifically over privacy and data security concerns of these companies' mobile technologies.¹⁴⁹

The FTC states that its interest in mobile payment systems “stems from its mandate to protect consumers in the commercial marketplace, as well as its broad jurisdiction over many of the companies that participate in the mobile payments ecosystem.”¹⁵⁰ The FTC has jurisdiction over these companies through the FTC Act¹⁵¹, the GLBA¹⁵², and provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act.¹⁵³ Through these acts, the FTC shares enforcement jurisdiction with the CFPB over “non-depository providers of financial products or services, such as payment processors”,¹⁵⁴ and this likely includes mobile payment companies and applications. The FTC can also regulate cellular providers when they are not engaged in common carrier activities, which may allow the FTC to regulate mobile carrier billing.¹⁵⁵

The FTC has broad jurisdiction over mobile payment companies, and can protect consumers from unauthorized charges.¹⁵⁶ The FTC has filed cases against Facebook and Google requiring each company to implement

143. *Id.*

144. Federal Trade Commission, *Our History*, (Apr. 5, 2015), <https://www.ftc.gov/about-ftc/our-history>.

145. 15 U.S.C. § 45(a).

146. Robinson, *supra* note 21, at 3.

147. In the Matter of Google, Inc., 102 F.T.C. 3136 (2011).

148. In the Matter of Facebook, Inc., F.T.C. 4365 (2012).

149. *See generally* In the Matter of Google, Inc., 102 F.T.C. 3136 (2011), *see also generally* In the Matter of Facebook, Inc., F.T.C. 4365 (2012).

150. FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23, at 2.

151. 15 U.S.C. § 45(a).

152. 15 U.S.C. § 6801 et seq.

153. Dodd Frank Act § 5511.

154. FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23, at 3.

155. FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23, at 8.

156. FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23, at 3 (stating “The FTC’s jurisdiction reaches any person, partnership or corporation that affects commerce, except for limited exclusions such as depository institutions.”) *see also* 15 U.S.C. § 45(a)(2).

comprehensive privacy programs for mobile and online services.¹⁵⁷ Additionally, the FTC has held workshops regarding mobile payment issues,¹⁵⁸ and issued privacy reports urging companies to adopt basic privacy principles.¹⁵⁹ The FTC can likely also provide guidelines for privacy and data security for mobile payment companies through the GLBA.¹⁶⁰ However, in addition to sharing enforcement and regulation powers with the CFPB, the FTC's use of the regulations they have power over do not explicitly protect consumer privacy and data security if used by a mobile payment company. Though many of the laws the FTC enforces *may* have an effect on mobile payment companies, none of these laws or statutes has been used to prosecute or require anything from mobile payment companies. As such, mobile payment companies may operate outside of the regulatory atmosphere of the FTC, leaving consumer's privacy and data security vulnerable.

E. Consumer Financial Protection Bureau

The Consumer Financial Protection Bureau (CFPB) was established in 2011 through the passage of the Dodd Frank Wall Street Reform and Consumer Protection Act.¹⁶¹ The CFPB has rulemaking and interpretive authority of federal consumer protection statutes that will relate to mobile payment transactions.¹⁶² To date, mobile payment systems have not been explicitly included in a majority of these federal consumer protection statutes.¹⁶³ The CFPB proposes to change this with the CFPB's proposed "prepaid card" rule, which will firmly establish mobile payments as falling into the regulatory structure of the EFTA and TILA.¹⁶⁴

Currently, the CFPB has authority over mobile payments if a credit card or banking institution is involved in the underlying payment,¹⁶⁵ but it is not yet established whether the CFPB has authority over mobile payment transactions that involve nonbanks.¹⁶⁶ However, under UDAAP,¹⁶⁷ the CFPB is similarly poised with the FTC to prosecute mobile payment

157. In the Matter of Google, Inc., 102 F.T.C. 3136 (2011), *see also* In the Matter of Facebook, Inc., F.T.C. 4365 (2012).

