THE EVOLUTION OF BANKING:
A FLEXIBLE FIDUCIARY DUTIES
APPROACH WILL HELP BETTER PROTECT
MOBILE BANKING CONSUMERS

Isabel Peres

TABLE OF CONTENTS
I. Introduction................................................................. 212
II. Background................................................................. 215
   A. Current Regulation of Mobile Financial Services .............. 215
   B. What are the Characteristics of the Mobile Financial Industry
       and the Unique Risks to Consumers................................. 217
       1. What Exactly Are Mobile Financial Service: Mobile
          Banking and Mobile Payments................................. 217
       2. Participants in the Mobile Banking and Mobile
          Payment Industries.................................................. 219
       3. Unique Risks for Consumers in the Mobile Financial
          Services Industry.................................................... 220
          a. Third Party Risks................................................. 221
          b. Malware Threats................................................ 223
          c. Fraud and Security Risks..................................... 223
   C. Fiduciary Duties and Banks......................................... 225
      1. The Fiduciary Duty Obligation in a Bank-depositor
         Relationship......................................................... 226
         a. Cases Supporting Fiduciary Duties for Banks............. 227
         b. Cases Holding No Fiduciary Duties for Banks............ 228
   III. Analysis...................................................................... 229
      A. Current Consumer Protection Regulations Applicable to
         Mobile Financial Services: Why Fiduciary Duties Should
         Apply to Mobile Banking............................................. 230

* Isabel Freitas Peres, Esq., University of Illinois College of Law, May 2014. European Master in
  Law and Economics, University of Bologna/University of Hamburg, October 2012. LLM, University of
  Illinois College of Law, May 2010. I thank the JLTP staff for its diligence and dedication to publishing
  excellent work. I would also like to thank my Note Editors, Corbin Freres and Jeremy Tyrrell, for their
  guidance and feedback during the writing and editing of this Note. Professor Summer Kim deserves especial
  praise for her inspiring me to write this Note and for taking the time to share with me her comments and
  corporate and financial laws knowledge. I wish to thank my family in Brazil for their love, support, and
  understanding throughout my extensive law school career. Finally, I wish to thank my supporting husband and
  great friends for their continued support with everything I do.
I. INTRODUCTION

Mobile banking is here to stay. The increased popularity of mobile banking made it to Ellen DeGeneres’ talk show when she recollected the time when depositing a check would be accomplished by the following steps: “You had to sign the back of the check, then you had to fill out one of those deposit slips . . . [t]hen you had to add up all the numbers in your head, then you had to wait in line. Then you got to the front of the line and you had to make small talk with the bank teller . . .”\(^1\)

Mobile finance is a new delivery channel for financial products and services and a growing trend in the United States.\(^2\) Customers like Ellen DeGeneres are now using their mobile devices for checking accounts, shopping, and making purchases.\(^3\) In fact, mobile payment volumes are expected to reach $214 billion in the next three years, and approximately ten percent of the $2 trillion in cash transactions, involving $25 or less, could soon

---

move to mobile.4

While this evolution of technology allows consumers to conduct financial transactions using mobile devices, customers and regulators still expect the same level of consumer protection when using cellphones as they would expect from services at a brick and mortar bank.5 However, this new technology presents different risks than traditional banks. For instance, using mobile phones for financial transactions increases risks related to personal security because the number of intermediaries involved in providing the service increases the likelihood of errors.6 In addition, consumer still face several risks related to wireless carriers still employing outdated encryption technology in the United States.7

Consumers, however, are not alone when it comes to mobile technology. The Federal Trade Commission (FTC) is the independent agency of the U.S. government that protects consumer, by preventing fraud, deception, and unfair business practices.8 The Mobile Technologies unit in the Division of Financial Practices safeguards consumers in the mobile environment.9 This division coordinates mobile enforcement and policy work and develops surveys, reports, and educational materials to highlight mobile practices of concern.10 In a February 2013 report, the FTC noted that while mobile technology benefits consumers, the use of the devices raise a number of potential privacy risks.11 The FTC made recommendations for mobile application providers such as banks that offer mobile banking services, in order to provide “just-in-time [privacy] disclosures,” to require that providers obtain the consent of consumers before sharing sensitive information, and to improve coordination efforts between all parties involved in providing financial services.12 Similarly, a report from the Financial Conduct Authority (FCA), the financial systems regulator in the United Kingdom, raised concerns about the risk of using third parties in providing mobile financial services and about the potential of fraud and security issues in these services.13 According to banking law experts, while consumers demand mobile banking technologies, “banks need to be sure that they meet all their regulatory obligations when providing

---

4. Id.
6. Id.
10. Id.
12. Id.

In September 2014, the FTC issued a statement in response to the Consumer Financial Protection Bureau’s (CFPB) request for comments on the CFPB efforts to safeguard consumers from current unfair billing practices and concerns related to the privacy and security of consumers’ financial information on mobile payments (FTC Statement).\footnote{Request for Information Regarding the Use of Mobile Financial Services by Consumer and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers, Docket No. CFPB 2014-0012 (Fed. Trade Comm’n Sept. 10, 2014), available at http://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-consumer-financial-protection-bureau-regarding-use-mobile-financial-services/140912mobilefinancialservices_update.pdf.} The FTC Statement emphasized the five main consumer protection concerns raised by mobile payment and applications.\footnote{Id. at 6.} The FTC Statement also listed the actions taken by the agency so far to address these concerns, including the FTC’s engagement in policy and outreach activities, and business and consumer education.\footnote{Id. at 5.}

Despite the growing number of mobile banking users, instances of fraud, theft of personal data, and security breaches among consumers still cause an extensive disbelief in the technology.\footnote{See Rethinking Personal Data: Strengthening Trust, WORLD ECON. FORUM (May 2012), http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (discussing how the media appears to report in a daily basis breaches and missteps involving personal data).} Consumers cannot purchase safety from banks because they cannot bargain and contract exactly the terms of their mobile banking services.\footnote{Id. at 6.} Therefore, consumers can only trust their banks. Banks may, however, voluntarily adopt a “zero liability policy” to protect their mobile banking consumers from any losses, but they are not required to by law.\footnote{Id. at 5.} Consequently, consumers have no choice but to trust the knowledge and expertise of their bank, and if errors occur, consumers will blame the bank instead of third parties with whom the bank contracted to provide the service to the consumer’s bank.\footnote{See generally Frank H. Easterbrook & Daniel R. Fischel, Contract and Fiduciary Duty, 36 J.L. & ECON. 425, 432–34 (1993) (listing situations where it is costly to parties to contract fiduciary duties).} Since consumers require a safe banking environment and trust banks to provide such environment, banks make a potential candidate for fiduciary duties in state courts.\footnote{Timothy R. McTaggart & David W. Freese, Mobile Banking: What Banks Need to Know When Outsourcing Their Platforms, BLOOMBERG L. REPS. (2010) (noting that some banks have adopted a policy that “covers consumers for any unauthorized [transactions], including loss of interest, insufficient funds and overdraft charges . . . .”).}

This Note will explore the applicability of fiduciary duties to banks that provide consumers with mobile financial services. Part II will first describe the relevant aspects of the mobile financial services industry and the applicable
regulations. Part III will then analyze how courts may find fiduciary duties to apply to banks to protect consumers from the risks associated with mobile banking. This Note will discuss the case law on fiduciary duties of banks and how courts may apply to the law so that it will encompass the new technology risks presented by mobile banking and mobile payment. One of the major objectives of banking regulation is to guarantee that financial institutions comply with consumer protection laws. Banks, however, should be found not only liable for non-compliance, but also liable for the breach of their duties as a fiduciary to consumers of mobile banking. Part IV will shed a new light on fiduciary duties and will discuss possible solutions. Finally, Part V will conclude with the key ideas from this Note.

II. BACKGROUND

According to Sunil Gupta from the Harvard Business School, “banks will be myopic if they view mobile as just another channel for doing business. Mobile technology is changing the ecosystem of the banking industry . . . .” Mobile banking has become popular because it allows bank customers to, for instance, access accounts, check rates, transfer funds, make payments, and even apply for loans using remote handheld devices. The convenience and functionality that mobile banking affords is in line with the current consumer’s expectations for remote, real-time access to information and services from their banks. At the same time, banks may benefit from automated procedures for banking operations because it allows banks to reduce costs. Accordingly, for banks, one of the main advantages of mobile banking is that it reduces the costs of providing service to the customers. For instance, providing mobile banking services saves on significant managerial costs produced by branch office operations, such as the employment of human resources, rent of location, services, etc. Thus, mobile financial services may be a win-win case for consumers and banks.

A. Current Regulation of Mobile Financial Services

In terms of the regulatory framework of mobile technology, it was
uncertain until 2012 whether the current laws and regulations governing the traditional banking services offered by financial institutions would also apply to mobile banking.30 At a hearing entitled “The Future of Money: Where Do Mobile Payments Fit in the Current Regulatory Structure?” on June 29th of 2012, representatives from the United States Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN), the Federal Reserve Board, and the Consumer Financial Protection Bureau stated that the current financial services regulations also apply to mobile banking.31

Stephanie Martin, the Associate General Counsel at the Federal Reserve Board of Governors, affirmed that current regulations are broad enough to cover many of the mobile banking and mobile payments activities.32 The Federal Reserve Board is, therefore, of the opinion that the current financial service regulations should cover mobile banking and mobile payments activities.

