BANKING & FINANCE

LAW REVIEW

Revue de droit bancaire et de finance

CARSWELL®

Mobile Financial Services: The Need for a Comprehensive Consumer Protection Law

Professor Mark E. Budnitz[*]

The article first describes mobile financial services for consumers and the types of companies participating in the provision of those services. Anticipated consumer problems are explored, including: security, privacy, unauthorized transfers, error resolution, viruses, system breakdown, consumer mistake, and the need for documentation and a history of transactions. Public policy and government regulatory issues are examined. Applicable U.S. state and federal laws are reviewed; their gaps and inadequacies are identified. The article concludes with a description of a Model Law that provides satisfactory consumer protection.

L'auteur décrit d'abord les services financiers mobiles offerts aux consommateurs ainsi que les types d'entreprises qui proposent ces services. Les problèmes susceptibles d'être rencontrés par les consommateurs sont analysés : sécurité, confidentialité, transferts non autorisés, erreurs, virus, pannes de système, erreurs de leur part, obtention de documentation relative aux opérations et leur historique. Les politiques et les règlements adoptés par les autorités gouvernementales sont examinés par l'auteur. Les lois américaines applicables sont étudiées et leurs lacunes et déficiences mises en évidence. En conclusion, l'auteur donne la description d'une loi type qui offrirait une protection adéquate aux consommateurs.

1. INTRODUCTION

Consumers increasingly use cell phones to engage in mobile financial services. This article examines legal issues that are critical to adequate consumer protection. Part 2 of the article describes how various mobile financial services systems work and the types of companies participating in providing these services. Part 3 predicts what problems consumers likely will encounter when they use these services. Part 4 reviews applicable United States laws. Part 5 proposes a model law.

2. DESCRIPTION OF HOW VARIOUS SYSTEMS WORK AND THE COMPANIES PARTICIPATING

A comprehensive examination of the systems used to provide mobile financial services and the companies involved in offering those services is beyond the scope of this article. A brief description of certain elements, however, is necessary to provide background for the regulatory proposals that are the focus of this article.

---

* Mark E. Budnitz, Bobby Lee Cook Professor of Law, Georgia State University College of Law.

(a) The Three Channels for Delivering Services

Mobile financial services are being offered via three "channels":[1] text messages, wireless applications on cell phone Internet browsers, and software applications downloaded onto cell phones.[2] All three offer consumers many benefits.[3] However, the rising popularity of these methods also raises problems for consumers that merit possible regulatory attention.

Consumers may send text messages using the Short Message Service (SMS) to instruct banks to perform banking functions, such as transferring funds. Banks may use SMS to send messages, such as alerts when a consumer's balance is low and marketing promotions. Some providers permit person-to-person transfers.

Disadvantages of using SMS include its limitation to a small number of characters per message, the cost of sending text messages, lack of security due to a lack of strong encryption and user authentication procedures, infection by viruses,[4] and fraud through techniques such as phishing. In addition, there is a risk of mistake. For example, the consumer who intends to make a payment transfer of $20 to pay an obligation might unintentionally type $200 instead.

Using the cell phone's Internet browser provides consumers with all the advantages of on-line banking from a personal computer. Disadvantages include the risk of security breaches, viruses, fraud, and mistake.

Consumers may prefer to download software onto their devices. Telecommunications companies, however, have been unwilling to allow downloading mobile financial services software without their permission.[5] Even if permission is granted, there are disadvantages, such as the possibility of defective software and the risk of security breaches, viruses, fraud, and mistake.

---

1 Steve Bills, "Fiserv Mobile Product Handles All 3 Channels", *American Banker* (9 September 2008) (WL).

2 *Ibid.* Financial institutions offer a choice because they believe different customers will prefer different channels. For example, one analyst thinks consumers without bank accounts and younger consumers prefer using text messaging. *Ibid.* Credit unions are mainly using text messaging and browser services, but they may increasingly adopt software download programs. Bank of America reports that it has more than three million mobile banking customers, and that 43 percent use a Phone or iPod touch to do their banking. Susan Stellin, "Checks join the world of paperless banking. U.S. firm will let clients make deposits by using an iPhone's camera", *Int'l Herald Tribune* (11 August 2009).

3 See Steve Bills, "Text Service for USAA Members" *American Banker* (18 July 2008), online: American Banker <http://www.americanbanker.com/issues/173_140/-358144-1.html>; "USAA Catches up on BofA and other big players in mobile banking" *Ecommerce Journal* (19 May 2009), online: Ecommerce Journal <http://ecommerce-journal.com>; USAA Federal Savings Bank serves military personnel and their families throughout the world; it offers all three channels. *Ibid.*

4 Dan Balaban, "NFC Mobile Payment: A New Frontier In The Security Battle?", *Cards & Payments* (August 2009) (Lexis) ("phones generally have an insecure keypad, and viruses can infect handsets, which some experts — though not all — say could enable hackers to monitor PIN entry").

5 Bills, *supra*, n. 2.

(b) Two Types of Transfers: P2B and P2P

Consumers can perform two types of transfers of their funds to others: from the consumer to a business (P2B) and from the consumer to another individual (P2P).[6] Consumers have traditionally made P2B transfers to pay bills in many forms, including: cash, check, credit and debit cards, electronic bill paying, and preauthorized electronic transfers. Consumers have more limited options for P2P transfers because they generally are limited to cash and checks.[7] Mobile banking provides another option.

Companies are structuring P2P in various ways. MasterCard permits consumers to send funds from either their credit or debit card accounts using an iPhone or iPad.[8] The transfer is processed through MasterCard's network and the transfer takes place "nearly in real time."[9] Another company uses the automated clearinghouse network (ACH).[10] Payments through the ACH network take a day or more to settle.

(c) Types of Companies Participating in Mobile Financial Services Transactions

Consumers encountering difficulties with their mobile financial transactions face many obstacles to obtaining relief; some of those obstacles relate to the fact that several companies are involved in a typical transaction. First, the consumer must identify the source of a problem — potentially found in software, hardware, or transmission of a message. Second, the consumer must determine which company or companies among several that participated in the transaction might be responsible for that problem. Third, the consumer needs to determine how to try to resolve the problem with that company. Options include complaining directly to the company or returning to the store where the consumer purchased the product or service, which may be different from the company providing the service or that manufactured the goods. The consumer's problem is aggravated by the fact that the companies involved are very different types of businesses. Some may have physical stores, while others may only have an online presence. A given company may be more responsive to consumer complaints than others.[11] This may be, at least in part, due to the fact that some, such as banks, are regulated far more than others.[12] Consumers who want to resort to the law for protection encounter even more complications. Part 5 discusses how very different laws apply to mobile financial services depending on the nature of the consumer's problem and the type of company

---

6 Oz Shy, "Person-to-Person Electronic Funds Transfer: Recent Developments and Policy Issues" (2 March 2010) at 5, online: Federal Reserve Bank of Boston <http://www.bos.frb.org/economic/ppdp/2010/ppdp1001.pdf www.bos.frb.org>.

