Exhibits to Comments of
National Consumer Law Center
Center for Responsible Lending
Empire Justice Center
U.S. Public Interest Research Group
To Office of the Comptroller of the
Currency On Supporting Responsible
Innovation
(May 31, 2016)

Exhibit 1: Comments of NCLC to U.S. Dep't of the Treasury on Marketplace Lending RFI, TREAS-DO-2015-0007-0001 (Sept. 30, 2015), http://www.nclc.org/images/pdf/rulemaking/treasury-marketplace-loan-comments.pdf.

Exhibit 2: Comments of NCLC et al. to the CFPB on Request for Information Regarding Mobile Financial Services, Docket No. CFPB-2014-0012 (Sept. 10, 2014), http://www.nclc.org/images/pdf/banking_and_payment_systems/comments-cfpb-mobile-sept2014.pdf.

Exhibit 3: Comments of NCLC et al. to Federal Reserve Board On Regulatory Review under the Economic Growth and Regulatory Paperwork Reduction Act of 1996, Docket ID OP-1491, Regarding Community Reinvestment Act Availability of Funds and Collection of Checks (Regulation CC) (May 14, 2015) (EGRPRA CRA and Reg CC Comments), http://www.nclc.org/images/pdf/banking_and_payment_systems/nclc_egrpra_fed_rule_review_comments_on_cra_reg_cc05142015.pdf.

Exhibit 4: Comments of NCLC et al. to Federal Reserve Board on Regulatory Publication and Review Under the Economic Growth and Regulatory Paperwork Reduction Act of 1996, FRB Docket No. R–1510, Regulation II (March 22, 2016), http://www.nclc.org/images/pdf/rulemaking/EGRPRA-Reg-II-comments-consumer-groups.pdf.

Exhibit 1

Comments of NCLC to U.S. Dep't of the Treasury on Marketplace Lending RFI, TREAS-D O-2015-0007-0001 (Sept. 30, 2015)

NCLC®
NATIONAL CONSUMER LAW CENTER®

BOSTON HEADQUARTERS
7 Winthrop Square, Boston, MA 02110-1245
Phone: 617-542-8010 • Fax: 617-542-8028

WASHINGTON OFFICE
1001 Connecticut Avenue NW, Suite 510, Washington, DC 20036
Phone: 202-452-6252 • Fax: 202-463-9462

www.nclc.org

September 30, 2015

Submitted electronically through Regulations.gov
Laura Temel
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW, Room 1325
Washington, DC 20220

Re: Marketplace Lending RFI, TREAS-DO-2015-0007-0001

The National Consumer Law Center®, on behalf of its low income clients, appreciates the opportunity to submit these comments in response to the Department of Treasury's request for information on online marketplace lending.

The National Consumer Law Center® (NCLC®) is a nonprofit organization specializing in consumer issues on behalf of low-income people. We work with thousands of legal services, government and private attorneys and their clients, as well as community groups and organizations that represent low-income and older individuals on consumer issues. NCLC is also the author of the Consumer Credit and Sales Legal Practice Series, consisting of twenty practice treatises and annual supplements, including Consumer Credit Regulation and Fair Credit Reporting.

While the marketplace loan market is heavily focused on small business loans, some lenders make loans to consumers. Today, prime consumers are the main target, but there are signs that some marketplace lenders may be interested in moving into subprime markets. While businesses are not our constituency, we also note that many small businesses need the same protections as consumers, and yet are unprotected by consumer protection laws.

The marketplace lending market can increase competition and produce many benefits for consumers. Some of the marketplace loans on the market today tend to have relatively low rates and also transparent rates that are not obscured with high fees. Despite today's extremely low interest rate environment, many consumers are trapped in credit card debt, private student loans and other forms of credit at high rates that lenders will not refinance, even for borrowers who are keeping up with payments. Marketplace loans can offer options for these consumers and for others who seek a loan at a reasonable price below credit card rates.

Nonetheless, as others have commented, we do not believe that there is anything unique about marketplace lenders that should lead to any weaker consumer protections or regulatory exemptions. To the contrary, we fear that the market today is developing with

little oversight and some signs of problems. We therefore appreciate the Treasury Department's request for information and attention to this new market.

In these comments, we will briefly mention several issues that are not unique to marketplace lending but that could become, and in some cases already are, potential problems. In particular, we are concerned about:

- **Use of consumer data** in ways potentially inconsistent with the protections of the Fair Credit Reporting Act, privacy rights, and fair lending laws.
- Skewed origination incentives that could lead to **poor underwriting.**
- The mandatory or default **use of preauthorized electronic payments**, which can weaken consumers' control over their bank accounts, cause bank account closures, and create incentives for weaker underwriting.
- **Evasion of state laws**, including usury caps, consumer protection laws, and licensing and oversight requirements
- The use of **lead generators,** which could lead to the sale of sensitive financial information, potential for fraud, and other problems prevalent in the online payday loan market.

Use of Alternative Data and Underwriting Models

Many marketplace lenders boast about their use of alternative forms of data and new underwriting models derived from that data. Data is also used to identify "leads" and to sell those leads and sometimes the associated data to lenders.

Several potential problems can arise from the use of alternative data, including:

- Accuracy.
- Compliance with credit reporting laws.
- Disparate impacts caused by use of data associated with race or other factors.

In March 2014, we issued the report: Big Data: a Big Disappointment for Scoring Consumer Creditworthiness.[1] This report analyzed big data's promises to make better predictive algorithms that in turn can make better products available to the unbanked and underbanked. Unfortunately, our analysis concluded that big data does not live up to its big promises.

Big data proponents argue that multiplying the number of variables will expand access to borrowers with thin credit files. Expanding the number of data points also introduces the risk that inaccuracies will play a greater role in determining creditworthiness. Given these indications of accuracy problems, we conducted our own survey for our Big Data report of the information maintained on consumers by big data brokers. Even given our initial

[1] Persis Yu et al., National Consumer Law Center, "Big Data, a Big Disappointment for Scoring Consumer Creditworthiness (March 2014), http://www.nclc.org/issues/big-data.html.

skepticism, we were astonished by the scope of inaccuracies among the data brokers we investigated.

We are also concerned with big data brokers' attempts to evade the Fair Credit Reporting Act (FCRA). NCLC's analysis shows that many big data brokers could be considered consumer reporting agencies and subject to the FCRA. The FCRA imposes substantial duties on the CRA. Three of the most important functions of the FCRA deal with accuracy, disclosure, and the right to dispute items on the report. It is highly unlikely, given the size of the data set and the sources of information, that the companies that provide big data analytics and the users of that data are meeting these FCRA obligations. The Federal Trade Commission has warned companies that the presence of a disclaimer stating that reports should not be used for FCRA purposes is not sufficient to avoid FCRA coverage.[2] We hope that regulatory agencies will continue to take similar actions.

Additionally, we have serious concerns about the discriminatory impact of using big data to determine a consumer's creditworthiness. Because big data scores use undisclosed algorithms, it is impossible to analyze the algorithm for potential racial discriminatory impact. According to the companies' marketing materials, consumers are judged based upon data generated from their Internet usage, mobile applications, and social media. However, access and usage of these sources vary by race and socioeconomic status, and thus, as the FTC noted in its May 2014 Data Broker report, any algorithm based upon them may have racial disparities.

Use of social media poses special risks. For example, African Americans tend to have lower incomes and lower credit scores than white Americans. If a borrower's application or pricing is based, in part, on the creditworthiness of her social circles, that data can lead to clear discrimination against minorities compared to white borrowers with the same credit scores.

Finally, proponents argue that big data underwriting can increase access to credit and lower costs. But the marketplace loan market today is largely focused on prime borrowers, who have demonstrated creditworthiness and access to credit. These models are unproven in other contexts. To the extent that online underwriting models decrease costs, it may also be at the expense of a true ability to pay analysis that focuses on affordability, as discussed below. Our analysis of payday loan alternatives that use big data found that some of the loans are arguably "less bad" than traditional payday loans but that the products had very high costs and were not genuinely affordable alternatives.

We also share the privacy concerns discussed at greater length by the U.S. Public Interest Research Group, the Center for Digital Democracy and others with regards to the impact of targeted advertising on all Americans, most of whom have no idea that their personal data shape the offers they receive and the prices they pay online.

---

[2] FTC, Blog: "Background screening reports and the FCRA: Just saying you're not a consumer reporting agency isn't enough" (Jan. 10, 2013), https://www.ftc.gov/news-events/blogs/business-blog/2013/01/background-screening-reports-fcra-just-saying-youre-not.

Inadequate Underwriting for Ability to Pay

The cornerstone of responsible lending is underwriting for ability to pay. Ability to pay means that the borrower is able to afford to make the payments due on the loan on its original terms while meeting other expenses without reborrowing.

We are concerned about signs that the structure of the marketplace lending market may undercut incentives to properly underwrite the loans. Much like the toxic mortgages that led to the financial crisis, marketplace loans are often securitized and sold off quickly after they are originated. Lenders who make money by the origination process regardless of the ultimate outcome of the loan could be too eager to make loans without sufficient evaluation. Moody's Investor Services has warned that marketplace lenders do not have "skin in the game," a significant stake in how securitizations of their loans perform.[3] While Moody's concern is the protection for investors, inadequate underwriting can also leave consumers with debt they cannot afford to repay.[4]

These concerns are exacerbated by the unproven nature of big data underwriting, and indeed by the fact that use of big data to underwrite is not necessarily aimed at determining whether the consumer can afford the loan. Lenders may be too eager to push out loans quickly without gathering documentation of a borrower's income and expenses. One borrower "said the ease with which he could borrow from marketplace lenders — he took out four loans within 19 months in addition to his multiple credit cards — enabled him to live far beyond his means. In July, Mr. Mansour filed for bankruptcy."[5]

That experience does not appear to be unique. Indications that a growing number of marketplace loan borrowers are filing for bankruptcy is another warning sign of unaffordable lending.[6] As discussed below, other lender practices may also lead to unaffordable loans.

Compulsory electronic repayment

Marketplace lenders generally operate online and seek to have a purely electronic process. For example, the New York Times recently reported that Prosper borrowers "must allow the company direct access to their bank accounts so it can electronically deduct loan payments," and that a Lending Club loan "defaults to automatic bank withdrawals" but permits borrowers to opt out of the electronic withdrawals by calling or emailing the

---

[3] Moody's Investor Services, Press Release, "Moody's: Unique risks in marketplace versus traditional lending" (May 5, 2015), https://www.moodys.com/research/Moodys-Unique-risks-in-marketplace-versus-traditional-lending--PR_324544 ("Moody's, Unique Risks"). *See also* Michael Corkery, "Pitfalls for the Unwary Borrower Out on the Frontiers of Banking," New York Times (Sept. 13, 2015), http://www.nytimes.com/2015/09/14/business/dealbook/pitfalls-for-the-unwary-borrower-out-on-the-frontiers-of-banking.html?hp&action=click&pgtype=Homepage&module=mini-moth&region=top-stories-below&WT.nav=top-stories-below&_r=1. ("Pitfalls, NY Times").

[4] Pitfalls, NY Times, *supra* ("Marketplace companies do not suffer losses directly if the borrowers default, which may embolden them to lower their credit standards, Moody's said.").

[5] Pitfalls, NY Times, *supra.*

[6] *See* Pitfalls, NY Times, *supra.*

company, with a $7 processing fee for each paper check.[7] It is also possible that some marketplace lenders, like online payday lenders, refuse to disburse loans electronically if the consumer does not want to authorize electronic repayment.

When the borrower is a consumer, such practices may run afoul of the Electronic Fund Transfer Act, which prohibits any person from requiring repayment by preauthorized electronic fund transfer as a condition of credit.[8] Courts have found that lenders may not require the consumer to authorize electronic payment as a default method, even if the contract permits the consumer to use other forms of payment.[9] While Regulation E permits a modest discount to the interest rate or another "cost-related incentive" to pay electronically, [10] the rule does not permit practices that cross the line from an incentive to coercion and it may not permit nonmonetary incentives.

Automatic electronic repayment can be an important convenience for consumers and can help them to pay bills on time. But the EFTA ban on compulsory electronic repayments is an important protection that helps consumers to maintain control over their bank accounts. It enables consumers to prioritize their bills and prevents lenders from grabbing the consumer's paycheck before food or rent is paid.