James Freis, director of the FinCEN, also stated that in the eyes of the FinCEN, mobile financial services involve communication and direction from an account holder about their account at a depository institution.33 Thereby, if the use of mobile banking facilitates communication between the financial institution and its customer, then financial institutions are already under the scrutiny of different money laundering requirements.34 In terms of mobile payments, if the transaction involves a consumer directing funds outside of its bank account to affect payments, the FinCEN regulations clearly establish that the acceptance and transmission of funds or other value that substitutes for currency from one person to another person or location constitutes money transmission.35 And if there is a money transmission, any person engaging in this activity would likely be a money services business under the FinCEN’s regulations.


31. Id.; see also Erin F. Fonte, Overview of Mobile Payments in the United States, 32 NO. 8 BANKING & FIN. SERV. PER. Y REP. 1, 5 (2013).

32. Fonte, supra note 31; The Future of Money, supra note 30 (“To the extent nonbanks are involved, whether and the degree to which federal or state statutes and rules are applicable depends on the nonbank’s role in the transaction and the specific provisions of the particular statute or rule.”).

33. Fonte, supra note 31, at 5–6.


35. The Future of Money, supra note 30, at 5–6; Freis Statement, supra note 34.

36. Erin F. Fonte, supra note 31, at 5 (“FinCEN’s regulations also have made it clear that the acceptance and transmission of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another person or location, by any means, constitutes money transmission, and that any person wherever located doing business wholly or in substantial part within the United States engaging in money transmission, regardless of any other business lines the person is engaged in—such as the provision of telecommunications services—would likely be a money services business under FinCEN’s regulations, and as such must register and comply with all the reporting, record-keeping, and monitoring requirements applicable to a money transmitter.”).
Thus, as one that transmits money, one must register and comply with monitoring, reporting, and recordkeeping requirements applicable to a money transmitter. These regulators also stressed that application of such laws is not dependent upon the type of entity engaging in the services (i.e., Financial Institutions (FI), or non-FI), but rather it is dependent on the nature of the underlying activity itself. Thus, bank supervisors appear to have agreed to approach mobile banking and mobile payments practices in a similar fashion to traditional banking. Challenges to the direct application of existing norms to mobile banking will be discussed below.

B. What are the Characteristics of the Mobile Financial Industry and the Unique Risks to Consumers

Safety and soundness of financial institutions, along with consumer protection, are some of the main concerns for financial regulators. In fact, regulators have regarded consumer protection laws and financial laws as complementary to each other. There is no doubt that consumer protection is a core aspect of a stable financial system and that non-compliance can adversely impact the soundness of a financial institution. However, innovation in technology brings challenges to regulators to maintain and enforce consumer protection rules, and non-compliance and consumer protection complications resultant from the development of new technologies may have a direct effect on safety and soundness of the financial system.

In a recent poll conducted by GOBankingRates about the biggest fear of mobile banking users, more than half of those polled revealed that they were worried about identity theft. Thus, if financial institutions want to offer and take advantage of the mobile technology to retain and attract customers, they must also address the needs for safety in providing mobile financial services.

I. What Exactly Are Mobile Financial Service: Mobile Banking and Mobile Payments

Mobile financial services are generally referred to as finance-related services that employ mobile telecommunication technologies, including mobile
banking and mobile payments. Mobile banking can be described as “[an] electronic banking innovation business using mobile network and mobile communication technology to realize connection of mobile phones and other mobile devices to a banking system as well as getting a variety of financial services through the mobile interface or [text message] SMS.”

Typically, mobile banking offers all, or at least most, of the services in which banking activity is involved. For instance, many U.S. banks currently offer some combination of account inquiries and balances, payment and fund transfer services, and branch and ATM location services. According to the Report on Mobile Financial Services (the “Federal Report”) issued by the Federal Reserve Board, the most common mobile banking activities are checking financial account balances or making transaction inquiries (87% of mobile banking users), and transferring money between accounts (53% of mobile banking users). Additionally, 21% of mobile banking users reported using remote deposit capture services to deposit a check with their phone. In the United States, banks generally offer mobile financial services through three delivery channels: SMS, mobile web programs, and mobile applications (apps). For instance, apps for banking use a custom-designed software application that is installed on the consumer’s mobile device and is unique to each device.

Just as the case for mobile banking, mobile payment is a fast-growing market. According to a Federal Reserve representative, mobile payments include “purchases, bill payments, charitable donations, payments to another person, or any other payments made using a mobile device.” Consumers may make mobile payments by using a web browser on the mobile device, by sending a text message, or by downloading an app on the mobile device. In general, the wireless network provider’s system processes the transaction, where the bank or another service provider applies charges to a phone bill, credit card, or withdraws the amount from the consumer’s bank account.

47. Yao Huili et al., A Study of User Adoption Factors of Mobile Banking Services Based on the Trust and Distrust Perspective, 6 INT’L BUS. & MGMT. 9, 9 (2013).
48. Kim, supra note 27, at 110.
50. Id.
51. Lumsden, supra note 7, at 145–46.
52. MOBILE BANKING: REWARDS AND RISKS, FDIC (Winter 2011), http://www.fdic.gov/regulations/examinations/insights/swin11/mobile.html (“To appeal to a greater number of customers, some financial institutions are finding it advantageous to offer mobile banking through multiple delivery channels.”).
54. See Mobile Payments, supra note 32, at 1.
Non-financial institutions, such as PayPal or BilltoMobile, may also offer mobile payments, and banks are moving to offer customers similar mobile payments services as well. According to Marianne Crowe, in this current payment models, parties share responsibility and collaborate with technology. When one uses a mobile handset to initiate a payment, it is funded by credit, debit, or prepaid access payments. Consequently, in these new models, the financial institutions, which issue payments through traditional channels for clearing and settlement, still retain the responsibility for the payment providers.

2. Participants in the Mobile Banking and Mobile Payment Industries

Typically, mobile financial services involve “a combination of financial institutions, mobile network operators, agent network managers and payment service providers, linked into a seamless service delivery channel.” Distinguishable from the traditional banking services that involve direct contact with customers, mobile financial delivery involves third-party services providers, such as telecommunication companies, software developers, and third-party vendors and platforms, as well as contractual obligations that affect the relationship dynamics between bank and customers. Furthermore, mobile payments often involve entities such as “hardware manufacturers, operating system developers, application developers, data brokers, coupon and loyalty program administrators, payment card networks, advertisement companies, retailers, and other merchants.” Thus, successfully providing mobile banking services will depend on this chain of companies that provide specialized services.

57. Fonte, supra note 31, at 3; John Aquino, More Community Banks Offering Mobile Payments: ICBA, BANK INNOVATION (Nov. 22, 2013), http://www.monitessimobilefi.com/more-community-banks-offering-mobile-payments-icba/ (“The number of community banks that offer mobile payments is increasing; according to a recent survey from the Independent Community Bankers of America (ICBA)…[T]he 2013 ICBA Community Bank Payments Survey confirms what we are seeing anecdotally in the marketplace—that community banks are increasingly offering mobile banking services to meet the evolving needs of their customers and enhance overall customer service.’ ”). See also Yao Huili, supra note 47, at 9 (“[A] large numbers [sic] of banks have paid attention to promote the Mobile banking service because this could provide real-time services ubiquitously and reduce the operating costs.”).


59. Id. at 3.

60. Id.

61. See Mark Flaming & Aiaze Mitha, Why do Partnerships in Mobile Financial Services Struggle?, CGAP (Oct. 31, 2013), http://www.cgap.org/blog/why-do-partnerships-mobile-financial-services-struggle (noting that the success of commercial partnerships is crucial to increase access to affordable, mass-market financial services through mobile services).

62. Jeffrey L. Hare, Regulatory Considerations for Mobile Banking, 13 NO. 2 ELEC. BANKING L. & COM. REP. 1, 1 (2008); see also Frederick M. Joyce et al., Mobile Banking, VENABLE L.L.P., 4 (Nov. 2008), http://www.venable.com/files/Publication/3188a1e1-fbaa-45fe-a7be-008f3d384c3c/Presentation/Publication/Attachment/52cc19ac-dd18-4cf6-b471-0663ce93a47d/2010.pdf (“[T]here distinct communications networks [play] a part in originating and terminating mobile finance transactions: the traditional wireline network, the Internet… and wireless cell phone… “).

services to banks and other non-financial institutions.  

Banks have a leading position in the service because of their existing customer base.  

A variety of vendors promote mobile banking products in the market, leading to many arrangements between banks and third parties.  

Vendor management programs are primarily used to provide the required software application and related technologies that allow the customers of the bank to undertake on their smartphone activities related to bank accounts.  

For instance, some of the many mobile banking vendors in the market are Clairmail (providing mobile banking and payments solutions for banking, payment, and card services markets), Infosys (providing platforms and access modes that integrates with host systems to bring cross-channel synergies), and mFoundry (providing a platform for mobile banking and mobile payments services).  

3. Unique Risks for Consumers in the Mobile Financial Services Industry  

In terms of regulation, while regulators approach mobile banking activities in a similar manner to traditional banking, the unique risks presented in mobile financial services raised additional concerns. In fact, a recent study has found that the reason many consumers do not adopt mobile banking technology is because of security concerns.  

