Comments of

National Consumer Law Center (on behalf of its low income clients)

and

California Asset Building Coalition

California Reinvestment Coalition,

Consumer Action

Consumer Federation of America

National Association of Consumer Advocates

to the

Consumer Financial Protection Bureau

On Request for Information Regarding

Mobile Financial Services

Docket No. CFPB-2014-0012

79 Fed. Reg. 33731 (June 12, 2014)

Submitted Sept. 10, 2014

Contents

Introduction

Thank you for the opportunity to comment in response to the Consumer Financial Protection Bureau's (CFPB) request for information on mobile financial services (MFS). These comments are submitted on behalf of the National Consumer Law Center's low-income clients, California Asset Building Coalition, California Reinvestment Coalition, Consumer Action, Consumer Federation of America and the National Association of Consumer Advocates.[1]

It is difficult to summarize the wide range of issues posed by the multitude of rapidly emerging and changing financial services that can be offered through mobile devices. If there is one common thread it is this: the CFPB's vigilance is essential, because it is impossible for consumers or even relatively sophisticated consumer advocates to monitor and understand all of the issues posed by mobile financial services. The CFPB must watch the field closely, think closely about how services work, scour terms and conditions, and keep a close ear to the ground for complaints or potential problems. The CFPB must take action in whatever form appropriate – including rules, enforcement actions, supervisory guidance, consumer alerts, and conversations with industry – whenever it sees gaps in protections or new issues that are not adequately covered by existing rules.

In these comments, we will begin with question 24: core principles for protecting consumers when engaging in mobile financial services. Section II will address opportunities and concerns for underserved consumers. Section III answers some of the CFPB's specific questions and provides cross references to sections I and II.

I. Core Principles to Protect Consumers in Mobile Financial Transactions

The mobile financial services (MFS) market is developing fast and in many different directions. MFS transactions have the potential to provide convenience, access and control to many consumers. Consumers can benefit from discounts on goods and services and information about items in which they are interested. Mobile systems can also open up the electronic financial services world and internet shopping to those who do not have traditional computer access.

But the products and technology often fit imperfectly with the older framework of legal protections. Consumers who make payments on a mobile device need many of the same protections as consumers who use more traditional systems. Yet some mobile products fall in gaps in existing consumer protection statutes. It is often unclear which, if any, protections apply, and some payment systems seem designed to avoid existing credit card and debit card rails and the rules that apply to them.

[1] Organizational descriptions are provided in the Attachment.

Mobile systems also present a wide array of new issues that are not covered in existing consumer protection rules. Among others, mobile payment systems present daunting issues of security, privacy, and full and effective communication of essential information.

As regulators grapple with the blizzard of new products and technologies, it is helpful to keep in mind several principles for mobile financial systems. These general principles should apply regardless of the form that the payment takes, even if specific rules may not be the same for every type of transaction.

A. Ensure Safety

Safety is obviously critical to mobile transactions. Both consumers' funds and their information must be kept securely and be protected.

1. Safety of Funds

Funds that are held in a traditional account at a financial institution are protected by the vigilance of bank regulators and the deposit insurance provided to consumers. But some mobile payment systems involve other types of accounts that do not receive the same regulatory oversight or deposit insurance. Funds may be held in pooled accounts not in the consumer's name (which may or may not comply with the rules for pass-through insurance). Funds may be held merely on the company's books and not at an insured institution. Accounts held by companies that are not banks, like American Express and LevelUp, are not insurable by the Federal Deposit Insurance Corp. (FDIC) or the National Credit Union Administration (NCUA) and do not have any other federal protection if the company were to become insolvent.

State money transmitter laws may apply to MFS transactions, but the protection they afford varies from state to state and is incomplete.[2] These laws do not guarantee that the consumer will not lose funds that are invested in a portfolio that loses value. Consumers' access to their funds could also be frozen for a period of time while bankruptcy proceedings are sorted out. The smaller, newer companies that are entering the mobile payments market may pose even greater risks to consumers' funds.

Any mobile product that functions as a bank account substitute, accepts deposit of wages, benefits, or other income, or holds substantial amounts of consumer funds should be required to carry deposit insurance and to be under bank regulator supervision. Not every mobile transaction needs the same level of protection as a bank account. For example, consumers may take the risk of insolvency when they transfer $10 into a parking app. But some developing payment systems that hold funds usable at a wide number of merchants effectively function like bank accounts even if they are built on a

[2] The Pew Charitable Trusts, Imperfect Protection: Using Money Transmitter Laws to Insure Prepaid Cards (March 2013), available at http://www.pewstates.org/uploadedFiles/PCS_Assets/2013/Pew_prepaid_money_transmitter.pdf.

different backbone. Consumer protection and fair competition will suffer if new competitors are not under the same regulatory oversight as banks.

Consumers do not and should not be expected to understand the different ways in which funds may be held and whether those funds are protected if the provider is insolvent. Disclosure is not a substitute for substantive protection of funds.

Even for accounts covered by deposit insurance, there could be gaps or ambiguities when there are multiple players involved. If a consumer deposits cash into a mobile account at a retail store, who is responsible if the cash never makes it into the underlying bank or prepaid card account? Industry players need to be responsible for the integrity of the frameworks they develop, and the consumer should not be on the hook if something goes wrong up the complex chain of vendors.

2. Safety of Data

MFS providers must also ensure that consumers' sensitive data is safe. Exposure of account information can lead directly to unauthorized charges on consumers' accounts, and theft of their personally identifiable information can be used in identity theft.

Whether this data is stored on or accessible through a mobile device that might be lost, is accessed while the consumer is transacting, or is stored on providers' own systems, MFS providers must have an obligation to protect consumers' data. Yet, currently, there are inadequate rules to ensure that the multitude of players who are involved with mobile financial services do their parts. The CFPB should work with other regulators to develop those standards.

If multiple parties are involved in a transaction, the consumer should not be expected to sort out where a data breach occurred or who is responsible. In general, the mobile provider, such as the app provider, that interfaces directly with the consumer should be responsible to the consumer. This is not to say, of course, that other entities might not also have liability to the consumer or cannot indemnify each other. But the consumer should have a clear obvious point of contact and help.

In addition to more comprehensive rules and oversight to prevent data breaches, MFS providers should also be prohibited from selling certain particularly sensitive personal information to third parties. Selling lists of consumers who might be interested in a particular product, if consistent with the prescreening provisions of the FCRA as applicable, is one thing. But information such as Social Security numbers, bank account or credit card numbers, passwords, or security verification information (e.g., mother's maiden name) is far too dangerous in the wrong hands, and should never be sold.

Mobile apps – and internet sites generally – should never be designed to encourage consumers to provide sensitive information that they think is being used by that particular provider but instead is being provided to a lead generator or data broker that intends to sell it to the highest bidder.

For example, some consumers have provided bank account numbers and other information online to an entity that they thought was a payday lender, only to find that the lender shared the information with other companies that were potential or purported lenders. In some instances, the buyer of the information – or an entity that submitted bids on but did not even buy the information – turned out to be a criminal that used it to steal from the consumer or hound her for debts she does not owe. This type of problem is compounded if an entity shares information with multiple potential buyers.

Fine print disclosures that a MFS provider is not a lender or is not directly offering another service are insufficient to protect against this serious harm. We need much stricter rules to prohibit the sharing or sale of particular information such as Social Security numbers and account numbers that is dangerous to share.

The Graham Leach Bliley Act prohibits the sharing of bank account numbers, but that provision only applies to financial institutions and their accounts, and not to sharing by or accounts of other types of providers.[3] The GLB provision also only prohibits sharing of account numbers for purposes of marketing, and some inappropriate sharing may fall outside that restriction. In order to stop fraudulent practices and unauthorized charges, the FTC has promulgated rules under the Telemarketing Sales Act that prohibit telemarketers from using pre-acquired account information to charge consumers' credit or debit cards without their express informed consent.[4] In the case of online transactions, Congress went even further in enacting the Restore Online Shoppers Confidence Act, which prohibits the initial merchant from disclosing a consumer's billing information to any "post-transaction third-party seller" for purposes of charging the consumer's account.[5]

But mobile transactions may not be covered by these protections or they may not be sufficient to protect consumers. Broader and stronger rules are needed to prevent sharing of sensitive information of consumers who conduct mobile financial transactions.[6]

B. Promote Consumer Understanding of the Features, Terms and Cost of Mobile Transactions

In order to promote consumer choice and to ensure safe and fair transactions, consumers must understand the features, terms and costs of MFS. Understanding is more than disclosure. Disclosures must be provided in a way that they achieve their goal of effectively informing the consumer before (and after) she engages in a transaction.