7 A few banks permit P2P transfers as part of the online banking service. *Ibid.*, at 6.

8 Will Wade, "MC Offers Cash-Transfer App for iPhone", *American Banker* (7 June 2010).

9 *Ibid.*

10 *Ibid.*

11 For further discussion see text accompanying notes 67-68.

12 For further discussion see text accompanying notes 19–25.

that may be liable.

There are several parties participating in mobile payment transactions.[13] Mobile network operators (MNO) operate the wireless networks through which transaction communications flow.[14] Financial institutions are another participant.[15] MNOs do not have a great deal of experience providing payment services, so they often need to collaborate with financial institutions.[16] Consumers using the mobile payments services charge their purchases to their credit cards; thus, MasterCard, Visa, and comparable companies are another type of participant.[17] For other types of mobile financial services, credit card companies may not be involved, but the consumer's financial institution usually is a key player because the money typically comes out of the consumer's account.[18]

There are several different types of financial institutions; an important policy issue arises from the participation of some institutions that have control over consumers' money but are not as strictly regulated as banks.[19] One example is PayPal, which has expanded aggressively into mobile financial services. It has partnered with companies that offer electronic commerce platforms to merchants enabling

---

13 Judith Rinearson, "The Next New Thing: Mobile Payments" (2007) 3 J of Payment Systems L 82 at 85-86. MNOs play a crucial role in mobile payment transactions because they "have a huge customer base, and because they control the subscriber identity module (SIM) and/or the wireless identity module (WIM) card of the mobile device . . .." *Ibid.*

14 Examples of MNOs include Sprint, Bruce Cundiff, "Obstacles, Opportunity For the Mobile Wallet" *American Banker* (15 July 2009), and T-Mobile, Ian Grant, "Google could launch Android phone today" *Computer Weekly* (12 January 2010), online: <http://www.computerweekly.com/Articles/2010/01/05/239813/Google-could-launch-Android-phone-today.htm>.

15 Rinearson, *supra*, n. 13 at 85. In addition to traditional financial institutions such as banks, PayPal also has entered the field. Daniel Wolfe, "PayPal Responds to Rapid Evolution in Smartphones", *American Banker* (20 January 2009) (reporting that all purchases made with BlackBerry devices will pass through PayPal's system).

16 *Ibid.* But see Chris Constanzo, "A Mobile Plan B: Bypass Carriers by Using Bluetooth", *American Banker* (9 January 2009) (reporting that a Hungarian company is promoting using the Bluetooth format for mobile payments, instead of NFC).

17 Daniel Wolfe, "Contactless Cards Go Untouched", *American Banker* (22 January 2010) (reporting that JP Morgan sent Visa contactless cards to its customers); Steve Bills, "Consumer Trends Bode Well For Mobile Payment Adoption", *American Banker* (15 October 2009) (reporting that MasterCard had entered into agreements with major retailers that made the technical improvements needed to accept contactless cards).

18 For example, credit cards are not involved where the payment may be made as an electronic fund transfer through the ACH network. Alternatively, the goods or services may be charged to the consumer's phone bill and the consumer may pay the bill with a check.

19 Cindy Merritt, "Mobile P2P money: Contemplating new risks while analyzing adoption potential" *Portals and Rails* (1 June 2010), online: Federal Reserve Bank of Atlanta <http://portalsandrails.frbatlanta.org/2010/06/mobile-p2p-money-contemplating-new-risks-while-analyzing-adoption-potential.html> ("[p]articipants in the payments value chain are increasingly disintermediated and outside the traditional legacy banking environment where the regulatory and legal governances are well established".).

consumers to pay using their PayPal accounts.[20] Most significantly, PayPal has opened access to its platform to third-party software developers.[21] For example, such a developer could offer an iPhone application allowing consumers to order pizza and pay using their PayPal account.[22] Commenting on PayPal's expansion, one industry observer noted, "PayPal is going 'anywhere the online channel reaches, so they're certainly not dependent on the browser.'"[23] Despite its growing presence in many aspects of payment systems, PayPal is not regulated as a bank. It is licensed as a money transmitter in 40 states and the District of Columbia.[24] Money transmitters are subject to minimal regulation that includes almost no consumer protection.[25]

Companies that manufacture cell phones obviously are also essential participants because "they control the technology and capabilities of the end-device."[26] Software manufacturers play a vital role as well because they "develop the means of implementing [a mobile payment] infrastructure by producing standard compliant software that will connect the different parts of the [mobile payment] process."[27] The various industry players may cooperate with each other.[28] Moreover, a company in one industry may invest in a company in another industry, such as when device manufacturer Nokia bought a stake in Obopay, a major software company.[29] Transactions such as these raise questions as to whether software companies can independently develop software that is best for mobile financial services as a whole, or only what can be best integrated into the device manufacturer's phones when there are financial incentives for such integration.

It is unclear which type of company will control mobile financial services. The telecoms such as Verizon and AT&T would seem to be in an excellent position to do so. If that happens, the industry will develop around a "carrier-centered

---

20 Magento, Inc., "Magento and PayPal Expand Relationship to Drive e-Commerce Innovation" (19 March 2010), online: Magento <http://www.magentocommerce.com/images/uploads/Press_March08_2010.pdf>.

21 Daniel Wolfe, "PayPal Looks Past Web to Find Its Future", *American Banker* (27 July 2010) (WL).

22 "PayPal poised to outgrow the rest of eBay's business", *The News Journal* (13 January 2010) (WL).

23 Wolfe, *supra*, n. 21.

24 *PayPal State Licenses*, online: PayPal <https://www.paypal-media.com/licenses>.

25 Mark E. Budnitz et al, "Home Banking Agreements: Don't Bank on Them" (2006) 61 Bus Lawyer 641 at 670. See also Courtney J. Linn, "One-Hour Money Laundering" (2007) 8 UC Davis Bus LJ 138, n.182; Patricia Allouise, Sarah Jane Hughes & Stephen T. Middlebrook, "Developments In The Laws Affecting Electronic Payments and Stored-Value Products: A Year of Stored-Value Bankruptcies, Significant Legislative Proposals, and Federal Enforcement Actions" (2008) 64 Bus Law 219 at 235.