The goal of the regulation in this emerging mobile environment for financial services is to guarantee a safe and sound market for consumers. Since 2002, the FTC has been examining the advantages and challenges to consumers associated with the use of mobile commerce and has been working to ensure the protection of consumers as new technologies emerge. According to the Federal Report, the risks presented in mobile financial services are the main deterrent to consumer’s adoption of the new technology, and the two main factors limiting consumer adoption of mobile financial services are distrust of the security technology, together with a belief that  

64.  FIN. CONDUCT AUTH., supra note 13 (“For firms to successfully provide mobile banking services to their customers, they will be dependent on IT systems, technical expertise and detailed knowledge of the payments system.”).  
65.  PwC’s Banking Views, supra note 3.  
67.  McTaggart & Freese, supra note 20, at 4; Hare, supra note 62, at 1.  
mobile services do not offer real benefits over the existing brick and mortar services already offered. The Federal Report acknowledges the unique risks associated with the use of mobile banking, and some of the specific risks will be detailed below.

a. Third Party Risks

Banks benefit from outsourcing part of its services to third parties. Banks thereby increase the ability of improving financial performance by taking advantage of the specialized and detailed knowledge of these third parties. In addition, banks may lower the costs of providing the service by using specialized technology companies. However, security risks related to sharing sensitive data information and the larger number of companies involved in a customer’s transaction increase the likelihood of an error to occur.

First, when banks utilize the service of third parties they allow multiple persons to have access to customer information. Within mobile payments, the sharing of consumers’ financial information raises significant privacy concerns, especially considering that insiders commit most identity theft by virtue of their position as they have access to a consumer’s confidential information, such as financial statements. If the mobile phone is lost or stolen, or there is a reasonable mistake by consumers, or even if security or data are compromised, the question becomes who is to blame. The telecoms may worry that they would be called upon to shoulder some of the responsibility, along with the person or company that designed or fabricated the secure chip on the new platform.

The second challenge is ensuring that banks associated with using third party vendors have adequate and risk-sensitive systems in place. The ability of banks to identify and manage potential financial harm to customers concerns

73. See Bd. of Governors of the Fed. Res. Sys. supra note 49, at 1 (“Consumers need to be provided with reliable and accurate information on the level of security associated with the various means of accessing mobile banking.”).
74. Id. at 4.
75. Hare, supra note 64, at 4.
76. Id. at 1.
77. Id.; see also Gupta, supra note 24, at 3 ("[M]ost banks believe that the mobile channel will help them reduce transactions costs as well as increase customer engagement and retention.").
78. PwC’s Banking Views, supra note 3.
79. Lumsden, supra note 7, at 157. ("[C]onsumers are willingly sharing their personal records with multiple parties . . . . This information can be retained and stored by service providers, as well as by various unregulated third parties.").
80. Id. (noting that “70% of all identity theft is committed by insiders, including ‘bank employees, phone operators, and government agencies.’").
regulators. The FTC statement, for instance, recommended that mobile app developers coordinate with third parties, such as companies that provide services for apps. Many banks work with third party companies to create services and financial tools. Regulators expect banks to ensure that arrangements with third parties address risks and comply with their rules when dealing with consumers. The goal of the regulators should be to guarantee that the relationship of banks and third party providers does not create more risks than the bank is able to identify and control.

Third, another challenge involves the involvement of wireless carriers. Wireless carriers provide the network that consumers use to access the Internet from their mobile devices. Wireless banking services allow the use of smartphones, but wireless carriers services have unique risks associated with this delivery channel. Some of the steps of a mobile payment that are facilitated by a wireless carrier occurs, for instance, when a subscriber prepay his account, thereby creating a credit towards the next billing cycle by using a debit or credit card. This same subscriber may subsequently make purchases via text or available applications using his mobile phone provided by the wireless carrier or a third party. Finally, the wireless carrier deducts the value of such purchases from the prepaid account; and . . . the wireless carrier transfers the funds to the merchant in the amount of the purchase price (‘Prepaid Carrier Payments’).

When an unauthorized Prepaid Carrier Payment charge occurs, a wireless carrier not subject to Regulation E (discussed in Section III) will likely not be liable to consumers, meaning that the regulation will not obligate the wireless carrier to resolve the dispute. Wireless providers have acknowledged the

---

84. Comments, supra note 72.
86. See Third-Party Relationships: Risk Management Guidance, OFFICE OF THE COMPTROLLER OF THE CURRENCY (2013) (“[T]he contract [between the bank and third party] should ensure that the third party implements and maintains appropriate security measures to comply with privacy regulations and regulatory guidelines.”). See also FCA Identifies Screen Size Risks Associated with Mobile Banking and Payments, supra note 82 (noting multiple issues that banks face in regards to mobile payments).
87. Vendor Risk Management, supra note 83.
89. Id.
90. Tom Wills, Mobile Banking: Emerging Threats, Vulnerabilities, and Counter-Measures, BANK INFO SECURITY, http://www.bankinfosecurity.com/webinars/mobile-banking-emerging-threats-vulnerabilities-counter-measures-w-285 (“Unsecured wireless network is a toll-free highway for fraudsters to gain access to mobile devices, either to seize control of or gain access to account information.”).
91. McTaggart & Freese, supra note 88, at 1.
92. Id.
93. Id.
94. Id. at 3 (noting that if the wireless carriers is subject to Regulation E “[they] would be responsible for resolving any claims by the subscriber that the Prepaid Carrier Payment was unauthorized and for providing the required disclosures.”).
risks involved and attempted to find ways to ensure the privacy of their users; however, despite their efforts, cybercriminals continue to access consumers’ private information.95

b. Malware Threats

Smartphones are at a greater risk of becoming infected with viruses than computers.96 Malware is a threat that can “gain[] access to a device for the purpose of stealing data, damaging the device, or annoying the user, etc.”97 The attacker deceives the smartphone user into downloading and installing the application, thereby gaining unauthorized access to its device.98 Research has found that most malware is used to collect user information, followed by “premium-rate SMS messages” sent to smartphone users.99 Moreover, the research also identified malware created to intercept SMS messages between banks and consumers and to capture the customer’s bank information.100 The stolen information is sold on the black market.101 Financial information remains the most valuable data for cybercriminals; “a single package with a victim’s credit card number, social security number, expiration date, and mother’s maiden name [may be worth] $4 to $5 per victim.”102

The threat of malware in mobile devices is still small as compared to malware in computers.103 In the first quarter of 2012, for instance, there were nearly 7,000 types of Android malware threats, when approximately 83 million threats targeted PCs.104 However, experts expect the malware problem to worsen in coming years.105

c. Fraud and Security Risks

Security is important in every mobile app.106 While many may believe
mobile banking apps are, or at least should be, more secure than other apps, a new study detected that serious security vulnerabilities could potentially compromise sensitive user data in 90% of mobile banking apps from the top banks.107 Stories about security breaches scares mobile banking users, and many consumers lose interest about mobile technologies involving their financial data in light of such risks.108

According to the FCA, fraud in mobile banking “could result in consumers being unable to access their money or make payments, resulting in financial loss, inconvenience, and stress.”109 As financial transactions through mobile phones become more common, these phones become the targets of electronic crime.110 In 2012, identity fraud affected 5.26% of adults in the United States, while a study found that fraud among mobile users were found to be 33% higher than fraud involving the general public.111

One of the main risks in mobile financial services is the risk of leakage of sensitive user information, such as personal data that is stored or is transmitted through a mobile device.112 This data includes PINs, passwords, personal information, and account numbers.113 In August 2013, a scam targeted JP Morgan Chase mobile bankers, connecting them to a fraudulent login page that looked similar to the authentic bank’s mobile banking site.114 The cybercriminals lead consumers to fake login pages, so they could steal personal data, or download malware to the mobile device.115 Another common type of fraud involves cyber criminals sending SMS requesting that the consumer responds to the message with personal information.116

109. FIN. CONDUCT AUTH., supra note 13, at 6.
110. Lumsden, supra note 7, at 154 (“In August 2011, hackers successfully attacked the San Francisco Bay Area’s Bay Area Rapid Transit (‘BART’) system on three separate occasions. In one instance, confidential personal information of Bay Area commuters was leaked online: ‘The anti-BART hackers, angered at the agency’s tactics to curtail previous protests, posted the names, street addresses, email addresses, phone numbers and passwords of at least 2,400 of the website’s 55,000 email subscribers False’ In a separate attack, the group posted the private information of 102 BART Police Officers, including their home addresses, personal emails, and account passwords.”).
112. Data Leakage Prevention: A Newsletter for IT Professionals, JOINT UNIVS. COMPUTER CENTRE LTD. (JUCC), www.itst.jucc.edu.hk/newsletter/IT_05/IT_5_DLP.pdf.
113. Lumsden, supra note 7, at 153. See also Scott Thurm & Yukari Iwatanı Kane, Your Apps are Watching You, WALL ST. J. (Dec. 17, 2010), http://online.wsj.com/news/articles/SB10001424052748704694004576020083703574602 (“Few devices know more personal details about people than the smartphones in their pockets: phone numbers, current location, often the owner’s real name—even a unique ID number that can never be changed or turned off.”).
115. Id.
116. Id. (noting that another type of fraud involve cyber criminals sending spam emails pretending to be the bank and asking consumers to verify the information or visit a website).
Therefore, safety concerns pose significant challenges and risks to the financial institutions, and each delivery channel poses unique risks for both the financial institution and customers. Furthermore, from a security perspective, although Internet and mobile banking services have similar operating systems, the latter is still perceived by consumers as being more risky. One of the reasons for such perception is that while one may delete tracking files on a computer, mobile phone users have a limited ability to limit tracking. The use of wireless technology in providing financial services increases the risk that consumer information will be stolen, and such risks open the door to monetary and reputational harms for consumer and banks.