Mobile devices provide both opportunities and challenges for ensuring consumer understanding. The functionality, opportunity for pop-ups and alerts, and other features

[3] 15 U.S.C. § 6802(d).
[4] 16 C.F.R. § 310.4(a)(7).
[5] 15 U.S.C. § 8402(b).
[6] Other privacy issues are discussed in section I.D, below.

of mobile devices can promote understanding and convey information when it is most relevant and likely to be read and understood.

But the small screen may make it difficult to provide detailed or complex information. Smart design can use that small screen as an advantage, to provide clear information in manageable bites, enhancing understanding. But agreement is a farce if it is based on lengthy terms and conditions that are even harder and more frustrating to read than on a desktop computer. The seductive ease of use, the "cool" factor of mobile apps, and the difficulty in going back to study an agreement in detail can lead consumers to be less aware of what they are getting into.

Fees and other costs are obviously one central aspect that consumers must understand. Cost information should be provided in simple clear charts or other formats that are designed so that consumers will actually look at them and understand them. For products that encourage repeat use, where appropriate, consumers should be alerted to the costs each time they use a product.

Some types of products may be too complex for a mobile transaction. Even the best design may not be able to overcome the limitations of a small screen and the inability to print and study terms. Similarly, mobile devices encourage fast transactions and may not be suitable for transactions that require more study and the ability to go back and easily review the descriptions of a product or its terms. Mobile transactions should not be encouraged for those types of products. The CFPB should be on the alert for unfair, deceptive or abusive practices when complex products are promoted through mobile platforms.

The use of retail agents to sell mobile products is a double-edged sword for consumer understanding. Agents can explain products to consumers and do much more to help them understand and use the products appropriately than any written disclosure can. But agents must be well trained and monitored to ensure that they do not convey misinformation, lead consumers to ignore written warnings, or deceive consumers.

Consumers also need information in a form to which they can refer in the future. They should not be forced to rely on memory for a product's terms. Consumers should be able to retain a copy of account terms and to find cost information easily in an app or on a website after the consumer has entered into a transaction or before the consumer uses it each time.

C. Establish Clear, Effective Protections and Procedures in Case of Disputes, Errors, Unauthorized Charges

1. Regulation E Protections for Disputes with the Mobile Provider

In the case of errors or disputes, consumers need clear rules that protect them, setting forth who has the responsibility to address a dispute, what procedures must be

followed, and what liability or duties the entity has if something went wrong. The rules should not differ based on the type of payment system.

Regulations E and Z set forth reasonably good consumer protections for payments and credit. The rules require disclosures about fees, give consumers a right to statements or transaction histories, limit consumers' liability for unauthorized charges, provide clear time frames and procedures for resolving disputes, and impose clear responsibility on providers to resolve disputes and, where appropriate, re-credit consumer accounts.

While bank and credit card accounts, and certain types of electronic fund transfers, are covered, not all mobile financial services are clearly with the scope of Regulation E or Z. That needs to change.

Hopefully, the CFPB's upcoming prepaid card rulemaking under Regulation E will close the most significant gap. Whether or not the term "card" is used in defining the scope of Regulation E protections, virtual accounts that underlie many mobile financial transactions should be considered to be accounts under Regulation E.[7] If the mobile account holds only a small amount of funds and is usable only to purchase goods or services at one or a limited number merchants, the gift card provisions of Regulation E may be sufficient, with limits on inactivity fees and expiration dates. Services that hold more funds, transmit funds to a broader array of persons or entities, or have more functionality should be covered fully by Regulation E.

Many mobile payment systems are designed to avoid the interchange fees charged on debit and credit card payments. Those fees can be turned into rewards and discounts for consumers. But a side effect of pushing a payment off the debit and credit card rails may be unclear Regulation E or Z protections.

With rare exceptions, mobile financial transactions should not lose Regulation E or Regulation Z protections if the payment changes form. On the one hand, if a consumer uses a credit card to transfer funds into a Starbucks virtual account, for example, it may be appropriate for Regulation Z to cover the initial transfer and for Regulation E's gift card rules to apply to subsequent use of the mobile app. On the other hand, an app that is used to transmit funds to or from a consumer's bank account should not lose Regulation E protection merely because the funds pass through a stored value account.[8]

Consumers should not be expected to rely on voluntary dispute or liability policies. Many mobile systems claim to follow Regulation E, but determining whether they do requires scrutinizing fine print for complicated legalese. Even then, consumers' rights are not as strong, clear or enforceable as they would be if they fell under Regulation E directly. Vague assurances of voluntary compliance or industry standards

[7] For example, Regulation Z's protections for "credit cards" can apply to account numbers that function as virtual cards. *See* Off'l Interpretations of Reg. Z, § 1026.2(a)(15)-2.ii.C.

[8] That should be true even if the funds stay in the stored value account for a period of time. Once prepaid cards and virtual equivalents are covered by Regulation E, coverage will hopefully not be an issue.

are simply not enough to protect consumers. Consumers need clear, uniform, enforceable legal rights.

Mobile transactions that are based on a bill-to-carrier model can be particularly dangerous and subject to abuse. Regulation E may not apply to such transactions, which may have the fewest protections.[9] Cramming has been a serious problem on phone bills.[10] While the major telecommunications providers no longer allow most third-party billing charges on landline bills, they do on mobile bills. Federal telecommunications laws include no liability limits or strong dispute rights for unauthorized charges when the phone bill is used as a payment device.[11] A few states have some anti-cramming protections, but the dispute rights are not as robust as Regulation E and do not always prevent the carrier and merchant from passing the buck back and forth if the consumer disputes a charge. Moreover, with the growing complexity of wireless bills, which are often combined with internet, cable television, and landline bills, consumers can easily overlook other charges.

Outside of de minimis, mobile-related charges such as non-recurring app purchases of a couple of dollars, mobile financial transactions should not escape error and dispute rights through bill-to-carrier systems. Regulation E is the more appropriate framework for providing consumer protections for mobile financial services.

Even if a mobile financial transaction is clearly within the scope of Regulation E, there may be some areas that need clarification. Mobiles financial services often do not provide consumers clear information about how to dispute charges or what their rights are if they question a charge.[12] Some terms and conductions are unclear or deceptive about the timing of the consumer's dispute rights, implying that a consumer has only two business days to dispute a charge. Under Regulation E, a consumer must notify the provider with two business days of learning of the loss or left of an access device in order to guarantee that her liability will be limited to $50. But even if the consumer takes

---

[9] *See* Suzanne Martindale & Gail Hillebrand, "Pay at Your Own Risk? How to Make Every Way to Pay Safe for Mobile Payments," 27 Banking & Fin. L. Rev. 265 (Mar. 15, 2011), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1787587. Bill-to-carrier transactions are nonetheless a form of credit that is potentially covered by Regulation Z, especially the Fair Credit Billing Act procedures. *See id.* at 277-79.

[10] *See* Sen. Comm. On Commerce, Science and Transportation, Office Of Oversight And Investigations, Majority Staff, "Cramming on Mobile Phone Bills: A Report on Wireless Billing Practices" (July 30, 2014), available at http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=a4dd76e2-5822-4741-b483-8a5905c7b022.

[11] For a discussion of needed protections, see Comments of Consumers Union, NCLC et al., In the Matter of Empowering Consumers to Prevent and Detect Billing for Unauthorized Charges, CG Docket No. 11-116, Consumer Information and Disclosure, CG Docket No. 09-158, Truth-in-Billing and Billing Format, CG Docket No. 98-170 (FCC Oct. 24, 2011), available at http://www.nclc.org/images/pdf/energy_utility_telecom/telecommunications/cramming-comments.pdf and Reply Comments in the same docket (FCC Dec. 5, 2011), available at http://www.nclc.org/images/pdf/energy_utility_telecom/telecommunications/cramming-reply-comments.pdf.

[12] *See, e.g.*, Federal Trade Comm'n, "What's the Deal? An FTC Study on Mobile Shopping Apps" (Aug. 1, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/08/staff-report-mobile-shopping-apps-found-disclosures-consumers-are?utm_source=govdelivery.

longer than two business days, the consumer is only liable for charges that could have been prevented with timely notice, not for charges in the initial two days.[13] Moreover, if the access device has not been lost or stolen, the consumer generally has no liability if she disputes an item within 60 days of it appearing on a statement,[14] and can dispute charges that were not preventable with timely notice even after that date. Consumers should certainly be encouraged to report missing access devices and unauthorized charges as soon as possible. But consumers should know that they can obtain relief from an initial set of unauthorized charges even if they report them late.

Another area of confusion has to do with the consumer's obligations and rights if the mobile device is stolen. Is a smartphone or tablet an "access device" within the meaning of Regulation E, or is the access device the mobile app or account number and password? It is one thing to tell a consumer that she must inform her bank within two business days of realizing that her debit card is missing. But consumers should not be expected to notify, within two business days, every app that has been loaded onto a smartphone or tablet. Consumers may have no idea of what apps they have loaded or which ones have access to financial accounts. Consumers also may not know their account numbers or how to contact the app provider.