158. *See generally* FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23.

159. *Id.* at 14 (2013) (stating "At its core, the Privacy Report urged companies to adopt three basic practices: (1) 'privacy by design,' (2) simplified choice for businesses and consumers, and (3) greater transparency").

160. 15 U.S.C. §6801 et seq.

161. Dodd Frank Act § 5511.

162. *The Future of Money Hearing, supra* note 8, at 8 (2012) (statement of Stephanie Martin, Associate General Counsel, Board of Governors of the Federal Reserve System).

163. FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23, at 6.

164. *See generally* CFPB Prepaid Card Rule *supra* note 12.

165. *The Future of Money Hearing, supra* note 8, at 8 (2012) (statement of Stephanie Martin, Associate General Counsel, Board of Governors of the Federal Reserve System).

166. *Id.*

167. 12 U.S.C. §5536(a)(1)(B).

companies that the CFPB determines uses unfair, deceptive, or abusive acts or practices. As mentioned previously, these provisions are very reactive to wrong doing, and do not do an ample job of establishing guidelines to best protect consumer privacy and data security. The CFPB's Card and Payments Markets Division noted in a meeting with industry stakeholders that its three primary mobile payment concerns were disclosures, error resolution procedures, and security.¹⁶⁸ The pending prepaid rule will address disclosures,¹⁶⁹ but leaves much to be desired in the ways of data security and privacy.

IV. CFPB PROPOSED PREPAID CARD RULE

As indicated above, though there are many regulations at play in the mobile financial realm, a majority of these do not do an adequate job of protecting consumer privacy and data security. While Regulation E¹⁷⁰ and Z¹⁷¹ provide provisions that could be helpful in protecting consumers using mobile wallets funded by prepaid cards and pooled bank accounts, these regulations have not yet been adopted to clearly include these types of mobile wallets within the scope of products they regulate.¹⁷²

Prepaid cards and mobile wallets are gaining a foothold on ground previously dominated by debit and credit cards, especially in underbanked communities because mobile wallets cost less for consumers to maintain, do not include costly overdraft fees, and do not subject customers to credit checks.¹⁷³ As American consumers load tens of billions of dollars onto prepaid cards and mobile wallets,¹⁷⁴ the CFPB has brainstormed how to best protect consumers in this new space.¹⁷⁵ Currently, users of prepaid cards or mobile wallets are only guaranteed a few protections dealing with certain usage fees and expiration dates,¹⁷⁶ so the CFPB has aimed to amend Regulations E and Z to provide more comprehensive protections.¹⁷⁷

In December 2014, the CFPB published its proposed amendments to the EFTA (Regulation E) and TILA (Regulation Z).¹⁷⁸ The aim of the proposed changes is to “create comprehensive consumer protections for

168. PANDY, *supra* note 93, at 7 (stating “On June 11, 2014, the CFPB issued a press release announcing the launch of an RFI to collect information about mobile financial services, and products from the industry, including mobile access to the underserved, real-time money management, customer service and privacy concerns, and data breaches.”).

169. *Id.*

170. Regulation E, Electronic Fund Transfer Act § 1005.

171. Regulation Z, Truth in Lending Act §1026.

172. Robinson, *supra* note 21, at 2-3.

173. *Id.* at 3-4.

174. *Id.* at 1, *see also* FED REPORT, *supra* note 1, at 2.

175. *See generally* Robinson, *supra* note 21, *see also generally* *The Future of Money Hearing*, *supra* note 8.

176. *See generally* Robinson, *supra* note 21.

177. *See generally* CFPB Prepaid Card Rule *supra* note 12.