26 Rinearson, *supra*, n. 13 at 85.

27 *Ibid.*, at 85-86.

28 Wolfe, *supra*, n. 15; Bills, *supra*, n. 17.

29 Daniel Wolfe, "Nokia Money Moves Obopay Closer to Global Platform", *American Banker* (27 August 2009) (WL); Steve Bills, "Nokia Make a Call for Global Mobile Payments", *American Banker* (26 March 2009) (WL).

model."[30] But the phenomenal success of the iPhone and iPad may push them instead into the role of a mere "conduit for devices and content produced elsewhere."[31] Financial institutions are involved in most mobile financial services transactions and would seem to be in a strong position to control the marketplace. But their recent financial troubles have hindered their ability to invest in new payment technology to replace their legacy systems.[32] Meanwhile, nonbanks "continue to drive technology investment opportunities, which in turn lead to the development of alternative forms of retail payments."[33]

The participation of so many different types of companies poses a substantial challenge to regulators. Some of the industries involved are subject to rigorous regulation, others to little or none; some are governed by federal regulations, some by state regulations. If consumers are to be protected, the relevant agencies must cooperate. However, regulatory agencies "are accustomed to operating independently and autonomously from one another and may be challenged to work collaboratively."[34]

3. ANTICIPATED CONSUMER PROBLEMS

Consumer acceptance of mobile financial services may be seriously hampered by problems that consumers can reasonably anticipate, resulting in the loss of funds in the consumer's account.

(a) Security and Privacy

Security and privacy are major consumer concerns.[35] The two are closely related: to the extent the mobile financial services system has poor security, there is an increased risk that the consumer's privacy will be invaded. In addition, if security is inadequate, there is a greater risk of fraud, including identity theft and unauthorized transactions.[36] There are indications that unsatisfactory security has led to consumer privacy invasions and fraudulent charges. The FBI's Cyber Division has been investigating instances of malicious programs intended to interfere with mo-

---

30 Niraj Sheth, "For Wireless Carriers, iPad Signals Further Loss of Clout", *The Wall Street Journal* (28 January 2010), online: The Wall Street Journal <http://online.wsj.com/article/SB10001424052748703410004575029631361786998.html>.

31 *Ibid.*

32 Cindy Merritt, "If nonbanks drive payment innovation, will banks pay for the risk management?" *Portals and Rails* (7 December 2009), online: *Federal Reserve Bank of Atlanta* <http://portalsandrails.frbatlanta.org/2009/12/nonbanks-are-driving-significant-investment-in-the-retail-payments-space-today-a-healthy-signal-to-the-economy-that-contrast.html>.

33 *Ibid.*

34 Merritt, *supra*, n. 19.

35 Breffni McGuire & Marianne Crowe, "Mobile Banking in New England: The Current State of the Market" (August 2009) at 6, 31, online: Federal Reserve Bank of Boston <http://www.bos.frb.org/bankinfo/firo/publications/bankingpaypers/2009/MobileBanking-8-09.pdf>.

36 See text accompanying notes 53-54.

bile banking.[37] In June 2010, consumers who accessed their AT&T accounts to order the new iPhone found personal information about other customers was displayed.[38] Banks have been slow to offer apps for mobile banking.[39] As a result, software developers have been offering their own apps available on Google's Android operating system. Some of these apps have been removed because of suspected fraud, including theft of financial information.[40] For example, the "SMiShing" virus specifically infects mobile phones.[41] SMiShing and other malware "may be creating new and poorly understood vulnerabilities and hacker threats in the payments environment."[42] In another notable case, fraudsters placed a program on many Nokia phones that resulted in charges of small amounts to their wireless accounts.[43]

Companies can guard against security threats through encryption, requiring multifactor authentication, antivirus software, and transaction limits.[44] Bank examiners may require financial institutions to have adequate safeguards.[45] Those mea-

---

37 Spencer E. Ante, "Dark Side Arises For Phone Apps" *The Wall Street Journal* (3 June 2010), online: The Wall Street Journal <http://online.wsj.com/article/SB10001424052748703340904575284532175834088.html>. Consumers may be deprived, at least temporarily, of their ability to engage in mobile banking for other reasons besides those mentioned in the text. For example, Google removed dozens of unauthorized mobile banking apps because of trademark violations. *Ibid.* Mobile banking software may be infected by malware inserted by foreign countries engaging in espionage. *Ibid.*

38 Daniel Wolfe, "Apple Peeled", *American Banker* (23 June 2010) 5. See Debra Cassens Weiss, "Law Firm Abandons iPhone After Experts Warn of Security Issues" *ABA Journal* (9 December 2009), online: American Bar Association <http://www.abajournal.com/news/article/law_firm_abandons_iphone_after_experts_warn_of_security_issues> (reporting that the iPhone takes screenshots of users' data).

39 Daniel Wolfe, "Users Want Android, Banks Don't Have It", *American Banker* (17 June 2010) 1.

40 *Ibid.*, at 9. Aleksandra Todorova, "'Phishing' Scams Cast Net on Mobile Banking", *The Wall Street Journal* (31 January 2010).

41 "SMiShing" (3 February 2011), online: Wikipedia <http://www.en.wikipedia.org/wiki/SMiShing>.

42 Clifford S. Stanford, "Building a bridge: Will proactive discussions of fraud concerns help drive financial services and telecom industry collaboration in the emerging mobile payments context?" *Portals and Rails* (20 October 2009), online: Atlanta Federal Reserve Bank <http://portalsandrails.frbatlanta.org/2009/10/building-a-bridge-will-proactive-discussions-of-fraud-concerns-help-drive-financial-services-and-tel.html>.

43 Brad Stone, "As Phones Do More, They Become Targets of Hacking", *The New York Times* (21 December 2010).

44 See McGuire & Crowe, *supra*, n. 35 at 6. But see Sharon Nelson & John Simek, "Parting the Curtains on the iPhone's Security Problems", *Law Practice* 35:7 (Nov/Dec. 2009) 24, online: American Bar Association <http://www.americanbar.org/publications/law_practice_home/law_practice_archive/lpm_magazine_articles_v35_is7_pg24.html> (describing simple techniques that can decrypt the iPhone's encryption program).