Lenders who rely too heavily on automatic electronic repayment may do inadequate underwriting to ensure that the borrower can truly afford to repay their loans. For example, the Consumer Financial Protection Bureau recently proposed ability to pay requirements for higher cost installment loans that use preauthorized payments:

> While some installment lenders may analyze a consumer's finances in some detail, the Bureau is concerned that lenders who take a preferred means of collecting on a loan through account access or a security interest in the vehicle have little incentive to go beyond confirming that the consumer has some periodic income. The failure to determine whether a consumer can afford to repay the loans while meeting other major financial obligations and living expenses heightens the risk that the consumer will end up with an unaffordable loan.[11]

---

[7] Pitfalls, NY Times, *supra.*

[8] 15 U.S.C. § 1693k.

[9] See Fed. Trade Comm'n v. Payday Financial, L.L.C., 2013 WL 5442387 (D.S.D. Sept. 30, 2013) (lender violated compulsory use provision because loan was conditioned on agreement to repay by EFT despite right to cancel EFT payments even before first payment); Pinkett v. First Citizens Bank, 2010 WL 1910520 (N.D. Ill. May 10, 2010); O'Donovan v. CashCall, Inc., 2009 WL 1833990 (N.D. Cal. June 24, 2009) (finding violation of EFTA despite fact that borrowers could cancel authorization before the first payment); West Virginia ex rel. McGraw v. CashCall, Inc., et al., No. 08-C-1964 (W.V. Cir. Ct. Sept. 10, 2012) (same), available at www.nclc.org/unreported.

[10] Regulation E, Official Interpretations § 1005.10(e)-1.

[11] CFPB, Small Business Advisory Review Panel For Potential Rulemakings For Payday, Vehicle Title, And Similar Loans: Outline Of Proposals Under Consideration And Alternatives Considered at 21 (Mar. 26, 2015), http://files.consumerfinance.gov/f/201503_cfpb_outline-of-the-proposals-from-small-business-review-panel.pdf.

Underwriting to ensure that a lender will collect payments is not the same thing as ensuring that the consumer has the ability to make loan payments while also meeting other expenses. Indeed, "Moody's noted in a report this year about Prosper that the automatic withdrawals made it more likely that 'strapped borrowers' would pay their marketplace loans ahead of other expenses."[12]

Borrowers who set up preauthorized electronic payments can also lose control of their finances and even lose their bank accounts. This phenomenon is frequently seen in the payday loan market.[13] While NACHA rules and Regulation E give consumers the right to revoke authorization and stop preauthorized electronic payments,[14] lenders do not always comply. Borrowers may be forced to close their accounts to stop the payments. Yet once they lose a bank account, consumers may find that they are blacklisted from opening up another one.[15]

There are already reports that some marketplace lenders are making it difficult to stop electronic payments and have led to bank account closures.[16] Recurring charges may not stop even after the borrower files for bankruptcy protections.[17]One marketplace lender, OnDeck, is even reported to have continued to make electronic withdrawals from a new bank account that the borrower opened after closing the first one. While the borrower in that case was a business, which is not protected by the Electronic Fund Transfer Act, the authorization for electronic repayment is governed by NACHA rules. Chasing the borrower to a new account that the borrower did not designate for electronic repayment would not meet Regulation E and NACHA requirements for a clear and readily understandable authorization.[18]

Compliance with State Law

State laws regulate loans offered to consumers, including interest rate caps and licensing requirements. As discussed at greater length in the comments of the Center for Responsible Lending, state laws create important protections for borrowers. Financial institutions are often exempt from these laws, but the laws do apply to nonbank lenders.

While the key players in marketplace loans are not financial institutions, they often partner with those institutions in an effort to set up structures that will evade state laws.

---

[12] Pitfalls, NY Times, *supra.*
[13] Pew Charitable Trusts, Fraud and Abuse Online: Harmful Practices in Internet Payday Lending (Oct. 2014) ("In Pew's survey, one-fifth of online borrowers report that banks closed their accounts or that they did so themselves because of online payday loans."), http://www.pewtrusts.org/en/research-and-analysis/reports/2014/10/fraud-and-abuse-online-harmful-practices-in-internet-payday-lending ("Pew, Fraud and Abuse Online").
[14] *See* NCLC, Consumer Banking and Payments Law § 5.3.7 (2013 & online supp.).
[15] NCLC, Issue Brief: Introduction to Account Screening Consumer Reporting Agencies (October 2014), http://www.nclc.org/images/pdf/credit_reports/ib-cra-screening.pdf.
[16]Pitfalls, NY Times, *supra* ("Some borrowers like Mr. Mansour said they ended up closing their bank accounts because they thought it was the only way to stop the lenders from taking out the money.").
[17] *See* Pitfalls, NY Times, *supra.*
[18] NCLC, Consumer Banking and Payments Law §§ 5.3.1.1, 5.3.1.2 (2013 & online supplement).

Marketplace entities market, underwrite, and service the loan as well as market the securities and deal with investors. The financial institution may have little to do with the loan other than originating it and quickly selling it off. As in other rent-a-bank arrangements, the financial institution's role may be little more than a fig leaf to justify preemption of state laws.

Years ago, regulators put a stop to rent-a-bank arrangements used by payday lenders.[19] More recent court decisions have also rejected rent-a-bank arrangements and bolstered the role of state law.[20] But nonbank entities continue to attempt to use financial institutions to shield themselves from state lending laws. We believe that state laws offer important protections that should not be evaded.

Lead generation practices and misuse of consumer data

Finally, we are concerned about the role of lead generators in marketplace lending. Lead generators gather data about potential borrowers and sell it to the highest bidder. In the payday loan market, that data can sometimes include sensitive financial information such as Social Security numbers and bank account numbers. Indeed, many websites that appear to be lenders taking loan applications are in fact merely collecting data to sell.[21]

These lead generators cause several problems. First, if they are obtaining consumer report information, they may violate the Fair Credit Reporting Act, which prohibits using consumer reports for marketing purposes. More troubling, the buyers of that information could use sensitive information for fraudulent purposes. For example, consumers who never actually took out a payday loan have been targeted by phony debt collectors and have been subject to unauthorized charges against their bank accounts.[22] We hope that these problems do not spread to the marketplace loan market.

Conclusion

The marketplace loan market has enormous potential to offer affordable loans to consumers and businesses alike. As the market develops, it is essential that borrower protections be built in and potentially problematic practices eliminated before they become large problems.

---

[19] *See* NCLC, Consumer Credit Regulation § 9.6.1 (2012 & online supp.).
[20] Madden v. Midland Funding, LLC, No. 14-2131-cv, 2015 WL 2435657 (2d Cir. May 22, 2015); Final Order On Phase II Of Trial: The State's Usury And Lending Claims, State of West Virginia, ex rel. v. CashCall, Inc and J. Paul Reddam, Kanawha County Circuit Court, Civil Action No.: 08-C-1964, Sept. 10, 2012. http://bit.ly/16lOhAe (upholding the state's claim that CashCall was the de facto lender in violation of the state's usury limit, while finding that CashCall purchased all loans made under the arrangement from First Bank of Delaware three days later and clearly bore the economic risk of the loans).
[21] Pew, Fraud and Abuse Online, *supra*.
[22] Pew, Fraud and Abuse Online, *supra*, at 11-12; Press Release, Federal Trade Comm'n, "FTC, Illinois Attorney General Halt Chicago Area Operation Charged With Illegally Pressuring Consumers to Pay 'Phantom' Debts" (April 10, 2015), https://www.ftc.gov/news-events/press-releases/2015/04/ftc-illinois-attorney-general-halt-chicago-area-operation-charged.

Thank you for the opportunity to submit these comments and for your efforts to ensure the safety and fairness of the marketplace loan market.

Yours very truly,

Lauren Saunders
Associate Director
National Consumer Law Center (on behalf of its low income clients)

Exhibit 2

Comments of NCLC et al. to the CFPB on Request for Information Regarding Mobile Financial Services, Docket No. CFPB-2014-0012 (Sept. 10, 2014)

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 1

I. Core Principles to Protect Consumers in Mobile Financial Transactions 1

A. Ensure Safety 2

1. Safety of Funds 2

2. Safety of Data 3

B. Promote Consumer Understanding of the Features, Terms and Cost of Mobile Transactions 4

C. Establish Clear, Effective Protections and Procedures in Case of Disputes, Errors, Unauthorized Charges 5

1. Regulation E Protections for Disputes with the Mobile Provider 5

2. Chargeback Rights for Merchant Disputes 9

3. Clear Protections for Loading Problems 9

D. Protect Privacy 9

E. Use Consumer Data Fairly 11

F. Keep Credit and Deposit Accounts Separate 12

G. Provide Ample, Free and Convenient Access to Account Information and Customer Service. 13

1. Customer Service, Balances 13

2. Disclosures, Periodic Statements, Transaction Information 14

3. Form of Communications: Paper Can Still be An Important Choice 15

H. Ensure Access to Funds 18

I. Prohibit Unfair Fees and Tricks 19

J. Facilitate Choice and Competition 20

K. Protect Children and Parents 21

L. Allow Consumers to Exit Easily 22

II. Underserved: Opportunities and Concerns 22

A. Underserved: Opportunities 22

B. Underserved: Concerns 23

III. Answers to Specific Questions 26

IV. Conclusion 32

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

Exhibit 3

Comments of NCLC et al. to Federal Reserve Board On Regulatory Review under the Economic Growth and Regulatory Paperwork Reduction Act of 1996, Docket ID OP-1491, Regarding Community Reinvestment Act Availability of Funds and Collection of Checks (Regulation CC) (May 14, 2015) (EGRPRA CRA and Reg CC Comments)

Comments of
National Consumer Law Center (on behalf of its low income clients)
Center for Responsible Lending
Consumer Action
Consumer Federation of America
Consumers Union
National Association of Consumer Advocates
National Consumers League
U.S. PIRG
to
Federal Reserve Board
On Regulatory Review under the Economic Growth
and Regulatory Paperwork Reduction Act of 1996
12 C.F.R. Chapter II
Docket ID OP-1491
Regarding
Community Reinvestment Act
Availability of Funds and Collection of Checks (Regulation CC)
79 Fed. Reg. 32172 (Feb. 12, 2015)
Submitted May 14, 2015

The National Consumer Law Center, on behalf of its low income clients, Center for Responsible Lending, Consumer Action, Consumer Federation of America, Consumers Union, National Association of Consumer Advocates, National Consumers League and U.S. PIRG[1] submit these comments in response to the Federal Reserve Board's (FRB's) request for the public to identify regulations that are outdated, unnecessary, or unduly burdensome. These comments address regulations under the Community Reinvestment Act and the Availability of Funds and Collection of Checks as set forth in Regulation CC, 12 C.F.R. Part 229.[2]

The CRA needs to be modernized and strengthened to account for the changing nature of banking and to more effectively encourage investment in underserved communities. Reinvestment in struggling communities is more important today than ever. The impact of predatory lending practices, the foreclosure crisis, and the loss of wealth and assets have devastated lower and moderate income communities and communities of color. The approach to CRA examinations has also become antiquated and must be improved.

Regulation CC is outdated and needs to be updated. The FRB should (1) ban remotely created checks and remotely created payment orders for consumer transactions, (2) clarify the deposit hold times for

[1] Organizational descriptions are attached as Exhibit 1 at 8.
[2] We previously submitted similar comments on Regulation CC in response to the first EGRPRA Federal Register notice, mistakenly thinking that Regulation CC was part of that review.

check deposits to prepaid cards and by way of remote deposit capture, (3) help consumers avoid check scams. The lack of updates not only harms consumers but also imposes burdens on financial institutions.

Strengthen Implementation of the Community Reinvestment Act

The current review includes regulations under the Community Reinvestment Act (CRA). CRA examination and enforcement is outdated and needs to be modernized and strengthened to account for the changing nature of banking and to more effectively address community needs. Strong enforcement of the CRA is more important today than ever.

The CRA was passed in order to ensure that financial institutions are equally serving all neighborhoods and that all parts of this nation have access to financial services and investments necessary to thrive. While today's problems have evolved from the explicit redlining that led to passage of the CRA, neighborhoods across the country continue to suffer. In the past several years, the impact of predatory lending practices, the foreclosure crisis, and the loss of wealth and assets have devastated lower and moderate income (LMI) communities and communities of color. Many will take decades to recover. Financial institutions have a duty to be part of the solution.