C. Fiduciary Duties and Banks

Before delving into a more flexible fiduciary duty approach, this Note describes how courts currently impose fiduciary duties on banks, and how the law has evolved in the past decades. A fiduciary duty is the highest standard of duty implied by law. There are classic relationships that impose fiduciary duties, such as the trustee-beneficiary relationship, or the corporate officer-shareholder relationship. Depending on the particular set of facts, courts may impose fiduciaries duties outside the classic relationships. The Second Restatement of Torts, for instance, defines a fiduciary relationship as “between two persons when one of them is under a duty to act for or to give advice for the benefit of another upon matters within the scope of the relation.” A fiduciary relationship arises when a person has power over someone while, simultaneously, a duty to use such power in the best interests of the latter. Fiduciary duties are not some sort of moral duty, but rather they are derived and enforced as a contractual term. Courts may fill in the gaps in fiduciary relationships just as they fill gaps in other types of contracts.

In fact, “[o]ptimal fiduciary rules approximate the bargain that the parties would have reached if the costs of contracting were zero.” The purpose of fiduciary duties is to provide parties an alternative to “direct monitoring,” meaning that the fiduciary obligation should reflect that which the parties

117. FDIC, supra note 52.
118. Kim, supra note 27, at 54.
119. Lumsden, supra note 7, at 155.
120. Joyce et al., supra note 62, at 6.
123. Id.
124. Restatement (Second) of Torts § 874 (1979).
126. Easterbrook & Fischel, supra note 22, at 427.
127. Id. at 431 (noting that the fact that courts “treat fiduciary duties as presumptive contractual terms, promoting the parties’ welfare in the absence of express contracts, is all but inevitable.”).
would have bargained without incurring the costs, time, and effort associated with the bargaining process. Fiduciary duties serve a useful function by reducing the high economic costs of monitoring and detailed bargaining associated with the relationship.

1. The Fiduciary Duty Obligation in a Bank-depositor Relationship

Fiduciary duties have been found to impose stringent, albeit necessary, responsibilities upon banks. By virtue of finding a fiduciary relationship, it is relevant to note that a bank is prohibited from competing with a customer’s business, taking advantage of a customer’s business opportunity, or misleading the customer. Fiduciary duties also embrace positive obligations, such as providing broad disclosure to the customer, explaining the nature of the transaction and its results, and maintaining confidentiality. In general, if not under specific circumstances, it is often unclear when a bank may owe fiduciary duties to a customer. The existence of a duty and the scope of that duty are questions of law for a court to decide. As noted below, courts carefully define fiduciary duties in accordance with the unique relationship and circumstances of the case.

When looking at court decisions, courts differ in regards to the application of fiduciary duties to the bank-borrower and bank-depositor relationship. Many courts have held that banks that only have a traditional creditor-depositor relationship with a debtor generally do not owe fiduciary duties to their customers. As we will see below, other state courts, however, have acknowledged that in certain circumstances fiduciary duties may arise. In this note, the “flexible” approach to fiduciary duties as applied to banks offering mobile banking services will encompass both relationships because it is the mobile technology employed by the bank that is at stake.

133. Id.
134. Unless their relationship is one of the classic relationships that impose fiduciary duties, such as the attorney/client, executor/heir, guardian/ward, agent/principal, trustee/beneficiary, or corporate officer/shareholder.
136. Id.
137. Grant E. Buerstetta, Creating A Flexible Fiduciary Duty to Rule for Banks Entering into Proprietary Derivatives Contracts, 15 ANN. REV. BANKING L. 395, 403 (1996) (explaining the applicable rule when, for instance, solely acting as a debtor to an individual holding a checking account).
a. Cases Supporting Fiduciary Duties for Banks

Several courts have confirmed the applicability of fiduciary duties in bank-client relationships. In *Klein v. First Edina National Bank*, the Minnesota Supreme Court held that a bank-borrower relationship may give rise to fiduciary responsibility requiring the bank to disclose certain material facts. In *Klein*, the plaintiff sued when her bank foreclosed on the stock that she pledged as collateral for a loan the bank granted to her employer. The plaintiff was unaware that her employer already owed the bank and that the bank relied on the plaintiff’s stock as security for both loans. After the bank foreclosed on the stock the plaintiff pledged as collateral for the loan granted earlier to the employer, the plaintiff then alleged fraud based on the bank’s failure to inform her of all the details of the transaction. According to the court, in general a bank has no special duty to counsel its customers and inform them of every material fact relating to the transaction. However, the court noted that a special duty may arise where the bank knows, or has reason to know, that the customer places trust and relies on the bank to counsel and inform him.

In *Deist v. Wachholz*, the Montana Supreme Court recognized an exception to the principle that the relationship between a bank and its customer is that of debtor and creditor and does not give rise to fiduciary responsibilities. In *Deist*, the bank acted as the plaintiff’s financial advisor causing the plaintiff to rely upon it in a complicated credit transaction. The court stated that

> [a]s a general rule, the relationship between a bank and a depositor or customer does not ordinarily impose a fiduciary duty of disclosure upon the bank . . . . However, special circumstances may dictate otherwise . . . . [M]odern banking practices involve a highly complicated structure of credit . . . which often thrust[s] a bank into the role of an advisor, thereby creating a relationship of trust and confidence which may result in a fiduciary duty upon the bank . . . .

Another case where the court found fiduciary duties to apply to the bank-customer relationship was *Garrett v. BankWest, Inc.*, where the plaintiff asserted that BankWest breached its fiduciary duties when the bank improved its economic position without consideration of the effect its actions might have

---

140. *Id.* at 621.
141. *Id.*
142. *Id.* at 622.
143. *Id.* at 623.
144. *Id.* (noting that a duty may arise if “special circumstances exist, such as where the bank knows or has reason to know that the customer is placing his trust and confidence in the bank and is relying on the bank so to counsel and inform him.”).
146. *Id.* at 194.
147. *Id.* at 193 (quoting *Tokarz v. Frontier Fed. Sav. & Loan Ass’n*, 656 P.2d 1089, 1092 (1983)).
The Supreme Court of South Dakota held that a relationship between bank and its customer may become a fiduciary relationship if the following factors exist: (a) borrower repose confidence and trust in bank, (b) the bank exercises dominion, control, or influence over the borrower’s affairs, and (c) borrower is in a position of inequality, dependence, and weakness or lacks knowledge.

Finally, in *Yuster v. Keefe*, the Indiana Appellate Court held that while there is no uniform rule determining the existence of a fiduciary relationship, there must be not only confidence of the one in the other, “but there must exist a certain inequality, dependence, weakness of age, of mental strength, business intelligence, knowledge of the facts involved, or other conditions, giving to one advantage over the other.”

Thus, the cases show that courts do not generally impose *per se* fiduciary duties, but the circumstances of each dispute involving banks and consumers may give rise to a fiduciary relationship. A case by case analysis is in fact the wiser approach, since a sweeping prohibition would be “simply too rigid and narrow to account for the economic and commercial realities of how banks and their customers interact in the conduct of ordinary business transactions.”

In general, it can be said that important considerations to courts include whether (i) the counterparty reposed special trust or confidence in the bank; (ii) the counterparty sought advice from the bank; (iii) the counterparty relied on the information received; (iv) the bank knew that the counterparty relied upon information so furnished; and (v) the bank exercised superiority, influence, dominion, or control over the counterparty. These factors will guide courts in evaluating when, if so, fiduciary duties should be enforced in the context of mobile banking relationships.

b. Cases Holding No Fiduciary Duties for Banks

Courts generally refuse to find a fiduciary relationship between banks and depositors when the factors mentioned above are either weak or not found. Yet it is important to note what facts cause courts to reject finding fiduciary duties to a bank-customer relationship.

In *Kurth v. Van Horn*, the Supreme Court of Iowa held that a fiduciary relationship does not arise solely from a bank-depositor relationship. The plaintiff, the trustee of Gerdes’ estate who cosigned a note in connection with a bank loan to Mr. Hall, sued the bank alleging fraud and breach of fiduciary

---

149. Id. at 838.
151. Hunt, supra note 130, at 730 (“[C]ourts must examine the particular relationship in question rather than the normal relation of the parties.”).
152. Id. at 767.
The plaintiff claimed that a fiduciary relationship existed between the bank and Gerdes because Gerdes was eighty years old, was under pressure by Hall to secure the loan, made several visits with Hall to the bank, and was not advised of Hall’s financial problems of which the bank had knowledge.156

The court rejected the plaintiff’s assertion that the bank should have refused to conclude the loan.157 Accordingly, the court noted that this protectionism is beyond the exercise of what a banker should be responsible for; “the bank had no affirmative duty to prevent Gerdes from doing what the evidence clearly shows he wanted to do.”158

A recent Illinois decision also illustrates the absence of a fiduciary relationship. In *Geimer v. Bank of Am., N.A.*, the plaintiff, an account holder, claimed that the bank breached its fiduciary duty because the bank failed to prevent unauthorized fund transfers from her personal accounts.159 The plaintiff notified her bank about these unauthorized transactions, but the bank never investigated them.160 Instead, the bank simply told plaintiff “that the ‘money was gone and could not be recovered’.”161 The court first noted that to establish the existence of a fiduciary relationship, “a party must show that she ‘placed trust and confidence’ in the dominant party, and that the latter ‘gained influence and superiority’ over her.”162 In analyzing those factors, the Court held that the plaintiff did not demonstrate that she placed significant trust in the bank, or that the bank exerted dominance over her.163 Other courts have adopted a similar approach that generally a bank will not owe fiduciary duties to its customers.164