45 Frederick M. Joyce et al, "Mobile Banking: Challenges, Opportunities, and Need for Best Practices", *Banking Report* 91 (15 December 2008) 1137.

sures should require more than downloading satisfactory security controls when the consumer registers for mobile banking services:

> It is an ongoing process of monitoring, evaluating and adjusting to new threats. This means that the Financial Institution must have an ongoing capability to download upgrades, patches and changes to its Mobile Banking product which the customer must install to continue using the product.[46]

Even assuming bank examiners will require institutions to establish adequate security measures, many of the participants in mobile financial services transactions are not subject to regular examinations by government officials and are not subject to laws establishing security requirements for such services.[47] In order to ensure the safety and integrity of mobile financial services, government should bring these "non-banks" under the regulatory umbrella.[48]

Another type of security risk is impervious to the strongest encryption. If many consumers use their cell phones to engage in financial transactions and store financial and other valuable information, "would-be thieves will see every person walking down the street talking on his or her phone as a target for robbery," possibly resulting in "the ultimate form of identity theft".[49] The risk is not only that the thief will steal the phone and have access to the information stored in it with the ability to obtain access to the consumer's funds and identity — encryption arguably can safeguard against that. The risk also is to the consumer's physical security. The consumer may be injured or killed by a person bold enough to steal the phone.

In addition to the need for government oversight to ensure the security of the system, the various companies involved in a mobile financial services transaction must cooperate and coordinate in order to ameliorate the harm that consumers may incur as a result of a security breach or a stolen phone that could possibly result in a security breach. This may be difficult to achieve because financial institutions and telecoms have different registration and authentication protocols.[50] Moreover, the two types of companies may not communicate effectively when one detects a fraudulent transaction.[51] The failure of companies to agree on the procedures to follow when possible fraud occurs may have serious repercussions. For example, when a consumer tells a telecom that a phone is lost or stolen, the telecom may not inform the financial institution of the incident, preventing the financial institution from taking steps to avoid fraud.[52]

---

46 *Ibid.*

47 *Infra*, n. 107.

48 *Infra*, n. 127.

49 John D. Sutter, "Wallet of the future? Your mobile phone" (13 August 2009), online: CNNTech <http://articles.cnn.com/2009-08-13/tech/cell.phone.wallet_1_mobile-phone-cell-mobile-payments?_s=PM:TECH> (reporting the views of Lillie Consey, associate director of the Electronic Privacy Information Center).

50 Stanford, *supra*, n. 42 at 33.

51 *Ibid.*

52 *Ibid.*

(b) Liability for Unauthorized Transfers

Consumers also risk unauthorized transfers from their accounts. The *Electronic Funds Transfer Act* (EFTA) and the *Federal Reserve Board's Regulation* E likely apply to mobile financial services.[53] However, they provide only limited protection. The consumer's liability increases if he or she delays in notifying the financial institution.[54]

(c) Error Resolution

When a consumer discovers an error in an electronic funds transfer, under Reg. E he or she may complain to the financial institution, which is required to investigate its records.[55] But companies that are not regarded as financial institutions, often known as "non-banks", are becoming involved in mobile financial services;[56] these entities may claim that they are not "financial institutions" subject to Reg. E's error resolution requirements.[57] Furthermore, some systems bypass financial institutions altogether and consequently may not be bound by Reg. E.[58] If Reg. E does not apply, and the parties to the transaction refuse to cooperate and investigate the consumer's complaint, the consumer's only recourse is to sue in court or submit the complaint to arbitration if the parties' agreement requires the latter.

Even if Reg. E applies, its "four walls" rule generally requires a financial institution to examine only its own records to determine if it made a mistake, rather than requiring the institution to examine the records of others entities involved in the transaction.[59]

Regardless of what the law requires, a key missing link is the lack of any standards for cooperation and information sharing among the parties to the transaction. For example, if a consumer's cell phone is lost or stolen, the consumer's immediate and reasonable response would likely be to notify the telecom from which the consumer purchased the phone. There is no legal requirement or even industry protocol encouraging the telecom to promptly notify the consumer's financial institution.

(d) Viruses, System Breakdowns, and Power Failures

One of the advantages of using mobile financial services is the ability to delay paying bills until shortly before they are due. Viruses, system breakdowns, power failures, and other incidents completely beyond the consumer's control, however,

---

53 See text accompanying notes 82–93.

54 12 CFR §205.6; see text accompanying notes 97-98.

55 12 CFR §205.11.

56 See text accompanying note 26.

57 12 CFR §205.2(i) (defining "financial institution").

58 Marc Bourreau & Marianne Verdier, "Cooperation for innovation in payment systems: the case of mobile payments, communications and strategies", *Communications & Strategies* (1 July 2010) (WL).

59 12 CFR §205.11(c)(4); see text accompanying note 100.

may delay transmission of payment until it is past due.[60] This may result in late charges, penalties, and overdraft fees. If a consumer has made previous late payments, another late payment may cause serious consequences, such as commencement of eviction proceedings by a landlord or repossession of the consumer's car by a secured creditor.

Moreover, consumers' agreements with their banks likely provide that the bank is not liable for damages for this type of loss.[61] Consumers should be concerned about their lack of legal remedies if they suffer damages as a result of these occurrences.[62]

(e) Mistake

Consumers can simply make mistakes when engaged in mobile banking. For example, if the consumer does mobile banking over the web, the consumer may click on the wrong button. The *Uniform Electronic Transactions Act* provides limited relief.[63]

(f) Paper Documentation

Sometimes consumers need paper documentation of their transactions. For example, a landlord may claim the consumer never paid the rent and insist that the consumer provide a hard copy document from the consumer's bank as proof of payment. Consumers may be concerned that their banks will refuse to provide the paper documents, take too long to cooperate, or charge too much for this service.

(g) History of Transfers

Consumers sometimes require a history of their transfers and other mobile financial transactions, such as when they need an audit trail. Banks could refuse to produce this for the consumer or make it available only after undue delay or at an excessive price.

(h) Payment Disputes with Telecoms

Consumers have already been using mobile banking services that bypass the consumer's banks altogether. Instead, the consumer transfers funds and pays

---

60 Roger Cheng & Phred Dvorak, "Blackberry Maker Is Strained by Growth", *The Wall Street Journal* (24 December 2009) (reporting that because of a flaw in its instant-messaging program, BlackBerry users endured service interruptions for two days); Rob Gillies, "BlackBerry outage is second in a week", *Atlanta Journal Constitution*, (24 December 2009) (reporting that BlackBerry had two outages in December, 2009 and at least three in 2008); "T-Mobile once again selling Sidekick phones", *Atlanta Journal Constitution* (18 November 2009) (reporting that a server meltdown at Microsoft resulted in personal information disappearing from T-Mobile cell phones and consumers losing e-mail and web access).