Other organizations will submit more detailed comments on the CRA regulations, but we join with them in urging that the CRA be strengthened and modernized.[3] In particular, we agree that:

- **Financial institutions must invest where depositors and borrowers live.** In today's internet and mobile age, narrow assessment areas tied to branches do not reach the communities where banks take deposits and make loans through credit cards, nonbank mortgage lenders, online banks and prepaid cards.
- **Financial institutions should be assessed based on effective access to affordable services, not the mere fact that a product is offered.** Financial institutions must affirmatively market good products and design them so that they are affordable and desirable. CRA exams should look at the number of accounts actually used, opened and closed by LMI people and in LMI geographies and in communities of color.
- **Branch access remains critical.** The expansion of mobile and online banking cannot be used as an excuse to justify a lack of physical presence in underserved areas. In-person services remain important for many products and services; for seniors, lower income individuals and immigrants; for resolving problems; and for understanding the needs of a community.
- **Harmful practices should impact CRA grades.** The fact that a financial institution has regularly foreclosed unlawfully, has practices that lead consumers to incur multiple overdraft fees, or engages in other unlawful or abusive practices should be taken into account in its CRA score.
- **CRA grades should be more nuanced and tougher.** A Satisfactory or above rating is currently given to 98% of institutions. The crude measures used today do not distinguish institutions whose community reinvestment activities are barely satisfactory and need to be improved. An Outstanding grade should be more selective, demonstrating an institution that has gone above and beyond is and is a model for others.

[3] *See, e.g.,* Comments of Benjamin Dulchin, Association for Neighborhood and Housing Development, Inc., Economic Growth and Regulatory Paperwork Reduction Act of 1996 (EGRPRA), Community Panel for Boston Outreach Meeting (May 4, 2015), http://www.anhd.org/wp-content/uploads/2011/07/ANHD-EGRPRA-talking-points-to-Submit-Post.pdf.

- **Improve transparency and public input into the CRA assessment process.** The public should have full, easy access to CRA plans without the need of a public records act request. Regulatory benchmarks for an Outstanding rating should be transparent and informed by community needs. Public participation needs to be sought more affirmatively and encouraged through simple ways to comment.

The modern challenges to communities that have been left behind must be reflected in the CRA examination process. We urge you to update CRA regulations and practices to truly encourage full investment and opportunity for all communities.

Remotely Created Checks and Remotely Created Checks Should be Banned for Consumer Purposes

In December 2013, we submitted comments urging the FRB to ban the use of remotely created checks (RCCs) and remotely created payment orders (RCPOs) to obtain payments from consumers. We are summarizing those comments only briefly here and attaching them in full as Exhibit 2.[4]

RCCs[5] are used by payday lenders (storefront, internet and tribal), internet scammers, and other merchants in high-risk industries such as gambling advice, psychic readings, pyramid sales, terminated merchants, pawnbrokers, bail bondsmen, debt reduction services, and loan modifications. Our organizations have seen widespread use of RCCs to evade consumer protections, to compromise consumers' control over their bank accounts, and to facilitate unlawful, fraudulent, unfair, deceptive and abusive practices. Use of RCCs by unscrupulous merchants is likely to grow even further as regulatory and enforcement agencies work to stop abusive use of the automated clearinghouse (ACH) system.

Since the abuses we catalogued in our December 2013 comments, the evidence of scams using RCCs have continued to mount. In each of these developments announced this year, RCCs were used in scams:

- A court imposed a $10.7 million judgment against the ringleader of a scam targeting seniors.[6]
- CommerceWest Bank agreed to a $4.9 million consent judgment for facilitating over 1.3 million unauthorized RCCs for telemarketing scams, medical benefit discount card scams, and payday loan finder scams.[7]

[4] Comments of NCLC et al on improving the U.S. payment system (Dec. 13, 2013), http://www.nclc.org/images/pdf/high_cost_small_loans/payday_loans/rcc-fed-comments12132013.pdf, attached as Exhibit 2 at 10.
[5] As used in these comments, the term "RCC" generally includes both traditional RCCs and fully electronic payment instruments that are processed through the check clearing system.
[6] *See* FTC, Press Release, "Court Orders Ringleader of Scam Targeting Seniors Banned From Telemarketing" (Mar. 12, 2015), https://www.ftc.gov/news-events/press-releases/2015/03/court-orders-ringleader-scam-targeting-seniors-banned?utm_source=govdelivery.
[7] *See* U.S. Department of Justice, Press Release, "CommerceWest Bank Admits Bank Secrecy Act Violation and Reaches $4.9 Million Settlement with Justice Department" (Mar. 10, 2015), http://www.justice.gov/opa/pr/commercewest-bank-admits-bank-secrecy-act-violation-and-reaches-49-million-settlement-justice.

- Plaza Bank paid $1.2 million for letting fraudsters use RCCs to make unauthorized withdrawals from the bank accounts of tens of thousands of consumers.[8]

RCCs have outlived their usefulness. The few remaining legitimate uses can be replaced by more modern payment instruments that carry clearer consumer protections and clearer obligations for financial institutions. NACHA recently adopted rules to permit same-day ACH payments. But even without those rules, debit cards, traditional ACH payments and other payment devices now satisfy the needs that RCCs previously served.

The Federal Trade Commission (FTC) has proposed to ban the use of RCCs and RCPOs for any transactions covered under the Telemarketing Sales Rule. But the abuses do not stop there, and a complete ban for all consumer transactions would better protect consumers, simplify compliance for financial institutions, and avoid inadvertent violations of Regulation E and other regulations.

Until RCCs and RCPOs can be banned, the FRB should complete its 2011 rulemaking under Regulation CC and go farther to update the treatment of RCCs and RCPOs. As set forth in our September 2013 supplemental comments in that rulemaking,[9] in order to account for modern technology and practices, the FRB should:

- Extend RCC warranties to RCPOs;
- Clarify that RCCs and RCPOs are covered by both Regulation CC and Regulation E;[10]
- Improve monitoring of both RCCs and RCPOs;
- Treat remotely created items that bear a handwritten electronic "signature" in the same fashion as RCCs and RCPOs.

[8] U.S. Department of Justice, Press Release, "Justice Department Announces Settlement with California Bank for Knowingly Facilitating Consumer Fraud" (Mar. 12, 2015), http://www.justice.gov/opa/pr/justice-department-announces-settlement-california-bank-knowingly-facilitating-consumer-fraud.

[9] NCLC et al., Supplemental comments to the Fed and CFPB, 12 CFR Part 229, Regulation CC, Docket No. R-1409 (submitted Sept. 18, 2013), http://www.nclc.org/images/pdf/rulemaking/comments-regulation_cc_rcc_efaa_9-18-2013.pdf, attached as Exhibit 3 at 27 ("Sept. 2013 Comments").

[10] We encourage the FRB to work with the Consumer Financial Protection Bureau and the other regulators to clarify the scope of Regulation E and to ensure that supervisory guidance for Regulation E covers RCCs and RCPOs. RCCs (which, unlike RCPOs, are deposited in paper check form) have traditionally been viewed as a "transaction originated by check, draft, or similar paper instrument" outside of the scope of Regulation E. 15 U.S.C. § 1693a(7). However, RCCS are actually normally originated through an electronic transaction, such as a consumer's electronic agreement to take out an internet payday loan and to repay it through an RCC. RCCs do not originate with a paper check from the consumer. Consumers also have no way of knowing whether their bank account and routing number will be used to generate an ACH payment or an RCC. Consequently, RCCs should receive the protections of Regulation E and should not be included in the exemption for transactions that originate with a "paper instrument." To the extent that the statute currently excepts RCCs, the CFPB has the authority to make "adjustments and exceptions …. to effectuate the purposes of [the Electronic Fund Transfer Act], to prevent circumvention or evasion thereof, or to facilitate compliance therewith." 15 U.S.C. § 1693b(c).

Modernizing Regulation CC and requiring uniform treatment of RCCs and RCPOs (which are indistinguishable) would both protect consumers and clarify regulatory treatment in a way that simplifies compliance for financial institutions.

Close Loopholes in the Funds Availability Rules

Regulation CC's implementation of the Expedited Funds Availability Act (EFAA) is also outdated. The EFAA ensures that consumers have prompt access to funds that are deposited to their accounts. The FRB should update Regulation CC's funds availability schedule to account for modern technology, as discussed in greater length in our September 2013 comments.

Regulation CC is unclear as to the funds availability schedule that applies to deposits made on mobile and other devices through remote deposit capture (RDC). Deposits made through RDC should generally follow the same schedule as deposits through a proprietary ATM. There is also uncertainty around deposits to prepaid card accounts. The FRB should make clear that deposits to prepaid card accounts must be available on the same schedule as deposits to traditional deposit accounts.

We also continue to urge the FRB to complete other aspects of its 2011 proposal to amend Regulation CC to:

- Eliminate nonlocal checks and extend the local check available schedule to all checks.
- Reduce the maximum hold period for nonproprietary ATM deposits.
- Exclude declined debit card transactions from the exception that allows banks to extend hold times for consumers who have had "repeated overdrafts."[11]
- Reduce the reasonable hold extension period for non "on us" checks to two business days.

Update Reg. CC to Help Consumers Understand Check Clearing Times and Avoid Check Scams

In our September 2013 comments, we asked the FRB to do more to assist consumers in avoiding check scams such as the Nigerian check scam and the overpayment scam.[12] Fake check scams continue to be among the top scams reported each year to the National Consumers League.[13] Our organizations hear regular complaints about these scams, as well as problems with Craig's List and similar purchases with bad checks.

These scams flourish due to the lack of consumer information over when a check has truly cleared, as well as confusion over the difference between funds availability and check clearing. Consumers have

[11] The FRB should also consider whether it is appropriate for a financial institution that encourages overdrafts on ATM and debit card transactions to penalize consumers by imposing longer check hold times as a result of those overdrafts.
[12] *See* Sept. 2013 Comments at 9-10.
[13] *See* National Consumers League, Press Release, "Top ten fraud report finds rising rate of 'phantom debt' scams" (Jan. 20, 2015) (fake check scams are third most common scam reported to NCL in 2014), http://www.nclnet.org/2014_top_scams.

little way of knowing or determining when a check has actually cleared. Bank customer service representatives may only know when funds are available in the account – and themselves may not understand the difference between clearing and availability. In fact, consumers are regularly deceived when banks lead them to believe that a check has cleared when it has not.[14]

Regulation CC does not give consumers a clear point in time when it is reasonable to expect that a check has fully cleared and the consumer should be given access to the entire amount of a check. This may have been appropriate years ago when check clearing was a more cumbersome process often dependent on the mail and on whether a check was local or not. But in today's modern check clearing world, the funds availability schedule is incomplete.

It would help consumers to avoid check scams and to have appropriate access to deposited funds if the FRB updated Regulation CC to add a date on which the consumer should be given access to the full amount of the check. That schedule would be based on the number of days that are typically sufficient for a check to clear, with longer hold times for checks that typically take longer or pose more risk (such as larger checks, and checks written on foreign banks). The schedule could also have an exception for unusual circumstances that raise suspicions about the validity of the check, but the bank would be required to give the consumer notice in that situation.

We also ask that the FRB study other ways to help consumers avoid check scams, such as through notices about clearing times provided when a large check is deposited or improved teller training.

* * *

The EGRPA inquiry is phrased in a way that focuses primarily on regulations that should be eliminated to reduce burden on financial institutions. But that question is a one-sided inquiry that does not include a much more important question: are there areas where regulations are insufficient to protect consumers, small businesses and the general public? The financial crisis and other events of the last several years have made clear that the real problem in this country is the lack of adequate regulations, not too much regulation. Stronger consumer protection regulations would have saved consumers, financial institutions, and the entire economy billions of dollars, far more than compliance with the regulations could ever cost.

The consumer protection suggestions that we have provided in these comments – focused on the regulations that are currently under review -- are just a few ideas that we have for how to better protect consumers. We urge the agencies to ask the questions not posed by the EGRPRA process about additional regulations and other measures that are necessary to protect the public.

Thank you for the opportunity to submit these comments.