The Regulation E procedures for lost or stolen devices are not appropriate for lost or stolen mobile devices. Mobile providers should be able to protect themselves and their consumers through passwords and other mechanisms so that the consumer is generally safe even if the mobile device is stolen. Providers should also give consumers the power to "kill" or disable access to a phone's apps remotely.[15] But consumers should still generally have an obligation to report unauthorized charges within 60 days of a statement or equivalent.

Finally, one single entity easily identifiable to the consumer should have responsibility to address and resolve any problems, including errors and disputes as required by Regulation E and, if applicable, Regulation Z. In most cases, this will be the consumer-facing entity, even if there are other parties involved. Many mobile transactions may involve multiple parties, including some that are registered money transmitters and others that are agents, service providers, or even lead generators. The consumer cannot possibly be expected to understand these complicated chains of command, and the consumer must be able to turn to the consumer-facing entity to receive and enforce consumer protection rules. That entity should not be able to disclaim responsibility by claiming that it is merely the agent of another party or through other devices in the fine print. This is not to say that entities that do not face the consumer should be free from liability: they should be jointly liable with the consumer-facing entity. But the consumer-facing entity should have full liability for the entire transaction and the responsibility to take action in response to a consumer dispute.

---

[13] *See* Reg. E, 12 C.F.R. § 1005.6(b)(2)(ii).

[14] Timelines and triggering date vary somewhat for payroll and government benefit cards.

[15] The consumer can of course turn off the entire phone. But keeping the phone on can assist in finding it if it was merely lost and not stolen. The consumer can call it and listen for the ring, and someone who finds it can call "home" or answer the phone and help get it back to its owner.

2. Chargeback Rights for Merchant Disputes

Consumers who use mobile payment systems to make purchases – as well as those who use bank account debit cards – should have chargeback rights in case of a dispute with a merchant, just as they do under Regulation Z with credit cards.[16] The likelihood of a problem with a purchase is no different whether the purchase is made with a credit card, a debit or prepaid card or a mobile payment system. Consumers need the same ability to dispute a charge if they did not get what they paid for no matter what type of payment system they use.

Consumers cannot possibly be expected to understand when they have protection and when they do not, or to examine individual provider policies for loopholes. Moreover, consumers do not expect something to go wrong, and they might be lured by a lower price in exchange for giving up protections that seem remote and technical. Disclosures are not a substitute for uniform protections.

3. Clear Protections for Loading Problems

Finally, clearer and more effective rules are need to protect consumers when they deposit or load funds.[17] Regulation E covers errors regarding transfers "to" an account, and not just from the account. But it is not clear if the entity that makes a mistake is covered if that entity does not hold the consumer's account. For example, if a retailer fails to deposit the full amount of cash to a mobile account, is the retailer covered by Regulation E? Does the mobile provider have a responsibility to investigate and fix the mistake? Someone must be identifiable to the consumer and be responsible for fixing the problem.

D. Protect Privacy

The amount of personal information that can be obtained from consumers who are conducting mobile financial transactions or other transactions on a mobile device is truly frightening. Payment card issuers, mobile payment providers, payment processors, app providers, and merchants may have access to detailed information that is not available from traditional card payments.[18]

---

[16] *See* Gail Hillebrand, "Before The Grand Rethinking: Five Things To Do Today With Payments Law And Ten Principles To Guide New Payments Products And New Payments Law," 83 Chi.-Kent L. Rev. 769 (2008).

[17] For a longer discussion of the issues involved with the load or deposit of funds, see NCLC et al, Comments to the Consumer Financial Protection Bureau on Electronic Fund Transfer (Regulation E), General Use Reloadable Prepaid Cards, Docket No. CFPB-20120019 at 63-70 (revised July 24, 2012) ("NCLC CFPB Prepaid Card Comments"), available at http://www.nclc.org/images/pdf/rulemaking/cm-prepaid-card-july2012.pdf.

[18] *See* Harley Geiger, Center for Democracy and Technology "Mobile Payments Can Expose More Consumer Data and Weaken Privacy Laws" (April 23, 2012), available at https://cdt.org/blog/mobile-payments-can-expose-more-consumer-data-and-weaken-privacy-laws/.

In many circumstances, consumers have absolutely no idea who is accessing their data, what data is shared, and how it is being used. Privacy disclosure often use vague and opaque, legalistic language, reserving broad rights to collect, use, and share consumers' information without truly informing consumers in a way they can understand or giving them options to decline sharing.[19]

To the extent that a mobile financial services provider is a "financial institution" under the Gramm Leach Bliley Act (GLBA), the protections of that law would apply. The protections of the Fair Credit Reporting Act (FCRA) affiliate sharing provisions could also apply. However, both GLBA and the FCRA affiliate sharing provisions merely provide consumers with notice about the institutions' privacy and information sharing policies, and a right to opt of sharing for the purposes of third party marketing.

The GLBA and FCRA data sharing provisions should be extended to other entities, but the CFPB also must go further and adopt additional protections governing data sharing. As discussed in section I.A.2 above, certain types of particularly sensitive personal and financial information should not be shared at all. In addition to data that could lead to identity theft, consumers also need protection for highly personal details of transactions, such as what a consumer purchased, who a consumer paid with a mobile device, what time and where the purchase was made.

To the extent that data sharing is permitted, consumers need far more control over who accesses their information and what types of data about them can be shared. Privacy should be built into the design of products. Providers should explain why information is needed. Consumers should be able to be selective – for example, to be requried to give affirmative consent, or at a minimum to be able to decline access, to location data or sharing with third parties. Using a mobile app should not be an all or nothing, take it or leave it proposition. If data sharing is not essential to the purpose of an app – like the infamous flashlight app that was secretly collecting data – consumers should be able to use the app even if they decline data sharing. And, as discussed above, personal financial information should not be sold to anyone.

Providers of mobile financial services should not be allowed to use the fine print of terms and conditions to obtain purported consumer consent to share their data. Mobile providers should be required to obtain actual consent after providing simple and clear disclosures in a form that consumers will actually read and understand. The model Regulation P disclosures under the Graham Leach Bliley Act are one example that could be adapted to the mobile setting and expanded to address particular types of data.

Consumers should have to affirmatively opt in to data sharing, be able to withdraw their consent, and not be declined services if they fail to opt in unless the product will not work at all. In some instances, consumers will be willing to share their data if it is clear to them why it is needed and they are given a choice. The consent pop-

[19] *See, e.g.*, Federal Trade Comm'n, "What's the Deal? An FTC Study on Mobile Shopping Apps" (Aug. 1, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/08/staff-report-mobile-shopping-apps-found-disclosures-consumers-are?utm_source=govdelivery.

ups that are currently being used for sharing location data with an app work relatively well. Consumers may be happy to reveal their location in order to find an ATM, and some will be willing to consent to alerts if they walk past their favorite store when it has a sale. But other consumers do not want their movements tracked.

Private information can also be combined in ways that are far beyond what consumers imagine and can set them up for a myriad of deceptive or predatory pitches (or for discrimination, as discussion in section I.E and II.B, below). Consumers who sign up for some prepaid cards already get besieged with emails pushing payday loans, and the same can happen in the mobile space.

The privacy notices required today are totally inadequate. Much stronger and more comprehensive rules are needed to adapt to the potential and peril of the mobile world.

E. Use Consumer Data Fairly

The use of data is at the center of many current mobile financial transactions and will be so increasingly in the future. Big data brokers promise to use information culled from internet searches, social media, and mobile apps to help providers make decisions as to creditworthiness of individuals, to target tailored marketing and discounts, to provide access to underserved individuals, to customize and improve the customer experience, and much more.

But the protections in place for the collection and use of data are woefully out of date. A recent report from the World Privacy Forum highlighted the fact that new types of predictive consumer scoring, fueled by thousands of pieces of information about consumers, are largely unregulated either the FCRA or the Equal Credit Opportunity Act.[20] Compliance is also spotty with one law that does provide important protections: the Fair Credit Reporting Act (FCRA).

When considering the use of data (big and small) in mobile financial transactions, policy makers and industry players alike should ask:

- Is the data or conclusion based on that data accurate?[21]
- Can the algorithms, when fed with good data, actually predict the creditworthiness or other characteristics of consumers?
- Does the use of data is assembled or evaluated by a third party for credit, employment, insurance, and other purposes comply with consumer protection laws?

[20] Pam Dixon and Robert Gellman, "The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future" (April 2, 2014), available at http://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

[21] Research by NCLC found serious inaccuracies in some uses of big data. *See* NCLC, "Big Data: A Big Disappointment For Scoring Consumer Credit Risk"(March 2014), available at http://www.nclc.org/issues/big-data.html.