61 Budnitz, *supra*, n. 25 at 643.

62 See text accompanying note 129.

63 *Uniform Electronic Transactions Act* (UETA) §10(2) (1999). See text accompanying notes 117–21.

through the telecom's billing procedure.[64] This is a risky practice for consumers; complaints about marketing and billing practices are a major source of consumer dissatisfaction with telecoms.[65] A billing error by a telecom is especially serious for consumers who are elderly, disabled, and live in rural areas far from banks and/or reliable and affordable Internet service. These consumers need to use their cell phones to engage in essential transactions; yet if they refuse to pay whatever charges the telecom demands, their cell phone service will be terminated, ending their ability to conduct mobile banking.

Fraudsters also put unauthorized charges onto consumers' telephone bills — a process known as "cramming".[66] At least one major telecom reportedly has no plans to verify these charges to make sure they are valid.[67] The Federal Trade Commission (FTC) has announced that it is considering requiring telecoms to investigate consumers' cramming complaints, but has not yet taken any formal action.[68] This type of fraudulent scheme is easy to accomplish: all the fraudster needs is the consumer's telephone number. In contrast, credit cards and debit cards come with security features, such as passwords, PIN, and signature requirements.[69] Federal law also places a cap on the consumer's maximum liability for unauthorized credit and debit card transfers.[70]

---

64 "Your Business", *Augusta Chronicle* (19 December 2010) (WL) (describing how persons can support Haiti disaster relief by sending a text message, resulting in charges to their cell phone bills).

65 See Joelle Tessler, "FCC oversight of wireless lax GAO looked at complaints; billing", *The Journal-Gazette* (14 December 2009) (WL) (reporting on GAO study of wireless carriers that found through a consumer survey that billing practices were a major complaint, that the FCC has not enforced its billing rules, and that states are reluctant to deal with billing disputes because they are uncertain they have the authority to do so); "FCC Should Adopt Consumer Policies To Facilitate Telecom Purchases, FTC Says", *Electronic Commerce & L Rep* (4 November 2009) (reporting on consumer complaints to FTC that consumers are confused by ads for communication services that do not disclose the full cost and cannot understand major features and the cost of options). See John Murawski, "Phone oversight may end", *The News & Observer* (18 April 2009) (WL) (reporting on a bill before the North Carolina legislature that would end the Utilities Commission's authority to resolve consumer billing disputes).

66 "Beat the new 'cramming' scams", *Consumer Reports* (August 2010) 13 (reporting on FTC actions against third party billers and billing aggregators who put unauthorized charges on consumers' phone bills); Ron Burley, "Well, I'll Be Crammed", *AARP* (May & June 2010) 22 (reporting on the FTC's two actions against a third party clearinghouse for unauthorized charges it placed on consumers' phone bills); "FTC Halts Massive Cramming Operation that Illegally Billed Thousands; Alleges Scam Took in $19 Million over Five Years" (1 March 2010), online: Federal Trade Commission <http://www.ftc.gov/opa/2010/03/inc21.shtmwww.ftc.gov> (reporting that an internet services company billed consumers and small businesses unauthorized charges that were put on the customers' telephone bills).

67 Burley, *supra*, n. 66.

68 *Ibid.*

69 *Ibid.*

70 12 CFR §226.12; 12 CFR §205.6.

4. PUBLIC POLICY & GOVERNMENT REGULATORY ISSUES

Several significant public policy and regulatory issues should be resolved in order to ensure that the costs of mobile financial services to society as a whole are not greater than their benefits. One important policy objective is "ensuring the integrity, effectiveness, accessibility of U.S. payment systems."[71] The Federal Reserve has a major responsibility for achieving this goal.[72] In addition to its macro role in setting national monetary policy,[73] the Fed is intimately involved in regulating the systems[74] and operating the automated clearinghouse network (ACH) through which mobile payments are transmitted.[75]

There are several facets to ensuring integrity, effectiveness, and accessibility, however, and the law is not clear about which government agencies are responsible for these facets as applied to mobile financial services. For example, because these services present many consumer protection issues, the Federal Reserve Board (FRB), FTC and the new Consumer Financial Protection Bureau may all be appropriate agencies to address these issues.[76] It is also unclear who should be responsible for the security of the systems providing the service.[77] Criminal law enforcement agencies should be involved because mobile financial services may be used for money laundering.[78]

Another law enforcement issue is consumers' physical safety. One company targeting Hispanic immigrants claims that using mobile financial services provides greater safety because using those services means consumers do not need to carry cash.[79] But there is greater safety only if the thief somehow knows that the victim uses a cell phone instead of cash, and that the thief knows the phone has built-in safeguards preventing him from being able to transfer funds to himself or obtaining

---

71 Marianne Crowe, Marc Rysman & Joanna Stavins, "Mobile Payments in the United States at Retail Point of Sale: Current Market and Future Prospects" (17 May 2010), online: Federal Reserve Bank of Boston <http://www.bos.frb.org/economic/ppdp/2010/ppdp1002.pdf>.

72 *Ibid.* In the future, the newly established Consumer Financial Protection Bureau also may play an important role. See Pub L No 111-213 (2010).

73 One "macro" issue related to mobile payments is changes such payments may cause in the "velocity" of money transfer. Mobile payments, including P2P, may result in money transfers occurring more rapidly. Greater velocity is a benefit to the economy. See Edris Kisambira, "MTN Unveils Mobile Money Transfer Service", *East African Business Week* (15 March 2009) 29.

74 *Regulation E*, 12 CFR Part 205 (regulating electronic funds transfers); *Regulation CC*, 12 CFR Part 229 (regulating availability of deposited funds and substitute checks).

75 Crowe, *supra*, n. 71 at 33 (stating that the FRB is "the primary ACH operator").

76 See *ibid.*, at 31.

77 *Ibid.*

78 Ana Cavazos-Wright, "Will the migration to mobile payments be tempered by potential money laundering risks?", *Portals and Rails* (21 June 2010), online: Federal Reserve Bank of Atlanta <http://portalsandrails.frbatlanta.org/2010/06/will-migration-to-mobile-payments-be-tempered-by-potential-money-laundering-risks.html>.

79 Will Hernandez, "Prepaid Account Offers Mobile Banking Service to Immigrants", *American Banker* (7 April 2009) (WL).

valuable information from the phone.

Several companies are developing applications that expose consumers to advertising on their cell phones alongside mobile financial services.[80] As with any advertising medium, there is the potential for unfair and deceptive advertisements. The FTC regulates advertising; it saw the need to revise its rules on celebrity endorsements to accommodate the web.[81] Advertisements accompanying mobile financial services also may require new or revised rules.

Finally, the large number and different types of parties involved in mobile financial service transactions present formidable problems when one of the parties becomes insolvent, resulting in a financial loss to the thousands of consumers whose transfers do not go through because of the insolvent party's failure to perform its part of a transaction.