[14] Numerous cases involving Nigerian check scams and similar scams are listed in NCLC, Consumer Banking & Payments Law § 4.7.5 notes 381, 382 (2013 & Supp.). In some of these cases, courts permit consumers to pursue common law claims against the banks, but in most cases the bank's right of chargeback deprives the consumer of a remedy. *See id.* § 4.7.2.

Yours very truly,

National Consumer Law Center, on behalf of its low income clients
Center for Responsible Lending
Consumer Action
Consumer Federation of America
Consumers Union
National Association of Consumer Advocates
National Consumers League
U.S. PIRG

Exhibit 1: Descriptions of Commenters

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.

The **Center for Responsible Lending (CRL)** is a not-for-profit, non-partisan research and policy organization dedicated to protecting homeownership and family wealth by working to eliminate abusive financial practices. CRL is an affiliate of Self-Help, which consists of a state-chartered credit union (Self-Help Credit Union (SHCU)), a federally-chartered credit union (Self-Help Federal Credit Union (SHFCU)), and a non-profit loan fund.

Consumer Action has been a champion of underrepresented consumers nationwide since 1971. A nonprofit 501(c)3 organization, 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.

Consumers Union is the public policy and advocacy division of Consumer Reports. Consumers Union works for telecommunications reform, health reform, food and product safety, financial reform, and other consumer issues. Consumer Reports is the world's largest independent product-testing organization. Using its more than 50 labs, auto test center, and survey research center, the nonprofit rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 8 million subscribers to its magazine, website, and other publications.

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.

U.S. Public Interest Research Group (U.S. PIRG) serves as the Federation of State PIRGs, which are non-profit, non-partisan public interest advocacy organizations that take on powerful interests on behalf of their members. For years, U.S. PIRG's consumer program has designated a fair financial marketplace as a priority. Our advocacy work has focused on issues including credit and debit cards, deposit accounts, payday lending, student loans, credit report accuracy, privacy of customer information (including data breaches) and, generally, any unfair and deceptive practices.

December 13, 2013

By email to: comment@fedpaymentsimprovement.org
Chairman Ben Bernanke
Board of Governors of the Federal Reserve System
20th Street and Constitution Ave., NW
Washington DC 20551

Re: Comments on improving the U.S. payment system

Dear Chairman Bernanke,

Thank you for the opportunity to comment on ways to improve the United States' payment system. These comments are submitted by the National Consumer Law Center (on behalf of its low income clients), Consumer Federation of America, Center for Responsible Lending, Consumer Action, Consumers Union, National Association of Consumer Advocates, National Consumers League and U.S. PIRG.[1]

We urge the Federal Reserve Board (FRB) to ban the use of remotely created checks (RCCs) and remotely created payment orders (RCPOs)[2] to obtain payments from consumers. RCCs are used by payday lenders (storefront, internet and tribal), internet scammers, and other merchants in high-risk industries such as gambling advice, psychic readings, pyramid sales, terminated merchants, pawnbrokers, bail bondsmen, debt reduction services, and loan modifications.

Our organizations have seen widespread use of RCCs to evade consumer protections, to compromise consumers' control over their bank accounts, and to facilitate unlawful, fraudulent, unfair, deceptive and abusive practices. Use of RCCs by unscrupulous merchants is likely to grow even further as regulatory and enforcement agencies work to stop abusive use of the automated clearinghouse (ACH) system.

RCCs and RCPOs should be banned because:

- They are too easy to use to debit bank accounts without consumer consent;
- They lack the consumer protections available for other electronic payment methods;
- They operate through the check clearing system, which lacks the systemic controls to police fraudulent and unlawful use;
- They are widely used to facilitate fraudulent and unlawful payments and to evade consumer protections and oversight;
- They are unnecessary in light of the wide availability of modern electronic payment systems;
- Their usefulness for a handful of legitimate uses is outweighed by their risks, and legitimate users can easily move to alternatives that are less susceptible to abuse;

[1] Organizational descriptions are in the Appendix.
[2] As used in these comments, the term "RCC" generally includes both traditional RCCs and fully electronic payment instruments that are processed through the check clearing system.

- A clean, complete ban will facilitate legal compliance.

We urge that RCCs and RCPOs be banned as soon as possible. However, if the FRB concludes that implementing a full ban on RCCs will take some time, we urge the FRB to take the following interim measures while implementing a full ban:

- Ban use of an RCC as a back-up payment method to an ACH or other payment.
- Require originating depository financial institutions (ODFIs) to identify use of RCCs, monitor returns, conduct greater due diligence on their customers and their customers' customers, and terminate relationships with payment processors or merchants with high return levels or unlawful business practices. The FRB and other banking agencies should take supervisory or enforcement actions as needed to ensure that ODFIs are not processing RCCs for unlawful or abusive purposes.
- Require that RCCs be marked in a way that they can be identified.
- Identify the current uses of RCCs and how those uses can be satisfied by other payment methods.

Canada banned RCCs in 2004. The National Association of Attorneys General has called for their abolition since 2005. In the last few years, the case for abolishing RCCs has become even more compelling as automated clearinghouse transactions are now available in situations where RCCs were being used, and the evidence of abuses of RCCs has become overwhelming. The time has come to ban RCCs in consumer (and potentially all) transactions. Until a ban can be fully implemented, the FRB should crack down on illegitimate use of this payment instrument in the meantime.

I. Background

A remotely created check (RCC) is defined in Regulation CC as "a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn."[3] Any merchant who obtains a consumer's bank routing and account number can create and print an RCC with the proper software or the help of a third-party payment processor. The payee or payment processor then deposits the RCC into its bank account for collection. Once an RCC is introduced into the check clearing system, it is virtually indistinguishable from a traditional paper check.[4]

A remotely created payment order (RCPO) (termed an "electronic item not derived from checks" in FRB Docket No. R-1409) is the all-electronic version of an RCC. An RCPO never existed in printed paper form but is nonetheless deposited into and cleared through the check clearing system. A telemarketer or seller simply enters a bank account number and bank routing number into an electronic file that is transmitted to a financial institution for processing via the check clearing system.[5] Like an RCC, an RCPO is indistinguishable from a traditional paper check that has been imaged. RCPOs are also indistinguishable from RCCs. However, as discussed below,

[3] 12 C.F.R. § 229.2(fff).
[4] Federal Trade Commission, Telemarketing Sales Rule Notice of Proposed Rulemaking, 16 CFR Part 310, RIN: 3084-AA98, 78 Fed. Reg. 41200, 41205 (July 9, 2013) ("FTC TSR Proposal").
[5] FTC TSR Proposal at. 13-14.

whether an RCPO is covered by the laws that protect checks, the laws that protect electronic transactions, both of these laws, or neither is unclear.

These comments use the term "RCC" to refer to RCCs that existed in paper at some point in time and to RCPOs as ones that did not.

Payment processors and originating banks play critical roles in the misuse of RCCs. Although in theory anyone with the right software can create an RCC, telemarketers, lenders, creditors, and others usually engage the services of a third party payment processor, who creates the instrument and introduces it into the banking system. The payment processor acts as an intermediary between the payee (i.e., the telemarketer, payday lender or other merchant) and the ODFI that submits the item to the check clearing system. The telemarketer or other merchant is a customer of the payment processor.

The payment processor deposits the RCC into its bank account at its own bank, known as the originating bank or "originating depository financial institution" (ODFI). That bank in turn processes the instrument though the check clearing system to the consumer's bank, often called the "receiving depository financial institution" (RDFI). The payment processor is a customer of the ODFI. The processor's bank may be the same as or different from the bank of the telemarketer or other merchant into whose account the funds are ultimately paid. The payment processor may be an independent third party or it may be a subsidiary or affiliate of the ODFI.

II. Problems Posed by RCCs

A. RCCs Can and Have Been Easily Used to Extract Payments Without Consumer Consent

RCCs require consumer authorization. However, purported authorization may be forged, obtained in fine print, through deception, or in contracts that are themselves unlawful and void. RCCs can even be created without any consumer authorization if a payee obtains the consumer's account and routing number through identity theft or in another fashion.

The payee may obtain the consumer's bank account information in a variety of ways. The actions of online lenders, lead generators, vendors of unrelated products and services, third-party payment processors, and complicit banks have vastly expanded the risks of unsigned payments beyond the telemarketing uses of RCCs that have been the focus of attention in years past.

The scam operator may obtain the account number by telling the consumer that he has won a lottery or contest and his banking information is needed to deposit the prize.[6] Some credit card finders/brokers use their service to discover the consumer's checking account number and then

[6] *See, e.g.,* Final Judgment and Order for Permanent Injunction, Federal Trade Comm'n v. Windward Mktg., Ltd., 1997 WL 33642380 (N.D. Ga. Sept. 30, 1997).

electronically take money out of that account.[7] The same is the case with credit repair organizations[8] and companies that promise, for a fee, to find the consumer unused scholarships and grants.[9]

Other scam operators ask for a checking account number to pay for specified services, but then withdraw funds from consumers' account without authorization and without providing the promised services.[10] A fraudulent company may obtain the consumer's authorization for one payment and use it to present new drafts month after month. Alternatively, the company may use the RCC to obtain more money than was authorized.

The case of *FTC v. Direct Benefits Group, LLC* illustrates how this system works to consumers' detriment. An online payday loan lead generator using multiple websites collected loan applications including bank account and routing numbers and unfairly sold consumers extra services that they did not knowingly order. The related "benefits" companies used the bank account information entered on the loan applications to create RCPOs used to extract monthly or annual fees from consumers' checking accounts. Not surprisingly, the cash-strapped payday loan applicants did not have sufficient funds in their accounts to pay the unanticipated "benefit" fees, resulting in the RCPOs setting off a cascade of insufficient funds fees. Over a two-year period, $35,628,176 was processed from the bank accounts of 628,546 consumers by the defendants' payment processors with returns of $22 million resulting in net revenue of $9,512,172.[11]

Another recent FTC case*, FTC v. Landmark Clearing, Inc.*, also involved an internet-based scam. The bank account information of consumers who applied online for a payday loan was used by a third party to make unauthorized withdrawals using RCPOs.[12] The FTC banned Landmark Clearing, Inc. from using RCCs and RCPOs to debit consumers' bank accounts without their consent. According to the FTC's complaint, Landmark's clients generated return rates higher than 80 percent, compelling evidence that its client merchants did not have valid consumer authorizations for the debits. Landmark processed payments for Direct Benefits among other companies through First Bank of Delaware.[13]

In a case going back to 2007, the FTC sued FTN Promotions, Inc., which did business as Suntasia Inc., and several other entities for debiting consumers' bank accounts for tens of millions of dollars for fees for membership clubs that consumers did not authorize.[14] Despite consent decrees reached in 2008 and 2009, problems persist. In 2011, First Bank of Delaware terminated the

---

[7] *See* Federal Trade Comm'n v. Mandy Enters., Inc., 5 Trade Reg. Rep. (CCH) ¶ 23,181 (D. S.C. 1992).
[8] *See* Proposed Consent Decree, Federal Trade Comm'n v. Ellis, 5 Trade Reg. Rep. (CCH) ¶ 24,179 (C.D. Cal. 1996).
[9] *See* Final Order for Permanent Injunction and Settlement of Claims for Monetary Relief, Federal Trade Comm'n v. Student Aid Inc., (S.D.N.Y. Aug. 7, 1997), available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/1997/08/student-aid-inc-adel-kovaleva-and-raimma-tagie.
[10] *See* Proposed Consent Decree, Federal Trade Comm'n v. Regency Serv., Inc., 5 Trade Reg. Rep. (CCH) ¶ 24,219 (M.D. Fla. 1997).
[11] Memorandum Decision and Order, Federal Trade Comm'n v. Direct Benefits Group, L.L.C. (M.D. Fla. July 18, 2013), available at http://www.ftc.gov/os/caselist/1123114/130730directbenefitsorder.pdf
[12] *See* FTC, Press Release, "FTC Action Bans Payment Processor from Using a Novel Payment Method to Debit Accounts," (Jan. 5, 2012), available at http://www.ftc.gov/opa/2012/01/landmark.shtm (including links to pleadings in FTC v. Landmark Clearing, Inc. et al.).
[13] Press Release, "FTC Action Bans Payment Processor from Using a Novel Payment Method to Debit Accounts," Federal Trade Commission, 1/05/12, available at www.ftc.gov/opa/2012/01/landmark.shtm.
[14] Complaint for Injunctive and Other Equitable Relief, FTC v. FTN Promotions, Inc., et al., No. 8:07-cv-1279-T-30TGW (M.D. Fla. July 25, 2007), available at http://www.ftc.gov/os/caselist/0623162/.

authority of one defendant to process RCCs through the bank due to the high "unauthorized transaction" rate.[15] In May 2013, the FTC filed a motion for civil contempt against three of the defendants.[16]

In January 2013, the FTC sued Elite Debit, Inc. and scores of other companies doing business under the IWorks name for charging consumers monthly fees for services they never agreed to purchase.[17] The scheme allegedly took more than $275 million from consumers via deceptive "trial" memberships for bogus government-grant and money-making schemes. The defendants recently settled, agreeing to permanent injunctions, monetary judgments and surrender of assets.[18]

Just this month, the FTC started distributing refunds to consumers whose accounts were debited by the payment processor Automated Electronic Checking Inc. (AEC). Using RCPOs, AEC debited many consumers who had never heard of AEC or its client merchants, some of whom included online discount shopping clubs and payday loan sites. Under a settlement, AEC was banned from payment processing and required to pay a monetary judgment.[19]

Use of RCCs to unilaterally withdraw payment from consumers' bank accounts also compounds problems caused by online lenders that use a variety of tactics to evade state consumer protection and credit laws and state supervision. Some lenders claim to operate off-shore, while others claim tribal sovereign immunity as defenses to enforcement of state laws. The consumer's authorization for the payment of fees is of questionable validity if the contract itself is unlawful. But the check clearing system does not provide an effective forum for the consumer to raise and resolve these disputes or for the system to monitor lenders or processors who operate illegally.