III. ANALYSIS

Mobile financial services are two-fold: while they offer many benefits to consumers, the risks presented by the fast pace of innovation in the sector may leave consumers subject to more risks than regulators can efficiently manage.165 Changes in technology are slowly causing the traditional bank-customer relationship to evolve, and the modern, “high-tech” relationship

---

155. *Id.* at 693.
156. *Id.* at 696.
157. *Id.* at 697.
158. *Id.*
160. *Id.* at 930.
161. *Id.* [internal citations omitted].
162. *Id.* at 932 (“In making these determinations, courts look to factors such as ‘kinship, age disparity, health, mental condition, education, business experience, and the extent of [the party’s] reliance’ on the dominant party.”).
163. *Id.*
164. Branch Banking & Trust Co. v. Thompson, 418 S.E.2d 694 (N.C. 1992) (“[A]n ordinary lender-borrower relationship generally does not give rise to such a “special confidence . . . .”); United Virginia Bank v. Air-Lift Assocs., 339 S.E.2d 90 (N.C. 1986) (holding that there are no special duties owed by the bank in addition to the duties in the parties’ contractual agreement and defined by the U.C.C.); Blon v. Bank One, Akron, N.A., 519 N.E.2d 363 (Ohio 1988) (holding that the bank had no duty to disclose a lower interest rate because bank and borrowers have no special relationship of trust and confidence).
demands developments in the law. This Note argues that courts have an opportunity to expand the obligations of banks by finding flexible fiduciary duties in connection to their mobile banking users. As noted, “mobile payments represent the forced marriage of two of the most regulated industries we have: telecommunications and financial services.” This section of the Note will approach the question of how the courts may better protect consumers. This section will approach this issue first by examining the current consumer protection laws applicable to mobile banking, and then by delving into the case law about how fiduciary duties should apply to banks. A short review of some of the elements, which courts have historically analyzed to determine whether fiduciary duties should be imposed upon banks, sheds light on a discussion of whether mobile banking activities may create fiduciary duties.

A. Current Consumer Protection Regulations Applicable to Mobile Financial Services: Why Fiduciary Duties Should Apply to Mobile Banking

While bank supervisors have generally agreed that mobile banking activities should be approached in the same way as traditional banking practices, no specific laws or regulations target mobile banking or mobile payments, and the unique risks related to mobile financial services may make application of existing laws to mobile banking quite challenging. Some of the most relevant laws protecting consumers, and their potential shortcomings, are briefly identified below to illustrate how current regulations may not entirely protect mobile banking consumers.

1. Electronic Fund Transfer Act/Regulation E

The Electronic Fund Transfer Act (EFTA)/Regulation E provides “a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund and remittance transfer systems.” The EFTA and Regulation E apply to electronic fund transfers that authorize a financial institution to credit or debit a consumer’s account. Regulation E also stipulates that consumers are liable only for up to $50, provided that they contact their bank within two days of discovering a loss of money.

As applied to mobile payments, particularly when the underlying

169. Jeffrey P. Talia, An Overview of the Electronic Fund Transfer Act & Regulation E & Their Application to E-Commerce, 57 CONSUMER FIN. L. Q. REP. 205, 205 (2003). See also McTaggart & Freese, supra note 20, at 4 (explaining that an electronic fund transfer occurs when a consumer makes a payment using, for example, his or her debit card).
payment is made via an electronic fund transfer, the EFTA and Regulation E establish disclosures and error resolution procedures for erroneous or unauthorized transactions.\textsuperscript{171} Yes, banking through a mobile phone presents more risks for errors in transactions, such as when the wireless service drops in the middle of operation or when a technical failure in the vendor’s platform interrupts the transaction.\textsuperscript{172}

Moreover, Regulation E defines a financial institution as 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 electronic fund transfer services.”\textsuperscript{173} Nonetheless, Regulation E is only applicable if the provider “(1) [i]ssues a debit card, (or other access device) that the consumer’s account held by a financial institution; and (2) has no agreement with the account-holding institution regarding such access.”\textsuperscript{174} Therefore, if third parties, such as wireless carriers, have an agreement with a financial institution, then they will not fall under the purview of Regulation E.\textsuperscript{175} If a wireless carrier was not subject to Regulation E, there may be implications for contracting financial institutions.

The exclusion of wireless carriers, and potentially other third parties, raises safety concerns for consumers utilizing electronic funds transfers through a mobile phone. While consumers who fund mobile payments by credit or debit card are protected against fraudulent or unauthorized transactions under the EFTA and Regulation E, consumers who use other funding mechanisms, such as prepaid cards or gift cards, do not have the same protections against unauthorized transactions.\textsuperscript{176}

2. \textit{Unfair, Deceptive, or Abusive Acts or Practices Under the FTC Act or Consumer Financial Protection Act of 2010}

The Unfair, Deceptive, or Abusive Acts or Practices Act (UDAAP) applies to any person or entity engaged in commerce and “engaging in an unfair, deceptive, or abusive act or practice with . . . any transaction with a consumer for a consumer financial product or service,” and the UDAAP is made applicable to banks pursuant to Section 8 of the Federal Deposit Insurance Act.\textsuperscript{177} The Consumer Financial Protection Bureau has reasonable

\begin{itemize}
\item 171. Drozdowski et. al, supra note 5.
\item 172. McTaggart & Freese, supra note 20, at 4 (noting also that transaction disruptions may be the result of mobile hackers interfering with the wireless network).
\item 173. 12 C.F.R. § 1005.2(i) (2014).
\item 175. See Hare, supra note 62, at 1. \textit{But see} McTaggart & Freese, supra note 20, at 3 (arguing wireless carriers may fall under the definition of Regulation E, because of the legislative intent behind the definition of “account” under Regulation E).
\item 176. Stephen Krebs & Duncan Douglass, \textit{Regulatory Devices in Electronic Banking and Payments}, 16 No. 3 ELEC. BANKING L. & COM. REP. 14, 14 (2013) (“[I]nconsistency in protections complicates the landscape for consumers who may not understand the differences between these funding sources.”).
\end{itemize}
discretion to determine whether a practice is unfair and abusive.\footnote{178}{12 U.S.C. § 5531 (2012).}

As applied to mobile financial services, determining whether an act is abusive or unfair to consumers is not an easy task. For instance, if banks require consumers to agree to terms and conditions on small screens, that will likely limit consumers’ understanding because one cannot easily read and comprehend terms and conditions on a portable, small device, even if apps are getting better in providing this service.\footnote{179}{How to Bank Safely From Your Smartphone, BULLGUARD, http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/secure-mobile-banking.aspx (last visited Apr. 20, 2015).} According to the Financial Conduct Authority in England, “companies providing mobile banking services must consider how to overcome limitations in mobile device screen sizes.”\footnote{180}{FCA Identifies Screen Size Risks Associated with Mobile Banking and Payments, OUT-LAW (Aug. 28, 2013), http://www.out-law.com/en/articles/2013/august/fca-identifies-screen-size-risks-associated-with-mobile-banking-and-payments/; Drozdowski et. al, supra note 5 (noting that “creative solutions may be required to display disclosures on a mobile device’s small screen.”.).} But whether this amounts to an action under the UDAP is for the Consumer Financial Protection Bureau to decide.\footnote{181}{Unfair and Deceptive Acts or Practices: Is it a Big Deal?, LATEST NEWS (Sept. 13, 2011), https://www.trinovus.com/2011/07/13/unfair-and-deceptive-acts-or-practices-is-it-a-big-deal/ (“One of the difficult issues with [the] UDAP is that the determination of what is or is not an unfair and deceptive act or practice is usually purely subjective; it is whatever your regulator thinks that it is and there is no reasonable method of appeal or review.”).} Similarly, it is unfair to customers if banks do not contract safeguards to protect the confidential information and security of customer.

3. **Gramm-Leach-Bliley Act**

The Gramm-Leach-Bliley Act (GLBA) protects consumers by providing that financial institutions have a continuing obligation to respect the privacy, and protect the confidentiality of, its customers’ nonpublic personal information.\footnote{182}{David L. Glass, The Gramm-Leach-Bliley Act: Overview of the Key Provisions: Presentation Before the State of New York Banking Department, 17 N.Y.L. SCH. J. HUM. RTS. 1, 27 (2000); see also Joseph A. Smith, Jr., Retail Delivery of Financial Services After the Gramm-Leach Bliley Act: How Will Public Policy Shape the “Financial Services Supermarket?” 4 N.C. BANKING INST. 39, 52 (2000) (“Gramm-Leach-Bliley contains provisions regarding privacy of customer financial information that were both path-breaking and heavily debated.”).} The GLBA also applies to non-financial institutions engaged in financial services, and it governs the relationship between the customer and the institution by imposing disclosure obligations, such as the disclosure of customers’ rights and obligations, and reminders about their privacy rights.\footnote{183}{Lumsden, supra note 7, at 171. See also Hare, supra note 62, at 1 (“Title V of the Gramm-Leach-Bliley Act defines a financial institution to include companies that provide services permissible for banks and bank holding companies”).} Moreover, if the GLBA applies and if the institutions intend to share customers’ personal information, then entities that have access to or use consumer information need first to disclose what information will be shared and request consent from customers.\footnote{184}{Lumsden, supra note 7, at 172.}

When applied to mobile banking, banks that offer mobile banking...
services are subject to the GBLA if they have access to and handle non-public customer information.\textsuperscript{185} As mentioned above, the participation of third party vendors may pose challenges to the GBLA. For instance, a challenge exists when a financial institution uses a third party vendor that also has access to customers’ information, in which case the financial institution should carefully monitor the third party use of such information.\textsuperscript{186} Thus, the unique issues of this emerging technology, and the absence of comprehensive privacy law challenge the adequacy of the current regulatory treatment of mobile financial services leaving gaps that render consumers unprotected.\textsuperscript{187}

\textbf{B. Fiduciary Duties May Be Found in Traditional Banking Relationships}

Fiduciary duties have long been an important aspect to the banking business.\textsuperscript{188} Traditionally, courts treat the relationship between a bank and its customer as a contractual one, governed by common law contract and debtor-creditor laws.\textsuperscript{189} At the same time, changes in technology that leave consumers more susceptible to frauds might call for a more progressive approach to current bank-client relationship. The objective of this section is to add an additional layer of protection to consumers, while establishing a balance between protecting consumers and not imposing excessive burden over banks beyond what should be their responsibility.