- Whether or not covered by existing rules, are procedures in place to correct mistakes, to permit consumers to know how their data is being used, and to enable them to exercise choices and correct mistakes?
- Is there the potential for a discriminatory impact on racial, geographic, or other minority groups?
- Are there other inappropriate impacts on disadvantaged groups such as low income consumer?
- Does the use of data actually improve the choices for consumers?

At a minimum, providers must comply with the FCRA for any data that is assembled or evaluated by third parties and might be used for credit, insurance, employment or other FCRA purposes. In particular, data should be provided to and used by mobile providers and others only if they have a permissible purpose under the FCRA. Collectors of the data must have procedures in place to ensure that the data is accurate, to give consumers access to their "files," and to give them an effective means to correct errors.

In any credit decision, providers must ensure that use of data does not violate the Equal Credit Opportunity Act by having a disparate impact on a protected group. Racial and other impacts can arise even if race is not directly collected, such as if data is collected on geography, credit scores or income of the consumer's acquaintances, or other factors.[22]

But credit should not be the only discrimination-free zone. Providers must look out for discriminatory impacts not only when extending credit, but also when offering other products, discounts, special offers, or differential pricing.

In other areas, discrimination between different consumers may be legal but it would still be troubling. For example, as discussed below under impacts on the underserved, lower income consumers should not be offered higher prices than higher income consumers.

F. Keep Credit and Deposit Accounts Separate

Both credit and deposit/stored value accounts can be offered through mobile financial products. Some providers may offer both, either through separate accounts or a single account with different features.

Consumers may want to move money between deposit and credit accounts and to choose different ways to make a payment or purchase. Mobile devices, wallets and apps offer the promise of a central place where consumers can manage accounts of various types and can move funds around between different types of accounts.

[22] *See* Solon Barocas & Andrew D. Selbst, "Big Data's Disparate Impact" (Aug. 8, 2014), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.

While consumers may benefit from that type of fluidity, it is essential that credit features be kept separate and distinct from deposit accounts and that mobile deposit/stored value accounts be free of overdraft fees.[23] Services that function as credit should be clearly offered as credit, subject to credit rules and ability to repay. Consumers who want to borrow should affirmatively and directly access those accounts.

Indeed, the very cross-functionality and communications potential of mobile devices make old-fashioned overdraft services unnecessary. Overdraft protection was designed in an era when a paper check took a while to clear and then was received by the consumer's bank with no ability to communicate with the consumer in real time. It has expanded into a crude, flawed product that exploits consumers.

Permitting overdraft fees to permeate mobile deposit/transaction accounts would undercut the potential of mobile to expand economic inclusion and reach out to underserved consumers. Problems with overdrafts, overdraft fees and credit products are a primary reason why many consumers do not have bank accounts.

Even for consumers who are not underserved, credit should always be offered in a form where it is honest about what it is, is performed with credit checks and is based on ability to pay, complies with credit laws, and promotes careful, conscious, selective and wary use of credit. Intermixing credit and deposit type products can undermine the price transparency of pricing of both and create worse, more expensive products that lead to a cycle of debt. Lenders can also obtain a preferred position to skim pay or benefits and jeopardize legal protections for funds needed for necessities. Keeping credit and deposit products separate improves both.

G. Provide Ample, Free and Convenient Access to Account Information and Customer Service.

Consumers who engage in mobile financial transactions should have ample free methods of determining their balances, viewing transaction information, asking questions, reviewing account terms, and keeping records. Mobile apps are one way of providing this information. But they must be supplemented by other forms of communication – oral, electronic and, at times, paper.

1. Customer Service, Balances

Free, convenient access to customer service is important for mobile financial transactions. Like all consumers, mobile users need the ability to ask questions and resolve the problems that can arise. All mobile financial services should be required to provide a toll free number to address problems. This is especially important because

[23] For a longer discussion of the importance of keeping deposit accounts separate from credit accounts and eliminating overdraft fees from prepaid cards, see NCLC CFPB Prepaid Card Comments, *supra*, at 3-42; NCLC Issue Brief: Keep Prepaid Cards and Credit Separate (July 2013), available athttp://www.nclc.org/images/pdf/high_cost_small_loans/ib-prepaid-and-credit-dont-mix-july-2013.pdf.

many mobile financial transactions are provided by companies that do not have brick-and-mortar locations with access to a human being.

Some mobile financial providers do not even have a phone number, or hide the number or make it impossible to get through the automated system. Others charge for telephone customer service, both for access to an automated menu to get account information and for live calls. Sometimes, consumers must enter long strings of numbers and navigate multiple menus to get to a live agent. Some providers have thinly staffed customer service centers with long hold times.

Access to customer service online or through an app is insufficient. The problem may be with the online or app channel itself or may not be simply to address electronically. The consumer may have lost the phone or lost mobile service, or may have used up a limited plan.

Consumers also need easy, free access to their balances. If a mobile device or mobile account permits ATM access, balance inquiries should be free. Any cost charged to the provider by the ATM owner should be bundled with any fee for ATM cash withdrawals so that access to information is not impeded. The MFS provider should be encouraged or required to offer multiple free ways to find out balances, such as by text message, so that consumers can find a convenient method that works for them.

Providers have reasons for encouraging consumers to use lower cost channels for information. More consumer friendly apps and clearer information about easy methods of obtaining information can steer consumers in that direction. But providers should not be allowed to impose rigid requirements that inhibit consumers from accessing the information they need to manage and understand their accounts.

2. Disclosures, Periodic Statements, Transaction Information

Regulation E and Regulation Z both require that consumers be provided with certain up-front disclosures, changes in terms, and periodic statements that reflect transaction activity. The unclear rules that apply to some mobile services may result in consumers not receiving or seeing important information. (Issues concerning the relevance of paper communications are discussed in the next section.)

Consumers who sign up for mobile financial transactions often do not receive any record of their account terms (in paper or by email). Mobile devices encourage consumers not to read or even skim terms and conditions for key fees and other terms, and consumers who do not receive a copy of their terms may be more likely to be subject to deceptive practices.

Consumers should always be able to readily access the key terms of an agreement. At a minimum, the consumer must be offered the terms by email. Additionally the terms agreed to by the consumer should also be accessible through any mobile app as well as online. The mobile app should also offer the capacity to obtain the copy through email

(so that it can be printed or viewed on larger device). Providers should mail copies for free upon request.

For mobile financial services that are used repeatedly, consumers must have real access to periodic statements. Some apps do not even transmit periodic transaction histories electronically, expecting consumers to remember to monitor their accounts regularly through the app or online. Regularly transmitted statements or transaction histories are important for several reasons. They ensure that consumers are aware of the funds that have been taken out of their accounts and the fees they are being charged. They serve as regular reminders to check for unauthorized charges and create clear timelines for disputing a charge.

3. Form of Communications: Paper Can Still be An Important Choice

For services covered by Regulation E or Z, disclosures and periodic statements must generally be provided in "written," i.e., paper, form unless the consumer has opted in to electronic communications in accordance with the procedures of the E-Sign Act.[24] Regulation E dispenses with the periodic statement requirement (but not the written disclosure requirements) for payroll cards. Many mobile services follow the "Reg E lite" payroll card provisions and also require consumers to opt in to electronic communications for all types of information.

The principles behind the E-Sign Act are intended to ensure that 1) consumers can choose the method of communication that works for them, 2) consumers can actually access the information being provided electronically, 3) the information is in a form that the consumer can keep, and 4) that the information does not change. All of these principles are essential to ensuring that consumers are protected. The consumer choice provisions of the E-Sign Act are still relevant in a mobile world. If written communications are otherwise required, E-Sign requires consumer consent to electronic communications and requires that consumers be able to withdraw that consent.[25]

While consumers who engage in mobile transactions generally have access to some form of electronic information, for some transactions a paper option will still be important. Paper copies of account agreements or statements may be unnecessary for mobile transactions that are used only once or for small dollar amounts. But for larger transactions and more significant, ongoing relationships, paper options can ensure that consumers can carefully read or reference account terms and can see ongoing charges.

Even for consumers who are very fluent with the capabilities of their mobile devices, those devices do not work well for viewing lengthy agreements, web content that is not formatted for a mobile device, or a pdf of a statement. The snapshot of recent transactions on a mobile app does not provide the same breadth of information as a full periodic statement. Consumers may want paper statements for their records or to help

[24] 15 U.S.C. § 7001 et seq.
[25] 15 U.S.C. § 7001(c).

them have a clearer monthly view of their fees, activity or budget. Consumers may also miss important information that is provided on statements – such as a monthly summary of fees or the three-year payoff rate for a credit card – when they are encouraged only to access the last few transactions.