178. *Id.*

prepaid financial products”¹⁷⁹ by changing various definitions within Regulation E.¹⁸⁰ Specifically, the proposed changes will change the definition of a “prepaid account” to include

[c]ards, codes, or other devices capable of being loaded with funds, not otherwise accounts under Regulation E and redeemable upon presentation at multiple, unaffiliated merchants for goods or services, or usable at either automated teller machines or for person-to-person transfers, and are not gift cards (or certain other types of limited purpose cards).¹⁸¹

Under this new definition of “prepaid account”, new consumer protection rules will apply to mobile wallets under Regulations E and Z.¹⁸²

The proposed rule will modify Regulation E to establish disclosure requirements regarding prepaid accounts, which will be provided by financial institutions.¹⁸³ Financial institutions must provide these disclosures to consumers both before and after a consumer establishes a mobile wallet using a prepaid card.¹⁸⁴ The proposed changes will allow mobile payment providers to offer alternative disclosure methods to consumers to allow them to check account balances and information instead of sending regular, periodic statements.¹⁸⁵ Additionally, the changes would require mobile payment companies to provide the CFPB with their mobile wallet terms and conditions.¹⁸⁶ All of these terms and conditions would be maintained by the CFPB on its website, in addition to individual company websites, and made available to consumers.¹⁸⁷

More important provisions in the proposed changes will include prepaid accounts in the services covered under Regulation E’s limited liability and error resolution provisions.¹⁸⁸ These changes will include mobile wallets using prepaid cards such as GoogleWallet. The proposed changes will also amend Regulation Z and E to allow the CFPB to regulate prepaid card accounts and mobile wallets that have credit features and overdraft services.¹⁸⁹ This amendment will classify prepaid cards that use overdraft or credit features as credit cards subject to Regulation Z and its

179. *Id.*

180. *Id.*

181. CFPB Prepaid Card Rule *supra* note 12, at 1.

182. *Id.*

183. *Id.*

184. *Id.*

185. *Id.*

186. CFPB Prepaid Card Rule *supra* note 12, at 2.

187. *Id.*

188. CFPB Prepaid Card Rule *supra* note 12, at 5.

189. CFPB Prepaid Card Rule *supra* note 12, at 2.

related credit card rules.¹⁹⁰ The proposed changes in these provisions would require that consumers consent to credit services and overdraft features, and allow consumers at minimum, 21 days to repay any debts stemming from the use of credit or overdraft features.¹⁹¹

Similarly, the proposed changes will amend Regulation E to require prepaid card and mobile payment companies to issue disclosures regarding overdraft and credit features linked to mobile wallets and prepaid accounts.¹⁹² The changes would also amend Regulation E to prohibit prepaid account companies from requiring consumers to set up preauthorized electronic fund transfers to pay debts on any credit or overdraft feature.¹⁹³

The proposed changes will also modify Regulation E to adopt specific prepaid account error resolution procedures and limited liability provisions.¹⁹⁴ As Regulation E currently limits liability to consumers for unauthorized transfers made through financial institutions if reported in a timely fashion, the proposed changes will look to extend this limited liability to prepaid accounts and mobile wallets.¹⁹⁵ Additionally, the proposed changes will include prepaid accounts to the regulatory regime of Regulation E, with a few modifications for timing requirements for unauthorized transfers and errors resulting from any periodic statement provision.¹⁹⁶ All of these changes will extend Regulation E only to registered prepaid accounts.¹⁹⁷ Through the proposed rule, if certain conditions are met, financial institutions that offer prepaid cards will be exempted from various long-form disclosures typically required under Regulation E until the consumer has actually acquired the prepaid account.¹⁹⁸

V. REGULATORY GAPS AND MOVING FORWARD WITH MOBILE PAYMENT SYSTEMS

The proposed changes to TILA and the EFTA do not do an adequate job of completely covering the regulatory gaps that exist in the mobile payments industry. Not only do the current regulations not go far enough, but also it is not clear which federal regulator should have lead authority over mobile payment systems.¹⁹⁹ Addressing each of these issues by establishing a clearer and regimented regulatory structure will help the mobile payments industry grow in the face of perceived privacy and data security concerns.