The variations on the scams using RCCs are endless. Regardless of the particular context, once an entity obtains a consumer's information bank account information, it can process new payments at will, beyond those legally authorized or anticipated by the consumer.

B. Some lenders claim consent to use RCCs to access "any bank account"

Some lenders extract purported authorization to create an RCC to withdraw payment from any bank account a borrower is found to own, not just the bank account number provided on the

---

[15] Plaintiff Federal Trade Commission's Motion for an Order to Show Cause Why Bryon Wolf, Roy Eliasson, and Membership Services, LLC, Should Not Be Held in Civil Contempt for Violating This Court's Permanent Injunction, FTC v. Bryon Wolf, Roy Eliasson, and Membership Services, LLC, No. 8:07-1279-JSM-TGW (M.D. Fla. May 21, 2013), available at available at http://www.ftc.gov/os/caselist/0623162/..

[16] *Id.*

[17] FTC v. Jeremy Johnson, IWorks, Inc.; Cloud Nine, Inc.; CPA Upsell, Inc.; Elite Debit, Inc.; et al, First Amended Complaint, No. 10-cv-2203-RLH (D. Nev. Jan. 18, 2013), available at http://www.ftc.gov/os/caselist/1023015/130118iworkscmptexha.pdf

[18] *See* FTC, Press Release, "Two I Works Billing Scheme Marketers Agree to Settle FTC Charges" (Nov. 26, 2013), available at http://www.ftc.gov/news-events/press-releases/2013/11/two-i-works-billing-scheme-marketers-agree-settle-ftc-charges.

[19] *See* FTC, Press Release, "FTC Sends Refunds to Consumers Victimized by Automated Electronic Checking Inc.," available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2013/12/automated-electronic-checking-et-al-federal-trade.

loan application. This type of broad authorization can lead to especially severe harm when consumers' bank accounts are hijacked by online lenders.

In our view, this use of "any bank account" to extract payments via RCCs is a form of nonjudicial wage garnishment and violates the Federal Trade Commission's Credit Practices rule. We also do not believe that such blanket authorizations comply with Regulation E and NACHA authorization requirements.

Yet the "any account" language in lender privacy policies and contracts is becoming widespread. Examples include:

> *Just Military Loans*: "Collection and Use of Bank Account Information: If we extend credit to you, we will consider the bank account information provided by you as eligible for us to process payments against. In addition, as part of our information collection process, we may detect additional bank accounts under your ownership. We will consider these additional accounts to be part of the application process."[20]
>
> *Loans 'n Go*: "If we extend credit to you, we will consider the bank account information provided by you as eligible for us to process payments against. In addition, as part of our information collection process, we may detect additional bank accounts under your ownership. We will consider these additional accounts to be part of the application process and eligible for payment retrieval."[21]

Similar language is included in the privacy policies posted by online lenders American Web Loan[22] and Military Financial [23]

C. The Check Clearing System Has Inadequate Controls to Monitor Use of RCCs

Unlike the ACH system, the check clearing system has few systematic controls to monitor the use of RCCs and the potential for fraudulent use. As the FTC compellingly explained:

> Unlike payments processed or cleared through the credit card system or the ACH Network, remotely created checks are not subject to systematic monitoring for fraud. This makes them an irresistible payment method for fraudulent telemarketers….
>
> Although telemarketers engaged in fraud obviously continue to look for ways to subvert the anti-fraud mechanisms of the credit card systems and the ACH Network, the specific initial due diligence and subsequent monitoring of return activity undertaken by the operators of these systems—as well as a steady stream of law enforcement actions by the Commission and other federal and state law enforcement agencies—make it more difficult for wrongdoers to gain and, critically, to maintain access to these payment systems.

---

[20] www.justmilitaryloans.com/why-choose-just-military-loans/privacy-policy/ viewed June 14, 2013.
[21] www.loansngo.com/privacy-policy/ viewed June 14, 2013.
[22] https://www.americanwebloan.com/privacy viewed June 14, 2013.
[23] https://www.militaryfinancial.com/PrivacyPolicy.aspx viewed June 14, 2013

> Therefore, telemarketers engaged in fraud and the payment processors who assist them have increasingly turned to remotely created checks and remotely created payment orders to defraud consumers. The systemic weaknesses of the check clearing system make it much more accommodating for them than the credit card system or ACH Network. It is much easier for a merchant to open an ordinary business checking account and use it to create and deposit remotely created checks or remotely created payment orders into the check clearing system than it is to establish a credit card merchant account or qualify for ACH origination services.
>
> Moreover, based on current practices, it is impossible for banks to systematically distinguish remotely created checks from conventional checks, or to calculate their isolated rates of return. The reason for this is rooted in the structure and history of the check collection system, which is highly decentralized and originally paper-based.[24]

NACHA has long had rules requiring ODFIs to monitor returns and conduct due diligence about their ACH customers. NACHA maintains lists of banned operators and an operator watch list. In the past year, NACHA has emphasized the role of the ODFI as the gatekeeper of the ACH system, which is "responsible for the valid authorization of every ACH debit processed in its name."[25] A proposed rule would increase the responsibility of ODFIs to scrutinize merchants and payment processors who have high levels of returned payments.[26]

There are no similar rules governing RCCs. Indeed, RCCs are often used by entities who wish to escape scrutiny by the systems used to detect fraud in other payment systems. Scammers may use RCCs after NACHA has banned them from the ACH system or in order to avoid NACHA's enforcement mechanisms.[27] The networks that handle credit and debit cards also have much more robust fraud detection mechanisms than the check system.

The most recent crackdown on improper use of the ACH system makes it all the more imperative to ensure that scammers do not migrate from the one to the other. Efforts to root out fraud in the system are welcome, but one result may be that unscrupulous parties shift their payments to RCCs, where there is far less monitoring.

D. RCCs Have Inferior Consumer Protections

The use of RCCs is popular for lenders and other businesses because the consumer protections available are weak or poorly enforced. RCCs lack the stronger consumer protections that apply to electronic fund transfers, debit cards and credit cards.[28] Compared to the protections

---

[24] FTC TSR Proposal, 78 Fed. Reg. at 41205-06 (footnotes omitted).
[25] NACHA, ACH Operations Bulletin #2-2013, "High-Risk Originators and Questionable Debit Activity at 2 (March 14, 2013) ("NACHA High Risk Originator Bulletin"), *available at* https://www.nacha.org/OpsBulletins.
[26] NACHA, Request for Comment, "NACHA Invites Comments on Proposed Rules toImprove ACH Network Quality" (Nov. 11, 2013), available at https://www.nacha.org/page/request-comment.
[27] *See* NACHA High-Risk Originator Bulletin at 1 n.2. NACHA maintains both a Terminated Originator List, https://www.nacha.org/Terminated_Originator_Database, and an Originator Watch List, https://www.nacha.org/originator-watch-list.
[28] *See* discussion surrounding Notes 32 and 33. Federal Trade Commission, Notice of Proposed Rulemaking, 16 CFR Part 310, Telemarketing Sales Rule. Available at http://www.ftc.gov/os/2013/05/130521telemarketingsalesrulefrn.pdf.

of Regulations E and Z, the UCC does not provide the same caps on liability for unauthorized charges, a right of re-credit, or clear error resolution procedures.

The sparse federal regulation of RCCs does not protect consumers. The warranties between banks provided by Regulation CC only apply to financial institutions and do not directly create rights for checking account customers.[29] As the FTC noted, "consumers victimized by telemarketing schemes that deposit unauthorized RCCs are forced to expend a significant amount of time, effort and money to resolve disputes with their banks over unauthorized withdrawals from their accounts."[30]

RCCs also lack the protections that apply under the EFTA when lenders seek preauthorization for electronic repayment. The EFTA bans lenders from conditioning the extension of credit on a requirement to make payments electronically. While consumers may voluntarily agree to make periodic payments via ACH, lenders cannot require electronic access to bank accounts. The EFTA also gives consumers the right to stop payment of preauthorized electronic fund transfers (EFTs) including future payments from the same merchant. None of these protections, other than the right to stop payment, apply to RCCs.

Consumers cannot protect themselves from the dangers of RCCs. RCCs use the same information -- bank account and routing number – as an ACH payment. Some ACH payment systems even call themselves "echecks." The complex differences between an ACH and an RCC – both of which are exotic instruments foreign to most consumers – are simply beyond the comprehension of the average consumer. Moreover, once he turns over his bank account information, the consumer has no way of knowing how the payment will be processed.

E. RCCs Even Evade UCC Stop Payment Rights

RCCs can also be used by scammers to exploit weaknesses in the check system that make it difficult for the consumer to make an effective stop payment order. While RCCs are covered by state Uniform Commercial Code (UCC) provisions, these laws are not very useful when a consumer needs to stop payment. The consumer may not know the RCC is coming, may not know how to identify it, or may find that the scammer can evade the order.

Although consumers have the right to stop payment of a check, consumers may lack the information to identify an RCC in a manner that the bank will recognize or honor. Automated stop payment systems typically rely on a check number and check amount to identify a payment that has been stopped. But the consumer does not have, or will not know, a check number for an RCC.

The consumer may not even know that an RCC has been created. RCCs are often used for payments that consumers do not expect or anticipate, such as collection of late fees, payday loan rollovers, add-on products, and other payments where consumer consent is questionable. Online lenders typically use RCC authorization as a secondary payment method, to be used if an ACH is returned or a consumer revokes authorization for an electronic fund transfer. Because a consumer

[29] FFIED, "Retail Payment Systems Booklet-February 2010, Note 41 at 9. http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_RetailPaymentSystems.pdf

[30] Federal Trade Commission, Notice of Proposed Rulemaking, 16 CFR Part 310, Telemarketing Sales Rule, p. 19.. Available at http://www.ftc.gov/os/2013/05/130521telemarketingsalesrulefrn.pdf.

did not choose to pay the loan via an unsigned paper check, she has no idea if or when a lender will create an unsigned check to send through the check clearing system. As a result, consumers would have to be clairvoyant to know when and how to stop payment on an RCC at their bank.

Even if the consumer knows the amount of an RCC, scammers also frequently manipulate the amount of the check – adding or subtracting a few cents or breaking up a transaction into more than one check – in order to evade stop payment orders. Here is one story that was posted on the internet site of a nonprofit organization about the consumer took out a payday loan:

> After we received [the payday loan], 2 weeks later the first payment was withdrawn automatically from our checking account. Within two and a half months the loan was repaid plus interest, but the payday loan company continued to withdraw money from our checking account.
> They wouldn't stop taking payments on their end even after I asked them to stop. So I had to do a stop payment at my bank. However even after I did the stop payment, they withdrew money from my checking account by making the amount they were withdrawing 2 cents less than the stop payment amount which was a red flag there.
>
> So on a $300 loan; we have over paid nearly $250 in interest. What a rip-off![31]

Such alterations may violate the UCC and make the check not properly payable. But these machinations are nonetheless effective. Consumers are powerless to protect themselves: they do not know the intricacies of check and payments law, and cannot afford to go without their income while they try to contest charges.