5. LAWS THAT APPLY TO MOBILE FINANCIAL SERVICES

(a) The EFTA and Reg. E

The EFTA was enacted long before the invention of cell phones and the development of mobile financial services. Thus, its language does not easily apply to cell phones used for these services. The EFTA and Reg. E, however, apply to transfers using cell phones under a reasonable construction of those laws.

The EFTA applies to electronic fund transfers.[82] Electronic fund transfers are defined, inter alia, as "any transfer of funds that is initiated through" a telephone.[83] But *excluded from coverage* is:

> Any transfer of funds that:
>
> (i) Is initiated by a telephone communication between a consumer and a financial institution making the transfer; and
>
> (ii) Does *not* take place under a telephone bill-payment or other written plan in which periodic or recurring transfers are contemplated.[84]

In other words, if a consumer initiates a transfer by phone, the EFTA applies only if the telephone transfer is pursuant to a plan "contemplating" periodic or recurring transfers.

At the time the EFTA was enacted, consumers rarely used their landline telephones to transfer funds. They called their bank for that purpose and only on an occasional basis when there was a special need to do so. Congress apparently believed consumers did not need the EFTA's protections under these very limited

---

80 Jessica E. Vascellaro & Emily Steel, "Giving Mobile Ads a Makover", *The Wall Street Journal* (28 January 2010); Nancy J. King, "Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices" (2008) 60 Fed Comm LJ 229.

81 "Guidance Governing Celebrity Endorsements and Bloggers" (5 October 2009), online: Federal Trade Commission <http://www.ftc.gov/opa/2009/10/endortest.shtm>.

82 12 CFR §205.3(a).

83 12 CFR §205.3(b)(1).

84 12 CFR §205.3(c)(6) (italics supplied). Reg. E's language closely tracks that of the EFTA, 15 USC §1693a(6)(E).

circumstances. In contrast, a consumer in the 21st Century who transfers funds using a cell phone does so pursuant to an agreement with a financial institution (a "written plan") whereby the financial institution agrees to permit the consumer to transfer funds using the institution's mobile financial services program whenever the consumer chooses to do so. Courts and regulators should interpret these payment transactions using mobile devices as taking place under a "written plan in which periodic or recurring transfers are contemplated" and therefore subject to the EFTA and Reg. E.

In a case involving an imposter and unauthorized withdrawals, the Fifth Circuit provided an alternative rationale for excluding transactions that do not occur pursuant to plans contemplating periodic or recurring transfers.[85] The Fifth Circuit concluded that Congress intended to exclude non-recurring consumer transfers initiated by telephone conversations because such transfers involve a "personal element" of "human contact" that makes such transfers less susceptible to fraud and unauthorized use than "computerized pay-by-phone systems." The court further noted that in a "non-recurring, consumer-initiated" telephone transfer, "the failure to attempt to make a positive identification of the caller might be considered negligence or a breach of the deposit agreement under state law." In other words, consumers did not need the benefit of the EFTA because state law could protect consumers. This rationale does not apply to cell phone transactions because there is no "personal element" or "human contact" when consumers send text messages or click on a website from their cell phones to engage in payment transfers.

The EFTA and Reg. E do not define "periodic or recurring," and nothing in those laws indicates those terms cannot apply to cell phone transfers. Moreover, under Reg. E, EFTA coverage is not restricted to bill paying because it covers "bill-payment *or other written plan.*"[86] Furthermore, the EFTA provision is not confined to plans involving payments because it uses the term "transfers". Reg. E makes it clear that an electronic transfer includes other types of transfers besides bill payment by including ATM transfers and direct deposits and withdrawals.[87]

Applying the EFTA and Reg. E to cell phone transfers is also supported by an Official Staff Interpretation. That Interpretation explains that the "plan" requirement is not limited to the situation (like the one in the typical preauthorized transfer plan) in which payments are made on a regularly recurring basis, such as paying rent or a mortgage. The Interpretation states that transfers are covered even if "[t]he consumer uses the plan infrequently."[88] The Interpretation also indicates that the EFTA should be read expansively by taking a broad view of the meaning of initiating a communication by telephone. The Interpretation states that a telephone call is covered by the EFTA "even though" the consumer uses a fax machine to initiate the transfer[89] or the consumer initiates the call using the bank's "audio-response or

---

85 *Kashanchi v. Texas Commerce Med. Bank*, 703 F (2d) 936 (5th Cir 1983) [*Kashanchi*]. See also *Abyaneh v. Merchants Bank*, 670 F Supp 1298 (MD Pa 1987).

86 12 CFR §205.3(c)(6) (italics supplied).

87 12 CFR §205.3(b)(ii)-(iii).

88 Supp I to Part 205, §205.3 at para. 3(c)(6).

89 *Ibid.*

voice-response telephone system."[90]

A broad construction that subjects mobile financial transfers to the EFTA is consistent with the EFTA's "primary objective," which is "the provision of individual consumer rights."[91] Furthermore, it is consistent with the EFTA's legislative history. Congress intended to exclude informal, incidental phone conversations, such as when a consumer calls a bank teller and requests a transfer from a savings account to a checking account to cover an overdraft.[92] The Fifth Circuit agreed with a commentator who explained:

> [T]elephonic communications were included in the definition of electronic fund transfers in order to extend coverage over computerized pay-by-phone systems; informal non-recurring consumer-initiated transfers were excluded, however, because they are not prone to computer error or institutional abuse since they are handled on a personal basis.[93]

Consumers using cell phones to instruct their banks to transfer funds via text messages or clicks on web browsers are engaging in transactions closely akin to computerized pay-by-phone systems and far removed from informal calls to a bank teller to transfer funds to avoid an overdraft. Moreover, the cell phone message is subject to computer error as described above in Part 3(d).

Which types of cell phone communications are covered by the EFTA is an important consideration because that statute provides important protections not otherwise available. For example, the consumer's financial institution is required to disclose essential information about electronic fund transfer transactions.[94] The law caps the consumer's maximum liability for unauthorized transfers.[95] The financial institution must establish an error-resolution procedure that includes requirements for investigating consumer complaints, imposes deadlines, and mandates restoring funds to the consumer's account.[96]

The EFTA imposes restrictions on unsolicited issuance of access devices.[97] "Access device" is defined, inter alia, as "a card, code, or other means of access to a consumer's account or any combination thereof, that may be used by the consumer to initiate electronic fund transfers."[98] A cell phone that can be used to engage in activities such as transferring funds to and from consumer accounts or to pay for goods and services is a means of access to the consumer's account because it uses "code" to accomplish that access. The Official Staff Interpretation lists "tele-

---

90 *Ibid.*

91 15 USC §1693(b). See *Kashanchi*, 703 F (2d) at 940.