190. *Id.*

191. *Id.*

192. CFPB Prepaid Card Rule *supra* note 12, at 6.

193. CFPB Prepaid Card Rule *supra* note 12, at 2.

194. *Id.*

195. *Id.*

196. *Id.*

197. CFPB Prepaid Card Rule *supra* note 12, at 6.

198. *Id.* at 5.

199. *See generally* FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23.

A. Remaining Regulatory Concerns

Mobile payments may be covered under many different regulations, though many of the regulations react to wrongdoing, instead of proactively preventing it. Through UDAAP and the FTC Act, the FTC and CFPB can prosecute mobile payment companies engaging in deceptive or unfair behavior,²⁰⁰ however, neither agency can do anything until wrongdoing occurs. While the CFPB's prepaid card rule does work to protect consumers by establishing error resolution and limited liability provisions,²⁰¹ these provisions mostly help consumers after something wrong has happened. Additional provisions should be written into the proposed prepaid card rule changes to better protect a consumer before some wrong doing, as more forward-looking provisions would help establish trust in the mobile payments industry. The existing disclosure and informational provisions of the EFTA and TILA simply do not go far enough to fully protect consumers using mobile payment systems. Neither the EFTA, nor TILA, establish any guidelines regarding how to best protect consumer privacy or secure consumer data.

One of the best ways to address the issues remaining after the potential adoption of the CFPB's prepaid card rule, would be to use the existing regulatory framework. While the EFTA and TILA are good resources to start creating more protections for consumers using mobile payments, the GLBA should also be used to establish privacy and data security provisions from mobile payment companies. The safeguarding and privacy protections established under the GLBA²⁰² would fit well over the mobile payments industry, and may already apply.²⁰³ The GLBA gives the FTC enforcement authority over financial institutions and nonbanks engaged in financial activity,²⁰⁴ though it has not yet been established whether the GLBA provisions will apply directly to mobile payment companies.²⁰⁵ As such, the FTC could write in a provision to the GLBA, similar to the one in the CFPB's proposed prepaid card rule.²⁰⁶ This provision could clearly enumerate mobile payment companies as "nonbanks engaging in financial activity,"²⁰⁷ and put mobile payment companies under the regulatory structure of the GLBA. Until the FTC uses its authority under the GLBA to establish standards in the mobile payments industry, consumers will be at risk.

Provisions such as those found in the GLBA, are necessary to best protect consumers as they begin to adopt mobile payment systems. However, since Congress, the federal regulators, and courts have not yet

200. 12 U.S.C. §5536(a)(1)(B).

201. See CFPB Prepaid Card Rule *supra* note 12, at 2.

202. 15 U.S.C. §6801 et seq.

203. 15 U.S.C. §6801 et seq. *see also*, Freese & McTaggart, *supra* note 46.

204. See generally 15 U.S.C. §6801 et seq.

205. See generally Freese & McTaggart, *supra* note 46.

206. See CFPB Prepaid Card Rule *supra* note 12, at 2.

207. See generally 15 U.S.C. §6801 et seq.

established that the GLBA will directly apply to mobile payments, consumers have been left to rely on mobile payment companies themselves to protect consumer information.²⁰⁸ Though banks handling consumers' personal information are subject to the provisions of the GLBA,²⁰⁹ many mobile payment transactions involve third parties who are not clearly regulated by the GLBA.²¹⁰ In response to issues like this, some mobile payment companies have voluntarily adopted GLBA-like provisions.²¹¹ Timothy McTaggart, a leading authority on mobile payment issues, recommends that all banks and mobile payment companies ensure that mobile payment initiatives are clearly covered by each company's individual safeguarding policies and third party vendor contracts.²¹² The industry as a whole would benefit from these provisions being statutorily required and enforced by a federal agency.²¹³

B. Who Should Take Ownership of Mobile Payment Systems?

Through the convoluted regulatory structure and various hearings, reports, and workshops held regarding mobile payments, two federal regulators have come out as the chief regulators of the mobile payments industry.²¹⁴ The FTC and CFPB currently share a joint custody of sorts over regulating the mobile payments industry, largely through the expansive powers granted to each agency through UDAAP. Other federal regulators, such as the FED and FinCEN have already carved out the specific instances in which they will regulate the mobile payments industry,²¹⁵ leaving most of the regulatory burden on the shoulders of the FTC and CFPB.