Consumers may not be comfortable monitoring financial accounts online, may want to keep a paper record, or may find it easier to review paper statements. Consumers with computers may not have printers, may not be able to afford the ink, or may find it more convenient to get statements in the mail than to have to remember to sign in each month, with a password, then navigate to the right location to find and print out documents.

Having a paper record can help the consumer to track down an account in the event that a mobile device is lost, the consumer has a gap in mobile service, or there has been a data breach and the account has been frozen. Consumers must have a way of identifying who they had accounts with and what their account number is if they wish to communicate with the provider through a means other than the mobile app.

Paper records can also be important to family members and others who are helping aging consumers. As consumers become less able to handle their own affairs, identifying the consumer's accounts is important. Imagine trying to help a parent who has had a stroke or developed dementia and cannot describe where they have accounts or what their passwords are.

Though mobile accounts are often viewable online as well on a mobile app, many consumers do not have internet access beyond their phones:

- According to a White House report, only 35% of consumers with less than a high school education have home broadband connections.
- Less than half of consumers (43%) with household incomes below $25,000 have access to broadband internet at home.
- Only about half of Hispanics (56%) and African Americans (55%) have the same access to broadband internet at home as white Americas.
- Only 32 percent of Americans 65 years or older expressed an interest in using the internet at home.[26]

For these consumers, access at another location, such as a library, is simply not sufficient. Many libraries do not have printer access, or they charge for it. Many have long lines to use computers with attached printers. Imagine not being able to receive mail at home, but instead being required to find a place to have the ability to open it, read it, and obtain special permission to print it or keep it (as one has to at a public library).

[26] White House Office of Science and Technology Policy, National Economic Council, "Four Years of Broadband Growth" at 8-9 (June 2013), available at http://www.whitehouse.gov/sites/default/files/broadband_report_final.pdf.

Access to digital resources may also be limited for consumers who have internet access at home or work. Many workers do not have permission or time to do personal business at work, a limitation that is likely increasing as employers find more ways to monitor employees on work computers. As for a home computer, many consumers have older, slower computers or slow internet that is cumbersome to use. Computer time may also be limited – and paper more convenient -- when the computer is shared between two spouses, other adults in the household, and children doing homework.

In addition, some consumers' only mobile connection is through a text message on a basic phone. Written communications are clearly essential for these consumers.

The E-Sign Act protects consumers by permitting electronic communications to substitute for legally required written ones only if the consumer opts in.[27] The E-Sign Act procedures ensure that the consumer can choose the method of account information that works best, that the consumer has the ability to access electronic information, and that the information is provided in a form the consumer can keep as a record. The Act ensures that a consumer who chooses electronic information is on the proper side of the digital divide, with real, meaningful and full internet access.

Yet many, and perhaps most, mobile financial products make only a token effort to comply with the E-Sign Act. Consumers are typically required to opt-in to E-Sign as a condition of the product and cannot opt out, despite the fact that the E-Sign Act is clear that it may not be used to require consumers to use electronic communications to replace written ones otherwise required.[28]

Some have suggested exempting mobile systems from the E-Sign Act. That would be a mistake. As discussed above, merely because a consumer has signed up for a mobile payment product does not mean that the mobile device is the appropriate method of providing all information about the account to all users.

It is also important to remember that the person who opens or views an account on a mobile device may not be the account holder. Family members, friends, lawyers, social workers and others might help a consumer to open an account originally or to find out information about it, but the consumer may not even have a mobile device. In that circumstance, it would be totally inappropriate for a mobile app to require consent to electronic communications and to have the consequence of turning off the consumer's access to paper statements or other communications.

---

[27] For a longer discussion of the importance of the E-Sign Act, see NCLC, Comments to the Consumer Financial Protection Bureau regarding Streamlining Inherited Regulations, Docket No. CFPB -2011-0039 at 17-23 (June 4, 2012), available at http://www.nclc.org/images/pdf/rulemaking/cm_cfpb_reply_comments_4_june_2012.pdf. For a discussion of conditions that should be placed on prepaid cards (including virtual prepaid cards on mobile devices) before granting any exemption from the Regulation E written statement requirements, see NCLC CFPB Prepaid Card Comments at 63-70.

[28] 15 U.S.C. § 7001(b)(2). Not all mobile transactions are covered by the writing requirements of Regulation E or Z. But to the extent that they are, consumers cannot be forced to accept electronic communications.

Bank accounts and credit accounts that are currently covered by full Regulation E or Z – as well as bank account substitutes that hold significant sums[29] – should continue to provide written communications unless the consumer has voluntarily opted out following E-Sign Act requirements. For other types of accounts, occasional, ad hoc requests for statements should be free and consumers should generally be able to opt in to periodic written statements for a minimal fee.

Mobile payment systems should not be a black box. Consumers should be able, and encouraged, to monitor their accounts easily in the manner that works for them.

H. Ensure Access to Funds

Many mobile services permit consumers to load funds that the consumer expects to be able to access. Yet a number of different situations can arise where the rules are unclear about consumers' ability to access and rely on funds in a mobile financial product or transaction. Both consumers and providers would benefit from more clear rules in these situations. Some of these situations could also occur in traditional bank or credit card accounts. Others pose unique issues due to use of the mobile device.

If a consumer's mobile device is lost or stolen, must the provider offer the consumer an alternative access device or interim access to funds until the mobile device can be replaced? In what time frame? Must the consumer pay, and if so how much? For some types of mobile products, like a parking app that holds only a few dollars, time may not be of the essence, and the consumer can wait until she replaces the mobile device. But if the account holds critical funds that the consumer needs today – especially if the consumer cannot afford to immediately replace the device or thinks that it may turn up – the consumer needs a way to get to those funds. Today, most such accounts would also come with a plastic card. But one can imagine a time when mobile payments become more ubiquitous and the consumer either will not have an alternative access device or will have considered it so irrelevant that it might be difficult to find.

Similar issues arise if an account is potentially compromised by a data breach. Can the provider unilaterally freeze the account? What efforts must be made to communicate with the consumer? What alternative provisions must the provider make to ensure the consumer has access to the funds? For how long may the account be frozen?

What if the provider wishes to freeze the account because it suspects fraud or suspicious activity by the user? This type of account freeze can cut both ways for consumers. Consumers who buy goods or services through PayPal, for example, are more likely to be protected against fraud if PayPal freezes the account of a merchant that is defrauding consumers. But the consumer could also be the one with the frozen account, and the provider's suspicions could be wrong. What kind of procedures must a mobile provider follow before or after freezing an account? What due process must the user be

[29] For recommendations for Regulation E modifications for prepaid cards, see NCLC CFPB Prepaid Card Comments at 60-72.

given? What time frame is appropriate for resolving a dispute? What are the criteria for resolving it?

A more straight forward issue involves access to funds deposited by check using remote deposit capture. It is unclear what time frames apply under the funds availability schedule of Regulation CC, or even if Regulation CC applies to all types of accounts.[30] In general, consumers should have the same access to checks deposited by remote deposit capture as they do for ATM deposits.

Another place where rules are unclear or lacking involves crediting and delivery of payments. If a consumer pays another person or entity through a mobile transaction, or receives a payment from someone else, the mobile provider should be required to promptly deliver and credit the payment. If a consumer uses a mobile device to pay a bill, the consumer needs to have confidence that the payment will arrive in time. Or, the consumer may be counting on the arrival of funds. The provider should not be allowed to hold the payment in limbo or delay it and collect interest, depriving both the payor and the payee of prompt access to the funds. Consumers need rules similar to those that apply to credit cards,[31] but governing both the prompt delivery and the prompt crediting of payments.

I. Prohibit Unfair Fees and Tricks

Mobile financial services systems will flourish and gain consumer support if they remain free of unfair fees and tricks or traps. Given the inherent limitations of disclosures on a mobile device, it will be especially important for the CFPB to be vigilant about unfair, deceptive or abusive practices and to enact clear rules or send clear signals through enforcement or supervisory action if they develop.

It is impossible to catalogue all of the circumstances under which a fee might be unfair or a consumer might feel that they have been lured into a trap. But a few general rules can provide some guidelines.

Mobile providers should eliminate penalty fees wherever possible or reduce them to the bare minimum. Not every fee is troubling. If a product provides a service, then the company is entitled to charge for that service. If pricing is simple enough to be understandable, consumers can decide if the value is worth the price. But nothing angers a consumer more than a penalty fee. And the potential for unfairness is immense if a provider makes a profit off of penalty fees and has an incentive to induce consumers into making mistakes.