92 *Kashanchi*, 703 F (2d) at 941.

93 *Ibid.*

94 12 CFR §§205.4, 205.7-205.8.

95 12 CFR §205.6.

96 12 CFR §205.11.

97 12 CFR §205.5(b). Whether a cell phone is an access device also can be a factor in regard to the extent to which the consumer's financial institution must investigate an alleged error. Supp I to Part 205, §205.14(a) at para. 1.

98 12 CFR §205.2(a)(1).

phone transfer and telephone bill payment codes" as examples of access devices.[99] Therefore, a cell phone that can transfer funds may come within the definition of an "access device."

Access devices typically are plastic cards that can be used at ATMs and as debit cards at the point of purchase. It is easy to apply the restrictions on unsolicited issuance to these cards. As applied to mobile financial services, the restrictions would not limit issuance of the cell phone because consumers purchase cell phones from telecoms, not from the financial institutions where they have deposit accounts. A reasonable application of the EFTA would be to apply the restrictions on unsolicited issuance to the situation where an institution provides a financial service that the consumer can use with a cell phone.

While providing substantial protections to consumers engaging in mobile financial services, the EFTA's coverage is inadequate in the cell phone environment. As described in Part 2, mobile financial services involve many parties, and as explored in Part 3, many different types of problems may occur at many stages in the transaction. Once a problem arises, consumers can lodge a complaint under the EFTA about transfer errors with their financial institution that the bank must investigate. As explained above, the scope of the bank's investigation is quite limited.[100]

(b) Other Applicable Laws

(i) Federal law

There are major gaps in general federal regulatory agency oversight and in specific regulations related to mobile financial services in areas not covered by Reg. E or other consumer protection laws governing payments. If a financial institution is involved, it may be subject to oversight by one or more federal agencies,[101] or to no agency at all.[102] In contrast, telecoms, an essential part of delivering mobile financial services, are subject to FCC oversight.[103] One agency arguably should have oversight authority over mobile financial services regardless of the nature of the companies involved.[104]

In addition to the gaps in regulatory agency oversight, there are major gaps in federal regulations. For example, there are no FCC regulations covering mobile financial services.[105] Federal law imposes limited security and privacy require-

---

99 Supp I to Part 205, §205.2 at para. 2(a).

100 See text accompanying note 59.

101 These agencies could include the FDIC, OCC, OTS, NCUA, and the Consumer Protection Bureau. See Crowe, *supra*, n. 71 at 29.

102 PayPal is licensed by individual states. See text accompanying notes 20–24.

103 Crowe, *supra*, n. 71 at 29.

104 Crowe et al. believe "the complexity and importance . . . of the payments system do suggest a degree of ongoing involvement by the Federal Reserve." *Ibid.*, at 30.

105 *Ibid.*, at 29. Cell phone messages travel through communication channels operated by telecoms. They are common carriers subject to FCC rules. Under those rules, telecoms must provide their services on "just, reasonable and non-discriminatory terms" but have no legal responsibility to consumers if the transmission goes awry except to refund the cost of the transmission if it is not completed. Joyce, *supra*, n. 45.

ments on financial institutions but not on other participants in mobile financial services.[106] There has been no government consideration of whether current payments law is adequate to cover particular applications of mobile financial services, such as P2P transfers.[107]

(ii) State law

When consumers attempt to conduct a mobile banking transaction using cell phones and the transaction does not happen or an error occurs, the fault may be in the cell phone's hardware. In such cases, the consumer may have a cause of action against the manufacturer of the phone for breach of contract or breach of warranty under the *Uniform Commercial Code* (UCC). The consumer may face numerous obstacles, however, because the UCC permits contractual disclaimer of implied warranties[108] and contractual limitations on remedies.[109] Moreover, the consumer may have difficulty proving the amount of damages. Under the UCC, the measure of damages for breach of warranty is the difference between the value of the cell phone that the consumer purchased and the value the phone would have had if it was as warranted.[110]

The consumer's problem with mobile financial services may alternatively be due to a defect in software provided by the consumer's financial institution. The agreement between the consumer and the financial institution likely provides that the consumer has no legal right to sue the institution for defects in the software.[111] Consumers who try to sue the software provider instead of the financial institution face several barriers. For example, the UCC "applies to transactions in goods."[112] It is not clear, however, that software comes within the meaning of "goods" under Article 2 of the UCC.[113] If software is not a good under the UCC, then contract law applies, law that includes little to protect the consumer, especially since the

---

106 See *Interagency Guidelines Establishing Standards for Safeguarding Customen Information and Rescission of Year 2000 Standard for Safety and Soundness*, 66 Fed Reg 8616 (2001).

107 See text accompanying notes 6–10. See Crowe, *supra*, n. 71 at 29.

108 UCC §2-316.

109 UCC §2-719.

110 UCC §2-714(2).

111 Budnitz, *supra*, n. 25 at 643.

112 UCC §2-102.

113 "Goods" are defined as "all things . . . which are movable at the time of identification to the contract for sale." UCC §2-105(1). Various parties engaged in a long, contentious, and ultimately inconclusive battle over whether to explicitly include software in Article 2 of the UCC or enact a separate statute to deal with software. Juliet M. Moringiello, "What's Software Got To Do With It? The ALI Principles Of The Law Of Software Contracts" (2010) 84 Tul L Rev 1541 at 1541–43. The American Law Institute has issued its *Principles of the Law of Software Contracts* (2010). It "accounts for the case law and recommends best practices, without unduly hindering the law's adaptability to future developments." *Ibid.*, at 2. See generally *In re Erving Industries, Inc.*, 432 BR 354 (Bankr D Mass 2010) (WL) (electricity is a good under the UCC, while phone and telephone signals are not); *Pilgrim's Pride Corp.*, 421 BR 231 at 239 (Bankr

software provider drafts the contract.[114] Moreover, assuming software is a good under the UCC, the consumer typically obtains the software through a license rather than an outright purchase. Major aspects of UCC Article 2, such as the provisions on warranties, apply only to sales of goods, not licenses.[115] Hence, the consumer may be stuck with remedies available under contract law.

The consumer also may make a mistake such as typing the wrong amount to be transferred when conducting a transaction. Most states have enacted the *Uniform Electronic Transactions Act* (UETA).[116] Under UETA, where the consumer's message is received by the recipient's automated equipment (called an electronic agent) rather than a human being, the consumer may "avoid the effect" of the error under certain conditions.[117] For example, the consumer can avoid the error only if the agent does not provide an opportunity for the consumer to prevent or correct the error.[118] If the agent does provide such an opportunity, "the effect of any error is governed by other law."[119] Even if the other party does not provide an opportunity for the consumer to prevent or correct the error, in order to avoid the effect of the mistake, the consumer must take several required steps.[120] Moreover, UETA does not require any notice to consumers informing them of the measures they must take to avoid the error. It is doubtful consumers are aware of them.