E. RCCs are Routinely Used To Evade EFTA Rights and Regulator Scrutiny and to Extract Payments Rejected by the ACH System

Entities that process RCCs often promote their use to merchants who are looking for ways to evade consumer protections and regulatory scrutiny. RCCs are also used by merchants who have been banned from the ACH system or card networks and to re-process ACH payments that have been rejected.

Some payment processors promote their RCC services for the very purpose of avoiding the legal protections that apply to other payment methods:

> *ACH Check Solutions* lists as a benefit of accepting echecks that "ACH Rules do not apply – Echeck Services are not governed by NACHA!"[32] The businesses accepted by ACH Check Solutions include gambling advice, psychic readings, pyramid sales, terminated merchants, pawnbrokers, bail bondsmen, debt reduction, senior activities and loan modification programs.[33]

---

[31] http://www.stoppaydaypredators.org/Personal%20victim%20stories.html.
[32] www.echeck-merchantaccount.com/ viewed 7/23/13
[33] www.echeck-merchantaccount.com/eChecklist.html , viewed 7/23/13

CheckWriter states that a benefit of using its check drafting software program is that it is not covered by "strict ACH regulations published by N.A.C.H.A."[34]

A blog posting by the CEO of *MyECheck* claims that NACHA regulations make it too easy for consumers to reverse payments with ACH e-checks and states that current payment systems "go too far with consumer protection."[35]

Internet payday lenders and lead generators who accept ACH payments use RCCs as a back-up payment method to defeat the consumer's payment options and to exert control over the consumer's bank account.

Use of an RCC is typically not the consumer's affirmative payment choice but is buried in the fine print of multi-page loan agreements. RCCs are often a back-up payment method used if the consumer exercises her right to withdraw authorization for or to stop payment of an electronic funds transfer. For example, loan agreements contain the following language:

Great Plains Lending: **"REMOTELY CREATED CHECK AUTHORIZATION:** If you terminate any previous ACH Debit Authorization you provided to us or we do not receive a payment by the Payment Due Date, you authorize us and our agents, successors and assigns to create and submit remotely created checks for payment to us in the amount of each payment owing under this Agreement, including any returned payment charges or other amounts owing to us upon acceleration of this Loan as a result of your Default. Your typed signature below shall constitute your authorization to us to authenticate remotely created checks, which are also known as demand drafts, telechecks, preauthorized drafts, or paper drafts." [36]

Zip Cash LLC: **The "Promise to Pay"** section of a ZipCash contract includes the disclosure that the borrower may revoke authorization to electronically access the bank account as provided by the Electronic Fund Transfer Act. However, revoking that authorization will not stop the lender from unilaterally withdrawing funds from the borrower's bank account. The contract authorizes creation of a remotely created check which cannot be terminated. "While you may revoke the authorization to effect ACH debit entries at any time up to 3 business days prior to the due date, you may not revoke the authorization to prepare and submit checks on your behalf until such time as the loan is paid in full."[37]

La Posta Tribal Lending Enterprises: **REMOTELY CREATED CHECK AUTHORIZATION**: "If you terminate any previous ACH Debit Authorization you provided to us or we do not receive a payment by the Payment Due Date, you authorize us

[34] http://checkwriter.net/check-draft.htm viewed 7/23/13. Other benefits listed include: "Any business, including telemarketing, credit repair and others can use. No merchant account is required to create check drafts."
[35] Ed Starrs, CEO, MyECheck, blog posting, June 20, 2012, www.myecheck.com/2012/06/20/merchants-are-at-a-disadvantage-in-most-e-commerce-transactions-due-to-deficiencies-in-payment-systems/ accessed 7/23/13. Website domain registered to eFinancial Corp in California.
[36] www.GreatPlainsLending.com Consumer Loan Agreement, dated 8/24/12, on file with CFA. The same language is used in contracts for installment loans from Plain Green, LLC. www.plaingreenloans.com Consumer Loan Agreement, dated 1/27/13, on file with CFA.
[37] Loan Supplement (ZipCash LLC) Form #2B, on file with CFA.

and our agents, successors and assigns to create and submit remotely created checks for payment to us in the amount of each payment owing under this Agreement, including any returned payment charges or other amounts owing to us upon acceleration of this Loan as a result of your Default. Your typed signature below shall constitute your authorization to us to authenticate remotely created checks, which are also known as demand drafts, telechecks, preauthorized drafts, or paper drafts. If you believe we charged your Bank Account in a manner not contemplated by this authorization, then please contact us. You authorize us to vary the amount of any preauthorized payment by remotely created check as needed to repay installments and any other payments due under this Agreement."[38]

eCash: **"Promise to Pay**:...You may revoke this (ACH) authorization at any time up to 3 days prior to the date any payment becomes due on this Note. However, if you timely revoke this authorization, you authorize us to prepare and submit ACH debit(s) and/or a check(s) drawn on your Account to repay your loan when it comes due. If there are insufficient funds on deposit in your Account to effect the ACH debit entry or to pay the check or otherwise cover the loan payment on the due date, you promise to pay us all sums you owe by submitting your credit card information or mailing a Money Order payment to: eCash. We do not accept personal checks, however, if you send us a check, you authorize us to peform (sic) an ACH debit on that account in the amount specified."[39]

Payday One Express of Ohio, LLC: **REMOTELY CREATED CHECK AUTHORIZATION**: "This Remotely Created Check Authorization applies only to Customers who have granted an ACH Authorization to CSO in connection with this Contract. If we are unable to process an ACH debit to your Bank Account or we do not receive a payment by the Payment Due Date, and provided that you have not revoked your ACH Authorization, you authorize us and our agents, representatives, successors and assigns to create and submit remotely-created checks for payment to us in the amount of the payment owing under this Contract, including any returned payment charges or other amounts owing to us under this Contract as a result of your default. Your typed signature below shall constitute your authorization to us to authenticate remotely created checks, which are also known as demand drafts, telechecks, preauthorized drafts, or paper drafts. If you believe we charged your Bank Account in a manner not contemplated by this authorization, then please contact us. You authorize us to vary the amount of any preauthorized payment by remotely crated heck as needed to repay any payment due under this Contract."[40]

Contract agreements such as these enable lender or merchants to evade rules governing ACH payments. The ACH system has rules to prevent merchants from manipulating the payment system to defeat consumer rights, but those rules are lacking in the check clearing system. NACHA rules would not allow an ACH authorization to be buried in fine print. Consumer authorizations

[38] La Posta Tribal Lending Enterprises payday loan contract, June 2013, on file with CFA.
[39] **eCash** payday loan contract (https://www.loanpointelms.com/lms/index.php?page=esig) loan dated 9.8/09, on file with CFA.
[40] Payday One Express of Ohio, LLC Credit Services Organization payday loan disclosures (https://www.paydayone.com/modules/directflow/apply.aspx?fn=Teriona&In=Thaler&ea=t... Accessed 6/18/13

must have clear and readily understandable terms.[41] But there are no similar rules governing the authorizations for RCCs.

By comparison, NACHA rules are also clear that a merchant may not re-process an ACH debit after a consumer has revoked authorization, whether directly or by stopping payment on the check that was the sources of an electronic check conversion. NACHA recently reiterated that, once the consumer has revoked authorization, a merchant may neither re-submit the item nor use the ACH system to initiate a late fee or other fee.[42] If either a check or an electronic payment has been stopped by the consumer or rejected as unauthorized, the item may not be re-presented electronically unless the consumer provides a new authorization. Any modification of the amount of the payment or any other change in an attempt to make the payment appear as a new entry also violates the NACHA rules.[43]

There are no similar rules that prevent a scammer from creating an RCC if a check or ACH payment has been stopped, authorization revoked, or the item was returned as unauthorized. The consumer can only contest the authorization using common law contract and agency law principles and the outcome may be uncertain. NACHA does not control when RCCs are used, even when they are being used to evade NACHA rules. RCCs enable lenders to game the system, collecting payments from borrowers' bank accounts even after consumers have revoked authorization and the lender can no longer collect the payment through the ACH system.

As the FTC documented in its recent rulemaking, payment processors have also promoted RCCs to scammers who have been banned from the ACH system, as well as to companies who fear scrutiny of their return rates. Landmark Clearing, for example, promoted its service on its website:

> Any company that has a 1% Unauthorized Returns or more will need to stop processing ACH and look for other payment methods. For legitimate companies that cannot meet this limit, [our service] is for you.[44]

Not surprisingly, the FTC found that several Landmark clients generated astronomical rates of return transactions, sometimes higher than 50%, 70% or even 80%.[45]

The use of RCCs to evade regulatory scrutiny is likely to grow as regulators crack down on improper use of the ACH system. Regulators and enforcement agencies are stepping up actions against ODFIs who enable payments for unlawful purposes. NACHA has also proposed to lower the unauthorized return threshold that triggers scrutiny from 1% to 0.5%, and to require scrutiny of any merchant whose data quality returns exceed 3% or overall debit returns exceed 15%.[46] These efforts, while welcome, will lead unscrupulous actors to turn to RCCs in order to continue their unlawful practices.

---

[41] 2013 NACHA Operating Rules 2.3.2.3.
[42] NACHA, ACH Operations Bulletin #3-2013, "Reinitiation of Returned Debit Entries" (July 15, 2013), available at https://www.nacha.org/OpsBulletins.
[43] *Id.*
[44] Ana R. Cavazos-Wright, "An Examination of Remotely Created Checks" at 13 (2009) ("Atlanta Fed Paper") available at http://www.frbatlanta.org/documents/rprf/rprf_resources/RPRF_wp_0510.pdf.
[45] *See* Complaint for Injunctive and Other Equitable Relief, FTC v. Landmark Clearing, Inc., et al, No. 4:11-cv-00826, available at http://www.ftc.gov/os/caselist/1123117/index.shtm.
[46] *See* NACHA, ACH Network Risk and Enforcement Topics, Request for Comment and Request for Information (Nov. 11, 2013), available at https://www.nacha.org/page/request-comment.

G. RCPOs Pose Even Greater Risks of Efficient, Mass Fraud and Unclear Legal Rules

RCPOs pose all of the same risks as RCCs plus two additional risks. First, the ability to by-step the paper stage of a check makes it easier to submit a high volume of fraudulent checks against numerous accounts. Second, the laws that apply to RCPOs are unclear.

A paper by the Atlanta Federal Reserve Board noted that the advent of RCPOs "allows vendors to debit a higher volume of checking accounts, including some that cannot be debited through ACH because they are ineligible."[47] Thus, fraudsters can operate with greater efficiency and scale than ever before. The use of purely electronic files also leads to "faster clearing and settlement than what is possible with paper remotely created checks."[48] That speed can also empty consumers' accounts faster before a data breach is identified or fraud is spotted. It should therefore not be surprising that the FTCs latest scam cases have involved RCPOs.

The legal framework for RCPOs is also unclear. RCCs begin as paper drafts, and thus are "checks" within the scope of the state laws that implement the Uniform Commercial Code (UCC), the primary body of law that regulates checks. But because RCPOs were never in paper written or draft form, they may fall outside those laws.

Because RCPOs are purely electronic and are not "checks," they should fall within the scope of EFTA and Regulation E. Indeed, the FRB has stated that the Board's proposal to extend RCC warranties to RCPOs under Regulation CC does not preclude a determination that RCPOs are also "electronic fund transfers" (EFTs) covered under Regulation E.[49] At least one court has so held.[50] But other courts may view RCPOs as checks because they look like checks and are processed through the check clearing system.