\textbf{1. The Rise, Fall and Lessons of Commercial Cotton Co. v. United California Bank}

In light of the challenges involving mobile banking, the issue becomes how courts can further protect consumers’ trust or confidence in, and dependency upon, a financial institution offering mobile financial services. In 1985, the California Court of Appeals advanced an innovative theory in \textit{Commercial Cotton Co. v. United California Bank}, a case involving a depositor suit against a bank.

In \textit{Commercial Cotton Co.}, the court held that the relationship between a bank and its depositor, like the relationship between insured and insurer, “is at least quasi-fiduciary.”\textsuperscript{190} The plaintiff was a company that maintained a checking account with the defendant bank.\textsuperscript{191} Upon discovering the loss of a

\begin{footnotesize}
\begin{enumerate}
\item Hare, supra note 62, at 1.
\item See McTaggart & Freese, supra note 20, at 3 (“A financial institution must integrate its mobile banking operations into its [GBLA] security program and should choose a Vendor whose security solutions ease this integration.”).
\item Id. at 514.
\end{enumerate}
\end{footnotesize}
number of blank checks, the company reported the loss to the bank. Years later when someone presented one of the lost checks to the bank containing a forged signature, despite its prior notice from the company, the bank honored the check. The Bank then refused to refund the plaintiff based on a one-year limitation on bringing repayment claims. Nevertheless, the court held that given the “quasi-fiduciary duty” of a bank to its depositor, depositors have a right to “reasonably expect a bank not to claim nonexistent legal defenses to avoid reimbursement when the bank negligently disburses the entrusted funds.” Moreover, the court awarded the plaintiff punitive damages based on the breach of the covenant of good faith and fair dealing, which was implied from the contract governing the relationship between the company and the bank.

The court in Commercial Cotton Co. recognized that a breach of the implied covenant of good faith and fair dealing by a bank subjected the bank to tort remedies in addition to any contractual remedies. In other words, by imposing tort liability, the court opened the door to the full range of tort remedies available by law. In order to support its holding, the court also relied on the fact that banking is a highly regulated industry that serves a vital public service. The court went on to hold that banks, just like the insurance companies, are part of very similar industries. In the context of the insurance industry, the courts in California have found that the characteristic elements of this industry are the public interest, fiduciary responsibility and the existence of adhesion contracts. Therefore, banking and insurance are greatly regulated industries that perform essential public services that affect the public welfare. Because of that, “[a] depositor in a noninterest-bearing checking account, except for state or federal regulatory oversight, is totally dependent on the banking institution to which it entrusts deposited funds and depends on the bank’s honesty and expertise to protect them.”

A year after the Commercial Cotton favorable decision to plaintiff, the same California Appellate Court found that fiduciary principles should be extended to not only situations involving bank and depositors, as held in Commercial Cotton, but also to the bank-borrower relationship. In Barrett v. Bank of America, the plaintiffs (the Barretts) instituted an action against the bank alleging breach of contract, fraud, conspiracy to defraud, intentional

192. Id.
193. Id.
194. Id.
195. Id. at 516. See also Hunt, supra note 130, at 750 (explaining that the bank’s defense on the basis of the expiration of a statute of limitations in Commercial Cotton was “spurious”).
196. Hunt, supra note 130, at 751.
197. Id.
199. See id. at 514 (“In the context of an insurance contract the Supreme Court [of California] emphasized the relationship between insurer and insured, characterized by elements of public interest, adhesion, and fiduciary responsibility created the necessary special relationship.”).
200. Id. at 516.
201. Id.
202. Id.
infliction of emotional distress, and negligence. The plaintiffs were principal shareholders in a company, and, to secure loans, they executed two personal guarantees to the bank. Less than a month later, the bank informed the plaintiffs that they were in default. The bank’s loan officer suggested that, in order to cure the default, the plaintiffs should bring in new investors by way of a merger or an acquisition of the company so that the new investor would be responsible for the loans. The plaintiffs began merger negotiations with Coded Communications (Coded), but Coded filed for bankruptcy when it could no longer make payments on plaintiffs’ loan. The bank thereafter assigned its collateral to the loan, including the plaintiffs’ note and personal guarantee, and forced plaintiffs to sell their home.

The Barretts sued the bank alleging fraud and that the bank failed to honor its promise that the personal guarantees would be released upon the merger of their company. The court held that evidence supported a constructive fraud theory in favor of plaintiffs. First, a constructive fraud generally “arises from a breach of duty where a relation of trust and confidence exists . . . [and] confidential and fiduciary relations are in law, synonymous and may be said to exist whenever trust and confidence is reposed by one person in another.” In order to support its constructive fraud theory founded upon fiduciary principles in cases involving loan customers, the Barrett court held the relationship of a bank and a depositor is at least, quasi-fiduciary, as in its holding in Commercial Cotton. Thus, the court concluded that sufficient evidence implicated a fiduciary relationship between the plaintiffs and the bank to support a constructive fraud theory.

Commercial Cotton Co. and Barrett were part of a broader shift in courts with regard to the special duties related to the bank lending and depository functions. However, courts, especially in California, have recently swung away from this previous trend of expanding fiduciary relationships to fit the bank–borrower relationships. Commercial Cotton was overruled in 1999 by the same court finding that “certain propositions of law enunciated in Commercial Cotton are no longer viable.” Despite criticisms, the court’s reasoning pertaining to the fragile position of bank customers is significant to

---

204. Id. at 1366.
205. Id. at 1365.
206. Id.
207. Id.
208. Id. at 1365–66.
209. Id. at 1366.
210. Id.
211. Id. at 1370.
212. Id. at 1369.
213. Id.
214. Id. (finding the fiduciary relationship was based in the fact that plaintiffs perceived their relationship with bank agent as a very close one, plaintiffs relied upon his financial advice and plaintiffs shared confidential financial information with the bank).
the current discussions involving the modern bank-customer relationship and the role that modern banks should play by offering mobile banking. That is because the level of dependency of consumers in relation to mobile banking apps, as well as the level of trust and confidence deposited in banks, are intensified.

2. A Trend to a Full-Blown Fiduciary Duty is Already in Place

Some argue that the UDAAP has stopped short of recognizing the general role of banks as fiduciaries, but it may have initiated the process of requiring financial institutions to act in the interests of their consumers. The UDAAP prohibits financial institutions and related service providers from “materially [interfering] with the ability of a consumer to understand a term or condition of a consumer financial product or service” or from taking advantage of consumer’s lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service; (B) inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or (C) reasonable reliance by the consumer on a covered person to act in the interests of the consumer.

The obligations imposed in the UDAAP changed the prior approach banks had towards consumers because section (A) above appears to focus on the consumer’s “ability to understand” rather than the state of mind or “the ability to understand” of the financial institution. In other words, a bank or a related party does not have to act intentionally to be found liable under this provision of the UDAAP. Section (B) forbids the financial institution from taking advantage of consumers’ lack of knowledge. This prong requires banks to take additional steps to guarantee consumers understand the terms of the services. While the CFPB has offered little guidance regarding the standard imposed in the rules, it is clear that the regulation requires more than good faith and fair dealing, and it may be said to be a step closer to protecting the interests of consumers rather than banks by consider the latter a fiduciary.

References:


222. Houlihan, supra note 220.

223. Id.

224. Id.
IV. RECOMMENDATION

To this date, no court has yet decided on a case involving the use of a technology, specifically mobile banking technology, in regards to fiduciary duties owed by banks. As smartphones become more popular, bank customers will likely bring the issue to the courts, and a traditional approach may not reflect modern bank-customer relationships and the modern risks involved to consumers. For that reason, courts should revive the arguments in Commercial Cotton Co. and Barrett in favor of imposing fiduciary duties on banks in cases involving mobile banking technology.

A. What Courts Can Do: a More Flexible Fiduciary Duties Approach Should be Applied to Mobile Banking Relationships

The use of mobile financial services enhances the traditional bank-depositor relationship; mobile consumers are not merely depositors, but they are consumers of a new service offered by banks that present unique risks. In policy terms, a more “flexible” approach to fiduciary duties prioritizing some elements rather than others may be a preferable approach to other contractual remedies already in place for the reasons discussed below. It may be called a more “flexible” fiduciary duties—fiduciaries duties are called “flexible” because, while the bank-consumer (either depositor or borrower) relationship may not satisfy every element in a traditional fiduciary duties test, the unique characteristics of mobile consumers interacting with apps provided by banks, as well as hidden third-party providers supporting the mobile services, should bring banks under a more heightened relationship with its customers. A “flexible” fiduciary approach argument is viable because fiduciary relationships are not set in stone; rather, they are “one of the most elusive concepts in Anglo-American law.” Consequently, fiduciary duties may be applied through analogies to the traditional relationships, and, as this Note argues, when its application will benefit consumers.