If there is no law specifically dealing with a consumer's problem, courts will determine the parties' rights according to the agreement between them. Because consumers play no role in drafting adhesion contracts with telecom companies, they are unlikely to offer consumers meaningful redress.[121]

ND Tex 2009) (electricity, television, radio, telephone, and internet signals are services, not goods, under the UCC).

114 See generally Kem Canner, *Bad Software: What To Do When Software Fails* (Wiley Computer Publishing, 1998) at 178–241; Ellen Taylor, "Applicability of Strict Liability Warranty Theories to Service Transactions" (1996) 47 SCL Rev 231.

115 Article 2 of the UCC applies generally to "transactions in goods." UCC §2-102. Several important sections, however, apply only to transactions involving the sale of goods. See *e.g.*, UCC §2-201 (statute of frauds); §2-204 (formation of contracts); §2-313 (express warranties); §2-314 (implied warranty of merchantability); §2-315 (implied warranty of fitness for a particular purpose).

116 Forty-seven states and the District of Columbia have enacted the UETA, online: <www.nccusl.org>.

117 UETA §10(2).

118 An example is a website that provides a "confirmation screen" or sends the consumer a confirmation prior to finalization of a transaction. UETA, §10, cmt 5.

119 UETA §10, cmt 5.

120 The consumer must: promptly notify the other party of the error and tell that party that the consumer does not intend to be bound; take steps to return or destroy any benefit received; and not use or receive any benefit or value from the other party. UETA §10(2).

121 See generally Nancy J. King, "Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms For Emerging Mobile Advertising Practices", 60 Fed Comm LJ 229 at 298 (stating that some telecom subscriber agreements may include provisions waiving consumer protection laws, privacy

6. MODEL LAW

Congress should enact a law that provides consumers with vital protections when they engage in mobile financial services transactions. Ensuring a minimum level of protection will benefit consumers by allowing them to avoid costly problems and help the businesses providing this service by bolstering confidence in mobile banking, thereby making consumers more willing to use the service. It is important to subject all participating parties to the law's provisions. Otherwise, it will fail to provide the protection that consumers need. In order to reduce the regulatory burden such a law will impose on businesses, it should be as consistent as possible with current law.

The new law should incorporate the EFTA's disclosure requirements, caps on liability for unauthorized use, and required error resolution and recredit provisions. In transactions involving the consumer's deposit account at a financial institution, the law's provisions should not be limited to the financial institution. As described above,[122] many other parties are involved in providing mobile financial services and they also should be included to the extent appropriate. For example, when consumers believe an error has occurred, they should be able to complain to their financial institutions, as under the EFTA, but institutions' investigations should not be limited to their own "four walls."[123] Instead, if the consumer's financial institution determines that it did not cause the error, it should be required to contact the other parties who might be responsible and they should be required to engage in their own investigations.[124]

Also, some mobile payment transfers occur without the involvement of the consumer's financial institution, as when the consumer's phone bill is charged for the payment.[125] In those instances, consumers should be able to lodge complaints with their telecoms; the telecoms should have responsibilities comparable to those of financial institutions.

Telecoms should be prohibited from terminating cell phone service solely because of disputes over charges related to mobile financial services.

Security and privacy are major consumer concerns.[126] Yet they are also among the most difficult to deal with legislatively. Vague, general security standards are easy to evade. Precise, strict requirements hinder the development and application of new technology. Thus, the new law should include general requirements and delegate to the Consumer Financial Protection Bureau (Bureau) the task

---

rights and judicial remedies); Budnitz, *supra*, n. 25 (criticizing the lack of consumer rights in home banking contracts).

122 *Supra*, text at notes 13–27.

123 See 12 CFR §205.11(c)(4) (requiringa financial institution only to review its own records).

124 For a somewhat comparable regime, see *Fair Credit Reporting Act* requirements that a consumer reporting agency contact the furnisher of allegedly inaccurate or incomplete information and that the furnisher is required to investigate and report back to the agency, which then must report the results of the investigation to the consumer. 15 USC §1681s-2.

125 *Supra*, n. 64.

126 See test accompanying note 35.

of issuing more specific rules. As technology develops, the Bureau can modify rules far more quickly and easily than Congress can amend the statute. In addition, the Bureau's staff will gain expertise in this task over time. At a minimum, the law should require that mobile financial services meet minimum requirements for encryption, security controls, antivirus programs, and multifactor authentication. Companies providing the service should be required to maintain adequate procedures to engage in continuing monitoring and the capability to take prompt measures to correct problems such as upgrades and patches.[127] Moreover, the new law must provide consumers with effective judicial remedies for damages resulting from security breaches and privacy invasions.[128]

Consumers face severe sanctions, such as eviction, foreclosure, or repossession if a payment is not made on time due to circumstances beyond the control of any party to a transaction. Examples include natural disasters and power failures. The law should permit consumers a reasonable time to make payments when that occurs, just as banks' obligations are suspended under current law.[129]

The law should delegate to the Bureau the following tasks: establishing minimum performance standards so that companies cannot avoid liability for defective products and services through warranty restrictions and disclaimers and limitations on remedies; establishing standards for fees imposed on consumers for items such as paper proofs of payment and histories of payments; establishing timetables for how promptly companies must deliver requested documentation; and studying the need to go beyond UETA in protecting consumers from liability for unintentional mistakes, such as requiring companies to suspend implementation of a transfer request until the consumer subsequently confirms the transaction.

7. CONCLUSION

Protecting consumers using mobile financial services will be a complex endeavour because many types of businesses participate and consumers may encounter problems requiring new laws. Legislators must engage in this daunting task, however. If consumers suffer serious harm in the absence of sufficient regulation, the lack of adequate legal remedies may drive many customers away from using mobile financial services — depriving them of the attendant benefits.

---

127 See text accompanying note 46.

128 Consumers must have access to judicial forums and not be forced into arbitration through pre-dispute arbitration agreements. See generally Richard M. Alderman, "Why We Really Need The Arbitration Fairness Act" (2009) 12 J Consumer & Com L 151.

129 See *e.g.*, UCC §4-109(b); 15 USC §1693h(b). See also EFTA 15 USC §1693j (suspending consumer's obligation when there is a system malfunction, a more limited relief than proposed in the text).