The industry has acknowledged the uncertain legal status of RCPOs. The ClearingHouse referenced a letter to the Federal Reserve in 2010 that stated:

> Paperless RCCs (RCPOs), while often indistinguishable from Paper RCCs to the depositary bank and to any transferring, presenting or paying bank, have uncertain legal status because, as currently defined under Regulation CC, an RCC must be reduced to paper, if even for a moment, in order to achieve definitional status as a 'check' under federal law. The uncertain legal status of Paperless RCCs is leading to increased market confusion as well as undue and unnecessary burden on depositary banks.[51]

The ClearingHouse solution was to include RCPOs as "checks" for purposes of Reg CC. NACHA supported the proposed application of warranties to RCPOs but did not support extending Subpart

---

[47] Atlanta Fed Paper, *supra*, at 13.
[48] *Id.*
[49] 76 Fed. Reg. at 16866.
[50] FTC v. Johnson, 2013 WL 800257 (D. Nev. Mar. 1, 2013).
[51] Robert C. Hunter, The ClearingHouse, Letter to Louise L. Roseman, Board of Governors of the Federal Reserve System, October 28, 2010 Re: Proposed Amendment to Regulation CC to Address Paperless Remotely Created Checks."

C coverage to RCPOs as "checks" pending a more thorough review of the appropriate legal foundation for this product.[52]

The Atlanta Federal Reserve Board's paper noted that "using electronic remotely created checks for ACH ineligible conversion eschews ACH unauthorized return monitoring and control procedures, while bypassing check law entirely."[53]

Whatever their technical legal status, RCPOs are identified by the check clearing system and bank operational systems as checks, not electronic transfers. It is virtually impossible for systems to distinguish them from checks. Thus, banks do not apply Regulation E procedures to RCPOs, and regulators cannot look for Regulation E compliance. Consequently, merchants who use RCPOs attempt to have it both ways: to enjoy the efficiencies of electronic payment systems without complying with the consumer protection and compliance regimes required of electronic payments.

[52] Ian W. Macoy, NACHA, Comments in Docket No. R-1409 (June 3, 2011).
[53] *See* Atlanta Fed Paper, *supra*, at 14.

III. The Risks of RCCs Outweigh the Benefits

A. Opposition to and Concerns About Use of RCCs are Widespread

For almost a decade, many regulators and advocates have called for the banning of RCCs. Many believe that any legitimate reasons to use RCCs instead of an ACH or debit card option for a payment are far outweighed by the risks of RCCs.

Canada prohibited RCCs (calling them "tele-cheques") in 2004 amid concerns over the high potential for fraud.[54] The Canadian Payments Authority explained:

> The key risk associated with a tele-cheque is fraud (i.e., risk of unauthorized payment). This particular type of payment does not contain the signature of the Payor nor is it supported by any other form of signed authorization. Given this, it is impossible for the Payor financial institution to verify that the Payor has in fact authorized the Payee to act as a signatory for the specific payment. Furthermore, the risk of unauthorized payments is elevated since a Payee could issue a tele-cheque against a Payor's account simply after obtaining the necessary account details. In this regard, to permit tele-cheque entry into the clearing system would increase the risk that unauthorized parties would use this vehicle to gain access to deposit accounts fraudulently.
>
> In studying the tele-cheque issue, the CPA considered whether procedures could be put in place to sufficiently mitigate the risks associated with this payment instrument. In its assessment, the PA consulted broadly with financial institutions and payment system service providers and users. There was a generally held view that tele-cheques represent an unacceptable level of risk, since the key to mitigating the risk of unauthorized transactions is the ability to verify authorization.[55]

In 2005, the attorneys general of thirty-five states, the District of Columbia, and American Samoa asked regulators to ban RCCs.[56] The AGs noted that fraudsters were switching to RCCs once they learned how easily ACH payments could be traced, and that legitimate companies no longer heavily relied on the RCCs. They cited evidence that the Canadian ban been successful and had not generated complaints from companies that used RCCs in the past.

Regulators in the United States have long been grappling with the risks of RCCs. In 2002, in light of fraud concerns, the National Conference of Commissioners on Uniform State Laws and the

---

[54] While there is no specific rule or law barring them, the Canadian Payments Authority, which operates Canada's payment clearing system, prohibits their use. Canadian Payments Authority, "Prohibition of Tele-Cheques in the Automated Clearing Settlement System" (June 1, 2003), *available at* http://www.cdnpay.ca/imis15/eng/Act_Rules/Automated_Clearing_Settlement_System_ACSS_Rules/eng/rul/policy_statement_telecheques.aspx.

[55] "Prohibition of Tele-cheques in the Clearing and Settlement System - Policy Statement," Canadian Payments Association (June 1, 2003).

[56] National Association of Attorneys General, Comment to the FRB Docket No. R-1226 (Proposed Amendment to Regulation CC/Remotely Created Checks) (May 9, 2005), available at http://www.federalreserve.gov/SECRS/2005/May/20050512/R-1226/R-1226_264_1.pdf; *see also* Oversight of Telemarketing Practices and the Credit Repair Organizations Act: Hearing Before the Senate Commerce, Science & Transp. Comm. (July 31, 2007) (testimony of Richard Johnson, Member of the Board of Directors, AARP, available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=b8655fb6-b7a3-457b-b675-69830dbea5ee

American Law Institute proposed altering longstanding payment rules of the UCC to create new warranties requiring the person or institution transferring an RCC to warrant that it was authorized.

After only a handful of states adopted the revisions, in 2006 the FRB stepped in and adopted similar warranties through Regulation CC. In 2011, the FRB proposed further amendments to Regulation CC – yet to be finalized – to extend those warranties to RCPOs.[57] But that amendment is merely a formality, as RDFIs cannot distinguish RCCs from RCPOs and would assert warranty coverage even if the item never existed in paper form.

The Regulation CC warranties have not stopped the problems with RCCs. Federal regulators continue to grapple with the problems they pose.

The Atlanta Division of the Federal Reserve Board outlined the risks of RCCs in a 2009 white paper.[58] The paper outlined a number of examples of RCC fraud and concerns about the rise of RCPOs.

In 2010, NACHA, the Electronic Payments Coalition,[59] published a white paper highlighting the risks of RCCs. NACHA's Risk Management Advisory Group concluded:

> ACH debit transactions, such as TEL transactions, offer a payment choice where the safeguards to Receivers outweigh the conveniences that RCCs currently offer to Payees. This conclusion is based on the following factors: (1) the heightened risk profile of RCC transactions that bear no evidence of authorization, (2) the fact that ACH transactions can be identified and monitored with relative ease, and (3) the fact that the Rules include clear and explicit authorization requirements for capturing evidence of a consumer's authorization of a transaction.[60]

In 2013, the FTC, after initially attempting to ensure that consumers have provided express verifiable consent for creation of an RCC, finally proposed to ban RCCs entirely in telemarketing sales.[61] The FTC articulated specifically and carefully why the uses of RCCs and RCPOs are abusive and cause substantial consumer economic injury which cannot be reasonably avoided.[62] The FTC explained that other payment mechanisms with significantly greater consumer protections are available as alternatives, such as credit card payments covered by the Fair Credit Billing Act and electronic fund transfers covered by the Electronic Fund Transfers Act. As the Commission says,

---

[57] Our organizations have supported the extension of the warranty as an interim measure but believe that ultimately RCCs and RCPOs should be banned. *See* NCLC et al., Supplemental Comments, 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.

[58] *See* Atlanta Fed Paper, *supra.*

[59] NACHA, Remotely Created Checks and ACH Transactions: Analyzing the Differentiators, A Risk Management White Paper (2010), available at http://www.macha.org/Portals/0/RCC%20White%20Paper%20031110%20Final.pdf.

[60] *Id.* at 12.

[61] *See* 78 Fed. Reg. 41200 (July 9, 2013). The FTC's proposal is limited to transactions that involve a telephone call and fall under the Telemarketing Sales Rule, but only because that is the limit on the FTC's effective rulewriting authority. The FTC's rationale also applies to purely internet transactions.

[62] *See* Section II.A.4, Federal Trade Commission, Notice of Proposed Rulemaking, 16 CFR Part 310, Telemarketing Sales Rule. Available at http://www.ftc.gov/os/2013/05/130521telemarketingsalesrulefrn.pdf.

> [t]hese alternatives offer both dispute resolution rights and protections against unlimited liability for unauthorized charges to consumers and are available to consumers who do not possess or do not wish to use credit cards.[63]

Our own organizations and others have highlighted the problems with RCCs for years. In 2005 comments filed with the FRB, NCLC, CFA, Consumers Union and NACA supported the Attorneys General call for a ban on RCCs.[64] AARP asked Congress to consider a ban on RCCs in 2007. [65] In 2008, NCLC, CFA, Consumers Union and NACA highlighted the problems of Social Security recipients who could have their bank accounts hijacked by payday lenders using RCCs.[66] In 2009, CFA testified in opposition to federal legislation that would have authorized payday loans based on the use of RCCs.[67]

Financial industry specialists have also called for the elimination of RCCs. George F. Thomas, a principal at Radix Consulting Corp., has argued:

> With the technology that exists today, there is no practical reason for continuing the use of remotely created checks. In fact, advanced technology makes them more dangerous than ever before. With the advent of new banking products such as remote deposit capture, those individuals attempting to commit fraud can submit unsigned checks without even paying a visit to a branch to deposit them. The remote submission of unsigned checks increases the velocity of items that can be submitted.[68]

The evidence and concerns have mounted to the point where the conclusion is inevitable: RCCs should be banned.

---

[63] Section II.A.4, Federal Trade Commission, Notice of Proposed Rulemaking, 16 CFR Part 310, Telemarketing Sales Rule. Available at http://www.ftc.gov/os/2013/05/130521telemarketingsalesrulefrn.pdf. P. 40

[64]Comments of NCLC et al, Docket No. R-1226, Proposed Amendment to Regulation J and Regulation CC Regarding Remotely Created Checks (filed May 3, 2005), available at http://www.nclc.org/images/pdf/banking_and_payment_systems/archive/rc-comments-fed5.pdf.

[65] ***See*** Oversight of Telemarketing Practices and the Credit Repair Organizations Act: Hearing Before the Senate Commerce, Science & Transp. Comm. (July 31, 2007) (testimony of Richard Johnson, Member of the Board of Directors, AARP, available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=b8655fb6-b7a3-457b-b675-69830dbea5ee.

[66] *See* CFA, NCLC et al, Comments to Department of Treasury, Social Security Administration Regarding the Use of Master and Sub Accounts and Other Account Arrangements for the Payment of Benefits, Docket No. SSA 2008-0023 (June 2008), available at http://www.nclc.org/images/pdf/banking_and_payment_systems/banking_comments_june08.pdf.

[67] Testimony of Jean Ann Fox, CFA, House Financial Services Subcommittee hearing, H.R. 1214, April 2, 2009 at http://www.consumerfed.org/elements/www.consumerfed.org/file/Testimony_of_Jean_Ann_Fox_on_H_R_1214_hearing_4-2-09%281%29.pdf.

[68] *See* George Thomas, "Viewpoint: Remote Checks Pose High Risk," *American Banker* (Feb. 17, 2010), available at http://www.americanbanker.com/issues/175_31/remote-checks-pose-high-risk-1014530-1.html.

B. RCCs are not Essential for the Few Remaining Legitimate Uses and their Risks Outweigh Their Benefits

As described above, RCCs and RCPOs are heavily used in an abusive fashion for the purpose of (1) processing unlawful or fraudulent payments, (2) defeating consumer rights and control over their bank account, (3) evading scrutiny of the electronic payment networks and regulators, and (4) processing payments by merchants who have been banned from other payment systems.

Setting these motivations aside, RCCs do have some advantages over other payment systems that explain their use in more legitimate settings. However, those advantages are minimal as electronic payment systems have adapted to new uses, and any advantages simply cannot justify the extensive risks of permitting RCCs in the payment system.