The FTC may already have the power to regulate mobile payments through use of the GLBA.²¹⁶ The FTC Act gives the FTC broad discretion to regulate mobile payment companies that are engaging in deceptive or unfair behavior.²¹⁷ However, the CFPB currently shares enforcement under this umbrella through UDAAP.²¹⁸ The FTC has been a leader in protecting consumer data online through filing multiple cases against tech giants such as Google²¹⁹ and Facebook.²²⁰ While the FTC may currently have the

208. See generally Freese & McTaggart, *supra* note 46.

209. *Id.*

210. *Id.*

211. See generally *PayPal User Agreement*, PayPal (Nov. 18, 2014), <https://www.paypal.com/us/webapps/mpp/ua/useragreement-full>.

212. Freese & McTaggart, *supra* note 46, at 495.

213. *Id.*

214. FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23, at 3.

215. See generally *The Future of Money Hearing*, *supra* note 8.

216. Freese & McTaggart, *supra* note 46, at 495.

217. 15 U.S.C. § 45(a).

218. *Id.*

219. See generally *In the Matter of Google, Inc.*, 102 F.T.C. 3136 (2011).

220. See generally *In the Matter of Facebook, Inc.*, F.T.C. 4365 (2012).

power to properly regulate mobile payments, going forward the CFPB should take the lead on regulating the industry.

Currently, the CFPB does not have the same powers as the FTC to regulate the mobile payments industry. The FTC can likely do more to regulate the privacy and data security concerns of the mobile payments industry through the GLBA, and this is a power, which, even with the enactment of the proposed prepaid card rule, the CFPB will lack.²²¹ However, the CFPB is positioning itself to be the lead regulator on mobile payments²²² and can work towards accomplishing this goal through the use of UDAAP and the new provisions being added by the CFPB's proposed prepaid card rule.

The prime reason the CFPB should be the lead federal regulatory agency regarding mobile payments revolves around one of the major weaknesses of the FTC. Many agencies have two different types of authority when promulgating rules.²²³ Under the Administrative Procedure Act (APA), most federal agencies are given the power to adjudicate through both informal and formal rulemaking.²²⁴ However, the FTC does not have this option after having the ability to promulgate rules through the informal process stripped from it in 1980.²²⁵ As such, the FTC has to either rely on formal rulemaking, which can take years to get anything done,²²⁶ or depend on Congress to grant the FTC the power to use informal rulemaking in a specific situation.²²⁷ The CFPB does not have this limitation on its powers²²⁸ and hence is the better option to regulate the changing industry of mobile payments.

Limits also exist on the CFPB using the APA to promulgate a rule.²²⁹ These limits require the CFPB to analyze economic impacts of any potential rule they promulgate and balance the costs and benefits of the rule.²³⁰ Additionally, the CFPB "shall issue a notice of proposed

221. See generally BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, IN THE MATTER OF REQUEST FOR COMMENT ON ADVANCE NOTICE OF PROPOSED RULEMAKING ELECTRONIC FUND TRANSFERS (REGULATION E) AND GENERAL PURPOSE RELOADABLE PREPAID CARDS (2012).

222. See generally Erin F. Fonte, *Mobile Payments in the United States: How Disintermediation May Affect Delivery of Payment Functions, Financial Inclusion and Anti-Money Laundering Issues*, 8 Wash J.L. Tech & Arts 419 (2013).