A traditional fiduciary duties approach usually requires showing of superiority and dominance of one of the parties. A more flexible approach to fiduciary duties would mitigate this prong in favor of recognizing the justifiable trust and confidence consumers have on banks and their services, what would allow the passive and unequal position of mobile consumers in

225. Id.
226. See infra Part IV.
227. Houlihan, supra note 220.
228. See A. Mason, THEMES AND PROSPECTS, ESSAYS IN EQUITY 246 (P. Finn ed. 1985) (noting that the fiduciary duty concept is in search of a principle); Deborah A. DeMott, Beyond Metaphor: An Analysis of Fiduciary Obligation, 1988 DUKI L. J. 879, 879 (1988).
230. Id. at 32.
relation to banks when using mobile banking technology to be enough to fulfill the “superiority and dominance” prong.

Thus, as technology advances, the adoption of fiduciary duty to be owed by banks might be a preferable approach to the types of risks consumers face in modern bank-customer relationships.

The claim of a “flexible” fiduciary relationship between mobile banking consumers and their banks hinges upon the expectations of trust and loyalty consumers have towards banks. This perspective is appropriate because of the beneficial incentives of finding a fiduciary relationship upon banks employing emerging technologies and entering arrangements outside consumers’ control.

Fiduciary duties have always been relevant to the banking industry, but, as pointed out in this Note, courts still struggle with applying the fiduciary duty test to each different set of facts that come before them. Mobile financial services have significant variances and pose new challenges to courts. Nevertheless, the underlining principle in this Note is the assertion that banks perform a “vital public services substantially affecting the public welfare.” Banks are not merely commercial lenders for the purpose of making money. They also significantly contribute to the development of an economy by facilitating business and serving as instruments of the government’s monetary strategy. Hence, the aggregate of financial services pertaining to mobile devices are a consequence of, and also part, of the essential role of the banks in the economy.

B. What Do We Need From Banks: “In Banks We Trust”

1. Trust is a Foundation of Banking

Info-Tech senior vice-president James Alexander properly stated that “[w]e have a culture where we trust our banks above anything else in terms of their security, financial stability, and viability . . . .” One type of fiduciary is

231. See Commercial Cotton Co. v. United Cal. Bank, 209 Cal. Rptr. 551, 555 (Ct. App. 1986) (“A depositor in a noninterest-bearing checking account, except for state or federal regulatory oversight, is totally dependent on the banking institution to which it entrusts deposited funds and depends on the bank’s honesty and expertise to protect them.”).

232. See supra Part III 2.B.


234. See Sanderson Abel, Role of Banks in the Economy, HERALD (Oct. 10, 2013), http://www.herald.co.zw/role-of-banks-in-the-economy/ (discussing the important role of banks in the economy, such as the ability of bank to increase the participation of the private sector in economic development by making available the loans easily on reasonable rate of interest). But see Kenneth W. Curtis, The Fiduciary Controversy: Injection of Fiduciary Principles into the Bank-Depositor and Bank-Borrower Relationships, 20 Loy. L.A. L. Rev. 795, 831 (1987) (stating that bank’s primary concern is its own financial interest, and not the financial interest of its customers).


236. Mashoka Maimona, Banks Intent on Becoming Pioneers of Mobile Payment Systems, FP STREET (May 08, 2013, 4:49 PM), http://business.financialpost.com/2013/08/05/banks-intent-on-becoming-pioneers-of-mobile-payment-systems/ (“Aside from enjoying the public’s trust, banks have their fingers on the pulse of
the “one-sided” relationship, where a “party places trust in and relies on the other because [the other party] is reasonable entitled to do so in the circumstances, or because the reliant party is in a position of vulnerability, subordination or information inequality.”

In the context of Internet banking, the fiduciary relationship is certainly one-sided: the consumer places trust in and reliance on the service offered by the bank. As mentioned above, reposed trust and confidence in a bank is the foundation of mobile banking. Recent research has indicated that trust has a striking influence on a user’s willingness to engage in online exchanges of money and personal sensitive information. Trusting a bank is not something special but it is a necessary requirement for the financial system to work. Mobile banking requires an even higher degree of trust from consumers because they involve more uncertainty and more risks due to the complex chain of companies involved in the service, which consumers are not aware.

First, even if consumers do not physically visit their “brick and mortar” banks, they perceive mobile banking as an extension of their conventional bank and services. The other way around is also true: consumers perceive and expect the same level of protection that they have in conventional banking to the applied to mobile banking. If fiduciary duties were to apply to a bank-customer relationship, they should also apply to a bank-mobile customer relationship. Second, users of mobile banking are in a passive position, meaning that their only recourse is to trust the mobile banking service as it is offered to them, or “as is.” Mobile users rely on the assumption that banks and any third party involved in the mobile services, and which contract directly with the bank, act responsibly to minimize consumer’s risks. For that reason, trust is a key factor for mobile banking users. Accordingly, two major concerns raised by consumers are their lack of trust in mobile banking.

240. See Alvin C. Harrell, supra note 189, at 643 (“Banks exist and operate almost solely by using public funds and are invested with enormous public trust.”).
241. Id.
243. Drozdowski et. al, supra note 5 (“[R]egulatory expectations for managing mobile payments are generally consistent with those associated with other financial services delivered through more traditional channels.”).
244. See Huili, supra note 47, at 10 (discussing the role of trust in mobile banking relationships and how the lack of understanding of the transaction program weakens consumers’ ability of controlling transactions).
technology and the security of mobile payments.\textsuperscript{247} A recent study on understanding the dynamics about initial trust and usage of mobile banking suggests, “[a] good reputation provides assurance of a firm’s ability, integrity, and goodwill, thus helping to increase trust even when consumers do not have first-hand knowledge of the service company.”\textsuperscript{248} Banks, therefore, take advantage of their position of trust in society, and consumers perceive dealing with their banks as a “safer” option than other companies (for instance, PayPal and Google Wallet in the case of mobile payments). Thus, consumers should invoke a fiduciary relationship to protect the trusting aspects of this relationship.

2. Trust and Reliance on Banks Are Reasonable and Justifiable

The next question becomes whether such trust in banks is reasonable. Banking traditions and practices cultivate and advertise the fact that society should trust banks.\textsuperscript{249} As the court in \textit{Commercial Cotton Co.} properly notes, “[a] depositor in a noninterest-bearing checking account . . . is totally dependent on the banking institution to which it entrusts deposited funds and depends on the bank’s honesty and expertise to protect them.”\textsuperscript{250} Banks have control over their mobile banking and payment systems\textsuperscript{251} (or, theoretically, control over any third party involved in the service), and reliance by consumers is justified because banks are the entity that can take proper measures to control and protect against related risks. In the particular world of Internet and mobile banking, when consumers of mobile financial services download an application or when they login into the bank page on their smart phones and make a deposit or effectuate a payment, they rely on the bank and trust that the accounts are carried through safely.\textsuperscript{252} Additionally, mobile consumers are in an unequal position in relation to their bank.\textsuperscript{253} A bulletin issued by the CFPB in April 2012 noted that financial institutions might be held accountable by the CFPB for any faults of vendors they work with.\textsuperscript{254} As CFPB Director Richard

\begin{itemize}
  \item \textsuperscript{248} Kim et al., supra note 246.
  \item \textsuperscript{249} Djowharzadeh v. City Nat. Bank & Trust Co. of Norman, 646 P.2d 616, 620 (1982) (“[T]he words ‘trust,’ ‘security’ and ‘guaranty’ are part of the name of many banks . . . .”).
  \item \textsuperscript{252} Tom, \textit{Demand for Transparency is Driving New Banking Services}, MRI BLOG (Feb. 6, 2014, 6:49 PM), https://www.marketratesinsight.com/Blog/post/2014/02/06/Demand-for-Transparency-is-Driving-New-Banking-Services.aspx (arguing that changes in banks have been directed because consumers “expect technology to deliver transparency, and they are starting to expect the same kind of transparency and frictionless transactions from banks and credit unions.”).
  \item \textsuperscript{253} Mobile Banking: ‘Banks do Their Best, but Consumers Should Protect Themselves’, \textsc{Telephone} (Jan. 14, 2011, 1:02 PM), http://www.telegraph.co.uk/finance/personalfinance/consumertips/banking/8259411/Mobile-banking-Banks-do-their-best-but-consumers-should-protect-themselves.html (noting that there are precautions consumer may take, such as double check whether apps are legitimate, avoid storing passwords on the phones and set automatic text alerts to flag unusual transactions).
  \item \textsuperscript{254} CFPB to Hold Financial Institutions and their Service Providers Accountable, CONSUMER FIN.
Cordray explained, “consumers are at a real disadvantage because they do not get to choose the service providers they deal with—the financial institution does.” In fact, financial regulators also expect banks to provide safety to mobile consumers and reduce risks related to third parties. It is important to note that a breach of fiduciary duty by a bank does not need to be an intentionally-inflicted injury, but rather “fiduciary dut[ies] may be breached inadvertently or through a failure to exercise care, whether or not that failure can be characterized as negligent.” If we find that a failure to adequately supervise is a breach of fiduciary duties to consumers, we are imposing a greater burden on banks, but such burden means greater protection to consumers. Regulators should account for this trade-off and rule in favor of consumer protection.