---

[30] We have urged the CFPB and the Federal Reserve Board to update Regulation CC to address hold times for checks deposited to prepaid cards (and mobile equivalents) and via remote deposit captures. *See* Supplemental Comments of NCLC et al, 12 CFR Part 229, Regulation CC: Docket No. R-1409 (Sept. 18, 2013), available at http://www.nclc.org/images/pdf/rulemaking/comments-regulation_cc_rcc_efaa_9-18-2013.pdf.

[31] 15 U.S.C. § 1666c(a).

As discussed above, information fees should also be eliminated. Consumers should not have to pay to get information about their accounts.

Beyond specific problematic fees, the CFPB should encourage providers to simplify, simplify, simplify and keep fees minimal and reasonable. The more fees a product has, the more chances for confusion and unhappy customers. Providers should help consumers to understand the cost of a payment system by eliminating all fees that are not necessary and giving consumers the choice of a monthly fee that covers routine usage and a pay-as-you-go model with a small number of fees for discrete services.

Products should work in the manner that the consumer expects and that cost what the consumer anticipates. Profit models should not be built on the expectation that consumers will use a product and incur costs in a fashion that is not clear and obvious up front.

Nor should products be designed in a way that impedes consumers from exercising choice and control over their spending and usage. For example, a parking app should not automatically add the maximum time to a meter and require the consumer to turn it off after she is done parking. Instead, the consumer should have the choice of how much to spend up front.

Negative options and unclear add-on products also have high potential for unfairness and confusion. Consumers should always affirmatively choose additional products or services, with clear pricing. Mobile devices should not be designed so that the consumer can inadvertently sign up for more than she realizes. Negative option sales and upsells of add-on products should be banned or severely restricted in mobile transactions.

Although clear disclosures can help avoid the potential for unfairness or deception, ultimately those problems are best addressed through substantive rules and product design than disclosure. Disclosure should not insulate providers from unfair, deceptive or abusive charges if their products trick consumers or cause them unanticipated harm. Even in non-mobile transactions, disclosures have proven to be a poor substitute for substantive regulation. The difficulty of making disclosures readable and accessible in mobile transactions is an addition reason that the CFPB should use its authority to ban products that are unfair, deceptive, or abusive.

J. Facilitate Choice and Competition

Consumers should be able to easily choose when and how to engage in a mobile transaction. They should not be steered into products or transactions that do not fit their needs. Many of the principles discussed above and below are important to ensuring choice (i.e., the ability to understand a product, to choose when and how to share personal information or pay on credit, and to decide whether children can access products).

More generally, especially with the development of mobile "wallets," there is the danger that dominant players may be able to use their market position to disadvantage other players and stifle competition. Mobile wallets should be content neutral: able to contain whatever cards a consumer might put into a physical wallet (subject to vetting for security considerations), with each "card" equally accessible or the consumer choosing which card to put on top. But one can imagine a dominant player requiring a consumer to use certain products, or making the consumer jump through hoops in order to use a different card (just as PayPal does right now by adding extra steps if the consumer wishes to use a credit card instead of an electronic withdrawal from a bank account).

Exclusive or revenue sharing deals with major providers such as a college, a transit network or a government agency could also pose problems. If consumers are steered into cards they would not choose or competitors are at a disadvantage, consumer choice could be limited and consumers could be at a risk for junk fees or other problematic terms. For example, if a consumer is required to have a particular mobile wallet in order to be able to enjoy the convenience of mobile payments for a subway ride, or to use a mobile device for student laundry or books, the consumer's choice is limited and competition is stifled. Regulators need to be alert to anti-competitive forces that frustrate consumers' ability to choose and use the best payment system for them.

K. Protect Children and Parents

Many children under the age of 18 have mobile devices. Monitoring children's use of those devices is more difficult than watching them use the family desktop or even laptop. Those devices can be used to access content that is inappropriate and to make purchases that appear on parents' mobile bills or credit cards.

The Federal Trade Commission's recent settlement with Google highlights these dangers. Google was forced to refund consumers at least $19 million to settle charges that it unlawfully billed parents for children's unauthorized in-app charges.[32] The FTC order requires Google to change its mobile app billing practices to ensure that consumers' consent is obtained before charges are levied. While the order is a warning to other mobile providers, it is not the same as a clear rule that applies to everyone.

Every party involved in a mobile financial transaction – the handset manufacture, communications provider, app stores, app providers and others – must keep in mind that the user may be a minor. Mobile financial services must have appropriate protections in place to ensure that minors are not accessing inappropriate content or incurring charges without parental consent.

[32] FTC, Press Release, "Google to Refund Consumers at Least $19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children's Unauthorized In-App Charges" (Sept. 4, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it.

L. Allow Consumers to Exit Easily

Consumers will often experiment with mobile financial transactions but then ultimately abandon them or decide to close their accounts. It is all too easy to load some funds into an app and then forget that they are there while they disappear through attrition. Providers should help consumers to remember where they have funds and should make it easy to close accounts and retrieve any remaining funds. The procedures for doing so should not depend upon using the mobile device, as the consumer may have lost it or run out of funds to pay for data.

For many consumers, the small amounts of funds lost to inactivity fees may be merely a nuisance. But "small" is in the eye of the beholder, and amounts that are trivial for a middle class consumer may mean several meals for a lower income or struggling consumer.

Inactivity fees should not start accruing for several months, should be very low, and should be charged only after active attempts to alert consumers that fees will begin to accrue. Inactivity fees may be an acceptable way of closing out an abandoned account that holds only $0.37, but the goal should be to give consumers back their money, not to use inactivity fees as a hidden profit center.

Inactivity, monthly or other fees should never be charged against a zero balance account, creating a debt for an account that the consumer may assume is empty and closed. Nor should a negative balance due to such fees be offset against newly deposit funds if the consumer resumes using a product after an absence or opens up a different account later with the same provider.

Mobile providers should provide clear instructions on their apps, websites and through customer service about how consumers can retrieve remaining balances if they choose to close an account. Consumers should not be charged fees to close an account or request a check for the balance.

II. Underserved: Opportunities and Concerns

A. Underserved: Opportunities

Mobile financial transactions hold significant potential to open up opportunities for underserved consumers. Mobile devices can save money for consumers who need every penny. They enable consumers who otherwise lack internet access to shop and pay for a wider array of goods and services, often with higher quality and better prices than are available locally. Consumers can also use their devices to help them to research and compare even while shopping at brick and mortar locations. The potential for discounts at favorite merchants also helps cash-strapped consumers.

Time is also a scarce commodity for underserved consumers, who may be juggling two jobs or family obligations, sometimes without a car. The ability to pay bills

conveniently in real time without traveling to a bill payment location can be extremely useful.

With the development of remote deposit capture, mobile financial services also can provider faster, more convenient, and cheaper options for cashing or depositing checks. While consumers may be willing to pay a small fee to cash a check and gain same day access, hopefully mobile systems will develop that encourage consumers to deposit checks without paying a check-cashing fee, taking advantage of funds availability schedules and relationships with the provider that permit access to some funds even before the check has cleared.

Mobile financial services can also be an entry point to mainstream financial services, helping consumers to gain experience in electronic banking. Once consumers learn how to manage money outside of the cash economy, they may be willing and able to access other products.

The communications features of mobile devices hold great potential to help underserved consumers. Easy, real time access to account information such as balances and recent transactions can help with budgeting. Financial literacy tools can also be embedded in mobile products or offered as stand-alone options.

B. Underserved: Concerns

While the world of mobile financial transactions clearly has high potential for underserved consumers, it also poses some special concerns. These concerns may limit the potential of MFS for underserved consumers. The issues discussed below should also be kept in mind when considering the effectiveness of consumer protections and the appropriate rules for all consumers.

One overarching concern is the cost of and limitations on access to data. Mobile carriers have moved away from unlimited data plans and generally limit the amount of monthly data. Low income consumers cannot afford high data plans. Consumers on limited means may also be using prepaid plans, which tend to be more expensive for the amount of data provided and can run out, leaving the consumer with service gaps.

Even if information or functionality is potentially available on a mobile device, that does not mean that the consumer can or will access it. Consumers may be reluctant to access the information for fear of exhausting the monthly allotment. At the same time, providers of all sorts – well beyond financial services – are pushing more and more uses of mobile devices that drain scarce data allotments. Financial services providers will be competing for limited data allotments with Facebook, YouTube, music and television streaming, sports, news websites, and other sites.

The lack of robust access to data also means that underserved consumers may be less able to research potential mobile services thoroughly. They may not want to waste data on a search for reviews of a product or provider or for alternative products by competitors.

Underserved consumers may suffer periodic, or total, interruptions in their mobile access. The prepaid amount may have run out, or consumers who are struggling with bills they cannot handle may not be able to pay the mobile bill. In either event, the consumer's access to the mobile device may be cut off. The disruption may be temporary, such as for a week at the end of the month, or much longer term.