223. See generally Heath P. Tarbert & Sunny J. Thompson, *Dodd-Frank, One Year Later: A Primer on the Federal Rulemaking Process*, The Metropolitan Corporate Counsel (August 1, 2011), <http://www.metrocorpcounsel.com/articles/15041/dodd-frank-one-year-later-primer-federal-rulemaking-process>.

224. *Id.*

225. See generally Joshua D. Wright, *Expanding FTC's Rulemaking and Enforcement Authority*, The Federalist Society, (May 26, 2010), <http://www.fed-soc.org/publications/detail/expanding-ftcs-rulemaking-and-enforcement-authority>.

226. See generally Tarbert & Thompson, *supra* note 223.

227. Spinelli, Cooper J. (2014) "Far From Fair, Farther From Efficient: The FTC and the Hyper-Formalization of Informal Rulemaking," *Legislation and Policy Brief*: Vol. 6: Iss. 1, Article 3 at 159.

228. Tarbert & Thompson, *supra* note 223.

229. *Id.*

230. *Id.*

rulemaking whenever a majority of the States has enacted a resolution in support of the establishment or modification of a consumer protection regulation issued by the CFPB.²³¹ Still, these limits are minor, especially in comparison to the inability of the FTC to use informal rulemaking in most circumstances.

While the CFPB does not currently have the power to amend the GLBA,²³² the CFPB has more freedom to create and amend rules than the FTC. An ability to quickly make changes is necessary, as the technology surrounding mobile payments is constantly changing. As such, the CFPB should establish itself as the lead regulatory agency of mobile payments due to its power to react in a timely fashion to this developing industry.

Without establishing a single regulatory agency to own the issues surrounding mobile payments, consumer trust in these systems will remain stagnant and stifle an industry as it looks to explode.²³³ The CFPB taking ownership over regulation of mobile payments and establishing a stricter regulatory structure that focuses on standards for protecting consumer data and private information will help the mobile payments industry grow in the United States.

CONCLUSION

As addressed in the FED's Consumer and Mobile Financial Services report, a large number of cell phone users do not use mobile payment systems due to concerns regarding their individual privacy and data security.²³⁴ Since concerns about whether increased regulation will hurt the innovative process surrounding mobile payments remain,²³⁵ establishing consumer trust is necessary for the mobile payments industry to grow.²³⁶ With 62% of consumers concerned about their privacy when using mobile payment systems,²³⁷ a lead agency, the CFPB, needs to establish itself as the go-to agency for issues concerning mobile payments. Many statutes that may have a hand in regulating mobile payments already exist, yet none of these statutes has directly addressed the issue of mobile payments. Through the CFPB's proposed prepaid card rule, more information and disclosures will be provided to consumers; however, this is not enough to adequately protect consumer privacy and data security. An agency needs to address whether the GLBA will directly apply to mobile payments. While the FTC currently has enforcement power under the GLBA, the CFPB should work to take a larger role in the mobile payments industry. The CFPB's proposed changes to the EFTA and TILA do not go far enough to protect consumer data and privacy, and the CFPB should adopt more

231. Dodd-Frank Act, § 1041(c)(1).

232. 12 U.S.C. §5536(a)(1)(B).

233. FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23, at 12.

234. *See generally* FED REPORT, *supra* note 1.

235. *See generally* *The Future of Money Hearing*, *supra* note 8.

236. FTC: PAPER, PLASTIC, OR MOBILE *supra* note 23, at 12.

237. FED REPORT, *supra* note 1 at 13.

regulations in the mobile payment space. Through the powers the CFPB possesses to promulgate informal rulemaking under the APA, the CFPB should adopt provisions similar to those found in the GLBA to establish data security and privacy procedures for mobile payment companies. Clearing the fog surrounding the mobile payments industry will help to establish consumer trust in mobile payment systems and allow for the mobile payments industry to thrive moving forward.