Furthermore, banks profit from mobile banking and from gaining the confidence of mobile banking users. For instance, Bank of America advertises that its mobile banking service “incorporates the convenience you want with industry-leading safety and security features that provide peace of mind.” Consequently, trust and reliance are “integral and non-excludable parts of modern banking,” and finding fiduciary duties are adequate to reflect and protect this trusting relationship.

3. Banks Know that “In Banks We Trust”

If trust is an essential part of the relationship between customers and banks, and such trust is reasonable, the next question is whether we can say that banks know or have reason to know that consumers trust and rely in their services. The answer is a definitive yes. Despite the current loss of confidence, regulators and banks know that consumers rely, respectively, on their oversight of the regulated industry and their judgment. However, banks seek profit. The traditional situation where fiduciary duties arise involves


255. Id.


257. Deborah A. DeMott, Breach of Fiduciary Duty: On Justifiable Expectations of Loyalty and Their Consequences, 48 ARIZ. L. REV. 925 (2006), available at http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2290&context=faculty_scholarship (“Many actors who breach fiduciary duties to which they are subject to do so without intending to cause harm or without knowing that harm is substantially certain to result.”).

258. Tim Matthews, Don’t Be Afraid of Mobile Banking Apps, BANK, SYS. & TECH. (Sep. 5, 2012), http://www.banktech.com/channels/dont-be-afraid-of-mobile-banking-apps/240006734 (“As more users take advantage of mobile banking, financial institutions will be able to improve customer ’stickiness,’ cut costs with automation and attract the unbanked into their electronic fold.”).


261. Rebuilding Customer Trust in Retail Banking, IBM (Sept. 2012), http://www-935.ibm.com/services/multimedia/IBM1049_Trust_White_Paper_05.pdf (noting that banks have dissipated the trust that was acquired over centuries, but that the trust is still an important part of the relationship between bank and consumer).
bankers providing customers advice on their financial affairs. When a mobile consumer uses a smartphone, the consumer is not directly asking for financial advice, but it is asking for a reliable and safe service. The bank-customer relationship is, of course, different than when a financial advisor provides advice directly, but the trust embedded in the relationship, the aspiring loyalty, and the general goal of regulators and courts of protecting consumers in a new emerging technology support a flexible fiduciary duties approach in regards to banks.

Other characteristics of the bank-mobile consumer relationship show that banks know that consumers are relying on them. The bank-mobile consumer contract imposes a special relationship because mobile financial service contracts are adhesive, and they involve the kind of technology that is unknown to consumers. Mobile consumers are in an unequal and passive position, which may amount to the superiority or control requirement mentioned in the case law. As noted above, mobile financial services involve unique risks of undisclosed third party relationships, malware threats, and identity theft. Since banks have the ability to control and monitor third parties and are in a better position to prevent those unique risks, banks know and should know that consumers rely on their services to ensure safe mobile financial services. At the same time, banks face competition with other banks, what requires them to modernize and respond to consumers’ demands—what may lead to decrease protections in order to increase profits.

In a market that does not have a specific or clear regulatory framework addressing the unique risks of this market, a potential race-to-the-bottom by mobile financial services providers will put consumers at great risk. Consumers usually trust the bank’s branch and human services, and once banks offer mobile financial services to consumers, it is reasonable to expect

---

262. Id.
263. See Tom, supra note 252 (arguing that changes in banks have been directed because consumers “expect technology to deliver transparency, and they are starting to expect the same kind of transparency and frictionless transactions from banks and credit unions.”).
264. Richard P. Sybert, Adhesion Theory in California: A Suggested Redefinition and Its Application to Banking, 11 Loy. L.A. L. Rev. 297, 323 (1977) (discussing the consequences from the fact that the formalized relationships that banks offer to customers “appear to have all the characteristics of contracts of adhesion”);
268. See Mary Wisniewski, Four Ways Banks Can Profit by Modernizing Mobile Commerce, Am. Banker (Mar. 17, 2014, 5:25 PM), http://www.americanbanker.com/issues/179_52/four-ways-banks-can-profit-by-modernizing-mobile-commerce-1066304-l.html (noting that banks have been pressed for profits and growth and are motivated to try services that could bring new revenue streams related to mobile banking, “a channel they are under constant pressure to update.”).
269. See Brandon Workman, The Mobile Banking Horse Race Has Only Just Begun, Here’s How It’s Shaping Up, Bus. Insider, (Nov. 24, 2013, 2:33 PM), http://www.businessinsider.com/the-mobile-banking-markets-horse-race-2013-10 (noting the existent mobile race and how banks are competing to differentiate themselves in order to gain market share and enlarge their customer base).
banks to know consumers will also rely on their professional ability to provide these services.\textsuperscript{270} Additionally, gross disparity exists in bargaining power.\textsuperscript{271} Mobile consumers do not have a chance to discuss or change contract terms before accepting them: they either accept the terms of the mobile financial services agreement, or they are not able to download and use the application.\textsuperscript{272} Competition in the industry might not solve the problem where many adhesion contracts offer similar services and risk that end up burdening consumers and relieving banks from liability. The ability of the bank to exploit a disparity in bargaining power alone is not a requirement for imposing fiduciary duties,\textsuperscript{273} but it is a factor that courts should consider when analyzing the kind of reliance consumers have on banks. I call this a “blind reliance” consumers have on banks. The fact that there is competition in the mobile financial services market\textsuperscript{274} should not be a cause to dismiss the problems of a “blind reliance” on banks. In fact, freedom of choice for consumers does not exist if the mobile banking industry shields itself from liability and offers only the minimum necessary to maintain good public relations.\textsuperscript{275} Because of the underlining public interest in the banking industry, the disparity of bargaining power argument is relevant even if there is competition among banks offering mobile banking services.

4. \textit{Conflicts of Interest Between Banks and Mobile Banking Consumers}

Once courts determine that fiduciary duties apply to banks, banks will have an incentive to act when providing mobile financial services, or a conflict of interest may arise.\textsuperscript{276} That is because, in the case of mobile financial services, the bank may initially have incentives to take actions contrary to the interest of mobile banking users, such as reduce monitoring and supervising of third parties in order to reduce costs. This is contrary to the bank’s role as a fiduciary.\textsuperscript{277} While concerns about reputation may lessen such risks, the fiduciary duties approach suggested in this Note will provide banks with full incentives to protect consumers’ interests.

One may argue that it would be unfair to place a bank in a fiduciary position. One argument is that banks “engage in commercial activity for the
purpose of making money” and the bank’s primary concern should be its own financial interest rather that of its customer. Another argument is that a bank cannot further and protect its own interest, e.g. make money, while under a duty to act for the benefit of its mobile customer. Another challenge in imposing broad fiduciary duties in banks is that costs to consumers, including the cost of providing mobile banking services may increase.

Despite the increase in potential costs, fiduciary duties will encourage banks to serve the interests of consumers and, in last instance, the associated interests of financial markets and society. According to John Glover, “[e]quitable intervention could be justified as being what is necessary to protect customers’ ‘reasonable expectations’ that their bank will act in their interest, not someone else’s interest.” Imposing fiduciary duties will force banks to take more preventive measures. For instance, after the CFPB called the attention of banks to their responsibility for faults of the vendors they work with, banks have improved their vendor management programs. In fact, in anticipation of such liability, Edward Kramer, executive vice president of regulatory affairs for Wolters Kluwer Financial Services, noted that “some banks made moves to put better programs in place in recent years, while other already had them... [for instance banks] dig deeper to find out if and when vendors are using third-party data centers themselves.”

Given the role of banks in society, there is nothing abnormal in requiring a bank to refrain from acting in a certain way to obtain an advantage at the expense of consumers. Banks will be probably burdened and profits might be hurt. Shareholders of financial institutions will likely complain. On the other hand, banks will survive because society needs banks. Fiduciary duties applied to mobile financial services serve exactly the purpose they were created for, which is to constrain banks from freely pursuing their profit-oriented interests at the cost of their customers.

V. CONCLUSION

Safety, soundness, and the protection of customer information by financial institutions, should always be the main concerns for regulators.

Mobile banking should afford customers the same level of protection that has always been guaranteed by the delivery of financial services through

---

278. Curtis, supra note 131, at 831.

279. Id.

280. Buestetta, supra note 137, at 413.

281. Glover, supra note 237, at 5.


283. Id.; FDIC, supra note 52 (“[F]inancial institution[s] should broadly consider the impact of its mobile banking strategy on operations and take steps to ensure the compliance management system addresses the types of mobile banking technology used by the institution.”).

traditional channels. Given the current regulatory framework, applying a more flexible fiduciary duties approach to mobile financial services will give incentives to financial institutions better provide and coordinate the service, as well as make these services more reliable and better able to protect the consumers of this new technology. Fiduciary duties will help fill this gap and will allow courts to impose the interests of society on bank, and not the other way around.

At the same time, fiduciary duties should not be found to impose such a burden to hinder beneficial innovation in this industry. Innovation through mobile financial services should be encouraged, but regulators should beware and utilize every option it has to protect consumers that are susceptible to the inherent risks created by mobile technologies. It is the role of courts to implement a more flexible approach and provide the parameters banks should be deemed to expect application of fiduciary duties to mobile financial services.