Uneven quality of data can be a special concern for rural consumers. While mobile devices could be very useful in bringing financial services to rural areas, the devices may not always work well. Access may be sporadic and data-heavy applications may not work well.

Thus, it is important to keep in mind that even if a consumer has initially accessed a transaction or account on a mobile device – and has opted in to E-Sign communications – communications may not actually get through. If the phone is shut off, the consumer may not receive emails, text messages, or phone calls, and may not be able to access an app or website.

Beyond communications, if the mobile device is the only or primary way in which the consumer accesses her account, what happens when she cannot do so any longer? Will the consumer lose access to critical funds? Consumers must always have another access method for important funds beyond the mobile device.

Another concern for underserved consumers is the greater potential for deception, misunderstanding and inadequate disclosure when all of the consumer's information comes from a tiny screen. Consumers who do not have access to desktop or laptop computers with large screens and printers have less ability to read over the details of a product or service and to understand how it works and what it costs. Mobile devices also encourage a quick skim and "I agree," and less thoughtful consideration. Consumers will have a harder time going back and remembering the terms of what they agreed to or reviewing what it is ending up costing them. While some of information can be provided by and stored in email, email is harder to search and organize on a smartphone than on a laptop or desktop, and attached pdfs are difficult to read.

As noted in section I.C.3 above, consumers who access products through mobile devices may be pushed to agree to E-Sign communications even when paper would serve them better. Consumers may be more apt to miss a bill when it comes as one of hundreds of daily emails than in the regular mail where it can be easily placed in a "to pay" pile.

On the other hand, the ability to use electronic means to deposit paper checks is a benefit, described above. But, presently, some providers impose inordinately long hold times, up to 10 days, on checks deposited through a mobile device. Struggling consumers cannot wait that long for their money and may be induced to pay a check cashing fee that they could have avoided if the hold time were reduced.

The potential for differential, more expensive pricing for underserved consumers is also worrisome. The ability of merchants to use big data to target particular consumers for offers may also mean that those offers do not come to all consumers equally, or that merchants learn who will pay more. A recent article discussed new software that uses big data to help banks set the interest rates on deposit accounts:

> Some consumers are very price sensitive and will move large amounts of money for a small increase in interest rate. Other customers, even offered a large increase, don't move their money. The software provides a predictive score of customers' price sensitivity, based on factors like past transaction activity, credit bureau score, and household income.[33]

Thus, providers may use the data gained in mobile transactions to disadvantage underserved consumers. Consumers with low credit bureau scores, and perhaps with a history of bounced checks and unpaid bills, may also be more locked into particular accounts and have less flexibility to move. Thus, they may be more susceptible to price increases.

It is a well-documented irony that prices are often higher in the low income neighborhoods where consumers can least afford to pay them. Mobile services have the potential to break down that isolation, but it may be that providers will learn who is desperate, has fewer options, or is less sophisticated about comparison shopping.

Discriminatory pricing based on race, gender or other protected classes would clearly violate the law. But disparate impacts on the pricing of higher and lower income consumers, or those with and without prime credit ratings, would also be extremely troubling.

Similarly, mobile devices offer the opportunity for predatory lending and marketing. For example, consumers who access prepaid cards through a mobile device could find themselves hit with offers for expensive payday loans. Segregated "neighborhoods" could develop in the virtual world as well as the physical, where problematic mortgage, auto loan or other financial practices are concentrated.[34]

Language access is also a potential barrier and significant concern for a number of underserved consumers. Many websites and apps are only available in English. Consumers who are not English proficient may not have access to the full potential of mobile devices. They also may receive English text alerts, emails and other forms of communication. Or, some services may be marketed in the consumer's primary language,

---

[33] Penny Crosman, "How Banks Are Using Big Data to Set Deposit Rates," American Banker (Sept. 4, 2014) (emphasis added), available at http://www.americanbanker.com/issues/179_171/how-banks-are-using-big-data-to-set-deposit-rates-1069760-1.html?utm_campaign=abla%20daily%20briefing-sep%205%202014&utm_medium=email&utm_source=newsletter&ET=americanbanker%3Ae3027968%3A677762a%3A&st=email.

[34] *See* Solon Barocas & Andrew D. Selbst, "Big Data's Disparate Impact" (Aug. 8, 2014), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.

but many of the details in the fine print will only be in English. Automated translation programs are entirely inadequate without a layer of human review.

III. Answers to Specific Questions

(1) What are some of the ways in which consumers use mobile technology to access financial services? What are some of the benefits to consumers of enhanced access via mobile?

See section II.A.

(2) How would making access via mobile differ from or improve overall access compared to only accessing financial services through an online channel?

See sections I.B, II.B.

(5)(b) Are there actions the federal government can take to enhance opportunities for providing services and products via mobile for economically vulnerable consumers at scale?

Clear, consumer protection rules that apply to all providers, make prices transparent, and eliminate incentives for unfair practices can help providers to offer products at scale to underserved consumers.

Clear, detailed rules can simplify compliance. Robust model disclosures can increase consumer confidence – driving up adoption – while reducing regulatory costs.

In addition, rules that promote transparent prices and prevent hidden, deceptive costs can make it easier for providers to charge an honest price that recoups real costs. Conversely, when some providers offer deals that prove to be too good to be true, honest providers lose business to deceptive competitors. When providers rely on back-end tricks and traps, underserved consumers also tend to lose, as they are hit with those traps disproportionately and either stay away from products altogether or end up subsidizing more well off consumers.

For example, weak rules that have encouraged an explosion of overdraft fees on bank accounts have made it extremely difficult to offer safe and fair bank accounts to underserved consumers. The fees have driven up consumer complaints and customer service costs, caused banks to lose customers, and led many consumers to become unbanked. The wrong kind of back-end competition has forced banks to offer "free checking" that is not free and made it more difficult to offer a basic bank account with a reasonable monthly fee. Over-reliance on overdraft fees also results in a totally inappropriate cross subsidy from lower to higher income consumers.

(5)(c) Does using third-party retail agents pose current and/or future risks to consumers?

Yes, use of third-party retail agents poses risks. There can be gaps in legal protections if the rules do not apply to retail agents, or agents can misrepresent how a product works. Retail agents must be properly trained and monitored in their promotion of mobile financial products, as with any financial product, to ensure compliance with applicable laws. See sections I.A.1, I.B, and question 15 below.

(10) Are there specific types of current or potential innovations that have been identified by community groups, consumer advocates, educators, or others as helpful to the underserved?

See section II.B. Remote deposit capture can be especially helpful to the underserved, provided it can be implemented in a manner that provides quick access to funds for free or a minimal fee below the cost of check cashing.

Services that enable consumers to pay bills, at low or no cost, are also helpful.

(12) Many low-income consumers use prepaid products for their daily financial transactions. What opportunities are there for low-income consumers to use these products via mobile devices?

See section II.A.

(15) Given the significant level of cash usage within the low-income population, are there mobile financial services or products that enable consumers to use their cash to pay for goods and services remotely?

PayNearMe is one service that permits consumers to shop online (or on a mobile app) but pay in cash. The service may provide benefits to unbanked consumers and those who prefer to pay in cash for various reasons. But there may be significant gaps and ambiguities in the consumer protection rules that apply.

The terms and conditions of PayNearMe state that "ALL PAYMENTS TO PAYNEARME AND THE PAYMENT LOCATION ARE FINAL AND NONREFUDABLE [sic]."[35] Neither the terms nor the FAQs include any provisions to assist consumers in the event that there is an error or dispute in the transmission of the cash from the retail store to the merchant. Although funds are transmitted electronically on the consumer's behalf, it is unclear whether the protections of Regulation E apply, either to the merchant that is accepting PayNearMe or to PayNearMe itself.

If the consumer has a dispute with the merchant, the terms give the consumer no recourse via PayNearMe. Whereas a consumer who shops in person and pays in cash can visit the merchant and obtain a refund in cash, a consumer who pays cash through PayNearMe must deal with the remote, online merchant and cannot get a cash refund.

[35] *See* http://www.paynearme.com/en/terms.

PayNearMe may also be used by children who are unable to obtain debit or credit cards to shop online. We are aware of at least one 11-year old who was able to use PayNearMe to complete an online purchase without informing his parents.

(16) Making payments for goods and services by charging them to mobile phone bills has been suggested as a way for unbanked consumers to be able to make electronic payments. What are the risks, if any, for these consumers? What are potential benefits for the unbanked and underserved?

See section I.C.1.

(17) Many subgroups of consumers face unique challenges in accessing financial products and services in ways that can improve their ability to meet their financial goals.
a. What are the barriers and challenges to using mobile to enhance access that are specific to these groups of consumers?
e. Are there additional consumer protections needed to address unique risks or barriers faced by these groups? Explain and please provide examples.

See sections I.E, I.K and II.B.

(18) Privacy and security concerns have been cited as reasons consumers do not use mobile banking and mobile financial management services. What are the specific types of privacy and security concerns? What actions should consumers take to protect their information and identity? Are there products, services or features that address these concerns? What mechanisms should exist to disable use of stolen or mislaid mobile devices that are enabled to provide financial services?

See sections I.A, I.C.1, I.D, I.E and II.B.

(19) What impediments are there to consumers opening a transaction or savings account remotely via mobile or online?

Consumers may need more personal attention to select the account that is right for them and to ensure that they understand the account's features and costs. (See question 23 below.) Virtual account opening also eliminates the opportunity for personal coaching.

Consumers may be wary of entering detailed personal information like Social Security numbers in a mobile or online device. There is also the potential for identity theft if an account is opened remotely.

Consumers should also not be coerced into consenting to electronic communications merely because they have used a mobile device to open an account. (See section I.G.2, I.G.3.)

(20) What types of customer service or technical assistance concerns are there in the context of mobile financial services? For example, should consumers always have access to a customer service telephone number and/or call center?

Yes, consumers should always have access to a customer service telephone number. See section I.G.1.

(22) What challenges and barriers exist for economically vulnerable consumers to access mobile financial services?

See sections I.G.1 and II.B.

(23) What are the concerns, if any, related to access for underserved consumers and communities if increased use of mobile financial services results in fewer bank branches?

While mobile devices can help bring needed services to underserved areas, their availability must not become an excuse for removing bank branches from those areas. Despite the spread of mobile devices, substantial numbers of consumers still do not have either mobile or internet access. In addition, as discussed in section I.G.3 above, mobile access alone is not the same as full internet access. Even for those with internet access, physical branches are still important.

Bank accounts are still primarily opened in person, and mobile account opening may be less flexible in accepting alternative forms of identification. In-person conversations when a consumer is considering a new account can ensure that the consumer has selected the right type of account and understands its terms.[36] This is especially important for consumers who are new to banking. Loss of bank branches would eliminate the potential for one-on-one financial counseling and guidance provided by tellers and bank customer service staff.

Complicated processes, like taking out a mortgage, cannot be accomplished online. Removal of bank branches could lead to a worsening of Community Reinvestment Act performance.

The physical presence of bank branches creates trust and familiarity. It helps build relationships that can help provide access to credit and other services beyond the initial account. Consumers may be less likely to use the services of an institution that is not seen in the community.

Many consumers are not comfortable depositing checks or cash at ATMs. In-person conversations can be important to resolve problems and answer questions. Some

[36] *See* Susan Burhouse, FDIC et al, "Assessing The Economic Inclusion Potential Of Mobile Financial Services" (Apr. 23, 2014), available at https://www.fdic.gov/consumers/community/mobile/Mobile-Financial-Services-and-Economic-Inclusion-04-23-2014revised.pdf.

services, like obtaining foreign currency, depositing coins, or obtaining cash in small denominations or odd amounts cannot currently be done at ATMs.

Language barriers can also be overcome in branches that are staffed with personnel who can speak to the local community. Consumers who are not 100% fluent in English will be left out if mobile services replace bank branches.

As more and more consumers transact on mobile and online, it is possible that fewer tellers may be needed, that branches can be re-tooled, and that duplicative branches are not needed in well-served areas. But there are already far too few branches in lower income areas. Mobile services should be used to make branches more efficient and expand outreach to underserved areas, not shrink financial inclusion.

(24) Various groups representing consumers have identified risks to low-income consumers when engaging in financial transactions via mobile, lack of accountability for all entities involved in the transactions, the "single point of failure" when consumers lose access to their mobile device and cannot access their financial accounts, possible move away from paper receipts or statements, and the use of data in ways that may promote products that pose risk to low-income consumers. What core principles would help ensure that underserved consumers are protected when engaging in financial transactions through mobile?

See section I.

(28) What risks does segmentation of the market through data created by mobile use present for underserved consumers? Is there a risk that data will be used to direct underserved consumers to higher-cost products and services than they would otherwise be eligible to purchase and that may pose greater risk of financial harm? Are low income consumers less likely to detect hidden fees, and, if so, does special attention need to be provided to the design of mobile payments products targeted at low income consumers? Is there any research that would help inform the data segmentation issue?

See sections I.B, I.E, and II.B.

(29) What are the types of fraud risk that low-income consumers may be exposed to when using mobile device to access financial services and products? Is the risk greater or less via mobile compared to accessing financial services online? Is the risk greater or less compared to using credit and debit cards or other means to access financial services? Please explain.

Consumers using mobile devices are exposed to the same fraud risks that exist online (and likely more), including identity theft, scams, and predatory products. Consumers may be using unsecured Wi-Fi that risks transmitting their financial information to criminals. Apps may have greater access to sensitive information stored on the device. The limited amount of information that may be conveyed on a small

screen can make it easier to be deceived and defrauded. Consumers may be less able to identify the company that is behind an app, alert or tweet and more likely to be deceived by a fraudster posing as a legitimate company. The risks are greater than with use of a plastic credit or debit cards because of the enhanced ability for fraudsters to communicate with the consumer and to use the information.

(30) Many low-income consumers use cell phones (phones without operating systems).
b. What are the challenges and barriers to communicating through "texting" for financial services and products?
c. Are there additional protections needed that may affect providers' ability to market or advertise to consumers via "text"?

See section I.G.3. The minimal information conveyed through texts poses real risks of deceptive practices and miscommunications.

(31) A significant percentage of low-income consumers mostly use their phone to go online. Are privacy concerns different depending on whether consumers access services online via a computer or via a phone or mobile application?

Yes, there are more significant privacy concerns while using a mobile phone to go online. Mobile devices store location data, and other data stored on the device is also more likely to be accessible to other sites than it is from a desktop computer.

(32) Are there unique challenges or risks associated with prepaid phones (pay-as-you-go or monthly) when using them to access financial services?

Yes, see section II.B.

(33) Are additional financial consumer protections needed to protect low-income or otherwise economically vulnerable consumers in the use of mobile financial services? Please explain.
a. Are additional protections needed to protect consumers' access to their financial accounts when they do not have access to their device because of loss, theft or non-payment of cell phone bill?

Discussed throughout, including in sections I.C.1, I.F., and II.B.

(33)b. Are there risks to consumers when third-party agents are used to facilitate transactions or provide other products via mobile?

Yes, see sections I.A.1 and I.C.

IV. Conclusion

The emerging mobile world is fascinating, exciting and frightening. New systems can hold tremendous benefits for consumers and can open up amazing new possibilities. But the complexity that occurs behind the scenes and the possibility that things will go wrong are not comprehensible to many consumers.

The mobile payments industry will benefit if consumers are assured that systems are safe, fair and honest. Voluntary measures are important, and many in industry are working hard to build in consumer protections. But voluntary measures cannot give consumers the assurances they need or protect the good industry players from the scandals that will taint the entire sector if things go wrong. There are always outliers, and problematic practices harm not only the consumers who use them but also the reputation of a developing industry.

Regulators can help both consumers and industry by leveling the playing field and establishing strong minimum standards. The industry should welcome thoughtful regulation to help bring consumer protections into the modern world to protect emerging payment systems.

Thank you for highlighting the issues posed by emerging mobile financial transactions and for this opportunity to comment.

National Consumer Law Center (on behalf of its low-income clients)
California Asset Building Coalition
California Reinvestment Coalition
Consumer Action
Consumer Federation of America
National Association of Consumer Advocates

Attachment: Organizational Descriptions

Since 1969, the nonprofit **National Consumer Law Center® (NCLC®)** has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people, including older adults, in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services, and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitive practices, help financially stressed families build and retain wealth, and advance economic fairness.

Consumer Action has been a champion of underrepresented consumers nationwide since 1971. Consumer Action focuses on financial education that empowers low to moderate income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers to advance consumer rights and promote industry-wide change. By providing financial education materials in multiple languages, a free national hotline and regular financial product surveys, Consumer Action helps consumers assert their rights in the marketplace and make financially savvy choices. More than 8,000 community and grassroots organizations benefit annually from its extensive outreach programs, training materials, and support.

The **Consumer Federation of America** is an association of nearly 300 nonprofit consumer groups that was established in 1968 to advance the consumer interest through research, advocacy and education.

The **National Association of Consumer Advocates (NACA)** is a nonprofit association of more than 1,500 consumer advocates and attorney members who represent hundreds of thousands of consumers victimized by fraudulent, abusive and predatory business practices. As an organization fully committed to promoting justice for consumers, NACA's members and their clients are actively engaged in promoting a fair and open marketplace that forcefully protects the rights of consumers, particularly those of modest means