As noted above, Canada banned RCCs in 2004 and in 2005 attorneys general in 35 states called for a ban in the United States. Even eight years ago, AGs noted that "anecdotal evidence suggests that demand drafts are used by legitimate businesses to only a limited extent at this time."[69] The AGs also noted that "there has been no complaint about the [Canadian] ban from companies that may have used these instruments in the past, such as bill collectors and payday lenders."[70]

In a 2010 white paper, NACHA identified three advantages to RCCs over electronic payments that supported some legitimate uses:

- same-day availability of funds;
- ease of collecting NSF fees by retailers; and
- the ability of a debt collector or others to obtain authorization for recurring payments with a single telephone call.[71]

But despite these advantages, NACHA concluded that the safeguards of ACH debit transactions outweighed the conveniences of RCCs, given their risks.[72]

In a 2009 paper, the Atlanta Federal Reserve Board outlined common uses of RCCs:

> (1) pre-authorized drafts, where for example, a consumer approves a payment of its insurance policy and the company issues an unsigned draft for the amount; (2) ACH administrative returns, where the ACH item is returned because the information originally provided from the MICR line cannot be properly processed and the merchant resubmits the ACH item as an unsigned draft; (3) telephone purchases, typically, where telemarketers call selling products or services to companies or individuals, and the telemarketer requests information from the consumer about its bank account for the purposes of obtaining payment; (4) depository transfer checks, instances where companies initiate transfer payments between their accounts, some of which may be between different banks; (5) return

[69] AG Letter, *supra*, at 6.
[70] *Id.*
[71] NACHA, "Remotely Created Checks and ACH Transactions: Analyzing the Differentiators" (2010), available at http://www.macha.org/Portals/0/RCC%20White%20Paper%20031110%20Final.pdf.
[72] Id. at 12.

item fees, created by merchants to cover fees for returned checks; and (6) bill payment, where the consumer authorizes a creditor such as a credit card company to create a remotely created check in order to timely pay a bill that would otherwise be late if paid with a traditional paper check.[73]

Most of these uses seem to stem from the three advantages NACHA identified above, and simply the inertia of legacy systems.

Since 2010, changes in NACHA rules, along with other ACH or debit card options, have all but eliminated the few legitimate advantages of RCCs over other forms of payment. Retailers can collect NSF fees through the ACH system in nearly the same manner as with an RCC. NACHA revised its rule for telephone authorizations to enable recurring payments to debt collectors and others. New internet and mobile payment systems now enable merchants to more easily collect ACH and card payments. The spread of smartphones and mobile payment systems will accelerate that trend greatly. Common uses of RCCs that are simply due to inertia could adapt to a world without RCCs.

In some circumstances, RCCs still have a slight advantage over ACH payments. The merchant's bank may give immediate access to the funds as soon as the check is deposited, even before it clears, while an ACH payment will take a day or two to settle. Even that advantage is dependent on bank courtesy, as the check may not actually clear any faster than an ACH payment. Moreover, this advantage is not important enough to outweigh all the risks of RCCs. Rarely will that day or two matter. Even if a consumer is trying to pay her mortgage or insurance on the day it is due, the mortgage or insurance company can treat the payment as if it was received on the day it is authorized even if it has not yet settled. In other situations, wire transfers are available if funds must reach the recipient the same day.

Improvements in the speed of ACH settlement would eliminate even this remaining advantage of RCCs. Indeed, the question of how to work towards a near real-time payment system is one of the key topics that the Board has posed in its request for comments.

But attention to the RCC problem should not await an overhaul of the ACH system. RCCs are causing real harm, today, that needs to be addressed. Canada has done without them for years. Merchants using RCCs today will have other options. At this point in time, the legitimate advantages of RCCs have outlived their usefulness and it is time to end them.

IV. Action by the Fed to Ban on RCCs and RCPOs is Necessary to Stop Fraudulent Uses

A. The FTC Does Not Have Sufficient Authority to Address RCC Abuses

The scammers who use RCCs are subject to FTC jurisdiction, and the agency has devoted considerable attention to the issue. Earlier this year, the FTC proposed to ban the use of RCCs and RCPOs in transactions covered by the Telemarketing Sales Rule (TSR). We support that proposal. But the FTC's proposal will not stop RCC abuses, because the proposal and the FTC's authority are limited.

[73] *See* Atlanta Fed Paper, *supra.*

First, the FTC's rulemaking authority under the TSR does not extend to transactions that do not involve a telephone call. Yet the same scams that happen in the telemarketing context also occur in exclusively internet-based transactions and others that are outside the current scope of the TSR. A telephone call is not a necessary element of the scams. Indeed, some of the cases cited by the FTC in support of its proposed ban involved internet scams.[74]

A new case brought by the FTC in September 2013 illustrates the problem. Sean C. Mulrooney and Odafe Stephen Ogaga and five companies they controlled bilked $5 million from consumers who went to the defendants' websites to get payday loans.[75] Instead of giving them loans, the defendants used consumers' personal financial information to create RCCs to debit their bank accounts in increments of $30 without their authorization. Websites with the names Vantage Funding, Ideal Advance, Loan Assistance Company, Palm Loan Advances, Loan Tree Advances, Pacific Advances, and Your Loan Funding collected consumers' names, Social Security numbers, bank routing numbers, and bank account numbers, which allowed them to access consumers' checking accounts. But because the conduct was online and did not involve telemarketing, the proposed TSR ban will not apply to this conduct.

Second, the FTC's proposed TSR rule also does not apply to banks. A ban on RCCs that only applies to telemarketers will be ignored by many scammers, who are already violating the law. In order for the ban to be effective, banks must be prohibited from processing the RCCs and must be responsible when they do so.

Third, it is difficult for the FTC to hold third parties like payment processors accountable when they facilitate scams. The FTC does have general authority over payment processors (at least those that are not bank subsidiaries), and the proposed TSR prohibits any person from assisting or facilitating practices that violate the rule. However, the rule only holds a third party liable if the person "knows or consciously avoids knowing" of the violation.[76] That is a difficult standard to prove and insulates many payment processors who are essential to a fraudulent scheme.

Without the ability to reach the banks and payment processors that facilitate scams, action against the scammers themselves is often a hollow victory. For example, in the IWorks case, the FTC obtained settlements with two defendants who alleged took more than $275 million from consumers. The settlement imposes monetary judgments of more than $289 million and $7.5 million, respectively, but the judgments will be suspended based on the defendants' inability to pay, provided they surrender certain assets to the FTC, including $20,000 from Payne and $1,000 from Pilon. Thus, consumers will not get restitution.

Consequently, the current approach will not stop fraudulent use of RCCs. Without further action that applies outside the telemarketing context, that applies to banks, and that does not rely on proving knowledge by those who facilitate fraudulent payment, RCCs will continue to be used to defraud consumers. The FTC does not have sufficient authority, and action by the FRB is critical.

---

[74] *See* FTC TSR Proposal, 78 Fed. Reg. at 41207-09.
[75] *See* FTC, Press Release, "At the FTC's Request, Court Halts Alleged Phony Payday Loan Broker" (Sept. 4, 2013), available at http://www.ftc.gov/opa/2013/09/vantage.shtm.
[76] 16 C.F.R. § 310.3(b).

B. Banks are Responsible When They Facilitate Unlawful Payments

Actions by bank regulators have made clear that ODFIs must avoid facilitating unlawful payments and are responsible for conducting due diligence about the payments they are processing. When banks have ignored warning signs of problems, they have faced consequences.

For example, in 2008, the OCC entered into a consent decree with Wachovia Bank, stating that the bank engaged in unsafe, unsound, and unfair banking by debiting consumer accounts for payment processors acting on behalf of telemarketers. The bank ignored allegations of consumer fraud from other banks and consumers, and failed to scrutinize its relationship with payment processors and telemarketers.[77]

In 2010, the FDIC entered into a consent order with SunFirst Bank in St. George, Utah, in large part caused by third-party payment processing problems. The FDIC required SunFirst to cease providing third-party payment processing for Triple Seven LLC, Master Merchant LLC, Powder Monkeys LLC, and Elite Debit, and their associated accountholders, customers and clients.[78]

Another FDIC-supervised bank paid a civil penalty of $15 million and lost its state charter, in part due to its activities in processing RCCs for high-risk merchants and originators. The Department of Justice alleged that First Bank of Delaware originated fraudulent debits for merchants, in many cases using RCCs, despite being well aware of the consumer fraud risks posed by payment processors and RCCs.[79] First Bank of Delaware originated more than 2.6 million RCCs totaling approximately $123 million "on behalf of third-party payment processors in cahoots with fraudulent Internet and Telemarketing merchants."[80] A class action lawsuit alleged that Zaazoom lured victims into applying for payday loans via websites and used applicants' banking information to drain their accounts without authorization.[81]

Federal bank regulators have also issued guidance to the banks they supervise to address the risks posed by relationships with payment processors and merchants. The FDIC has warned banks that they have a duty to look out for entities like telemarketers that pose a risk of processing unauthorized payments.[82] The OCC has also issued guidance to national banks for due diligence, underwriting, and monitoring of entities that process payments for telemarketers and other merchant clients, noting that certain merchants, such as telemarketers, pose a higher risk than other merchants and require additional due diligence and close monitoring.[83]

---

[77] *In re* Wachovia Bank, 2008-027 (OCC Consent Order for a Civil Penalty, Apr., 24, 2008) (.).
[78] FDIC, In the Matter of SunFirst Bank, Consent Order FDIC-10-845b, November 9, 2010, http://www.fdic.gov/bank/individual/enforcement/2010-11-23.pdf
[79] Press Release, "Department of Justice Announces $15 Million Settlement with Local Bank Accused of Consumer Fraud," November 19, 2012, www.justice.gov/usao/pae/News/2012/Nov/FBD_release.htm See, also, Samuel Rubenfeld, "First Bank of Delaware Loses Charter Over AML Problems," The Wall Street Journal, November 19, 2012 http://blogs.wsj.com/corruption-currents/2012/11/19/first-bank-of-delaware-loses-charter-over-aml-problems/
[80] United States v. First Bank of Delaware, Civ. No. 12-6500 (E.D. Pa. Nov. 19, 2012).
[81] *See* Marsh v. Zaazoom Solutions, LLC., 2012 WL 6522749 (N.D. Cal. 2012).
[82] The FDIC issued a revised guidance "describing potential risks associated with relationships with third-party entities that process payments for telemarketers," warning depositary banks that open accounts for these entities to be on the lookout for risks associated with these relationships. Federal Deposit Ins. Corp., FIL-3-2012, Payment Processor Relationships Revised Guidance (Jan. 31, 2012), *available at* www.fdic.gov/news/news/financial/2012/fil12003.html.
[83] *See* OCC Bulletin No. OCC 2008-12, Payment Processors (Apr. 24, 2008), available at http://www.occ.gov/news-issuances/bulletins/2008/bulletin-2008-12.html.

The actions are important. But they have not stopped the misuse of RCCs to defraud consumers.

B. A Complete Ban on RCCs is the Cleanest Way to Help Payment Processors and Originating Banks Avoid Facilitating Fraudulent and Unlawful Payments

To date, regulators have focused on banks and payment processors who ignored flagrant warning signs about the legitimacy of the payments that they have originated. Those actions are important and have highlighted the critical role that payment processors and originating banks play in facilitating unscrupulous practices by merchants.

But the focus on the most obviously egregious cases enables many other fraudulent payments to escape scrutiny. Fraudsters are becoming smarter in how they launder their payments. Payment processors may process payments for other processors, making it harder to see who the ultimate receiver of the payment is. Processors may also split up the payments among different ODFIs to ensure that no single bank can see the entire picture or that high returns do not pile up in one place for too long.

For example, the FDIC's 2010 consent decree with SunFirst Bank did not solve the problems caused by the payment processors who were using the bank for illegitimate purposes. One of SunFirst's clients, Elite Debit, was sued in January 2013 by the FTC for charging consumers monthly fees for services they never agreed to purchase.[84] The complaint mentions numerous banks, in addition to SunFirst, that the defendants processed payments through, including Wells Fargo, N.A., HSBC Bank USA, First Regional Bank, Harris National Association, Columbus Bank and Trust Company and The Village Bank.

A complete ban on RCCs would enable banks to "just say no" to RCCs. Regulators would not have to wait until red flags were obvious. Banks could avoid getting caught in an enforcement action if regulators believe that the bank should have seen the warning signs.[85] It is easier for a bank to determine if its clients are depositing RCCs than to know whether the underlining transaction was fraudulent. Originating banks are in a better position to ask their clients, or their clients' clients, whether they are submitting RCCs and to spot check them to ensure that they are not.[86] Evidence of even a single RCC would be a clear warning sign that the rule is being violated.

In many cases, banks may have indications of fraudulent activity, but current rules may not be strong enough to hold banks responsible for their role in facilitating that conduct. For example, the Sixth Circuit recently upheld the dismissal of claims against two banks that maintained accounts for, and were alleged to have conspired with, telemarketers to process RCCs and ACH payments for various telemarketers engaged in fraudulent activities. The court held that significant red flags of

---

[84] FTC v. Jeremy Johnson, IWorks, Inc.; Cloud Nine, Inc.; CPA Upsell, Inc.; Elite Debit, Inc.; et al, First Amended Complaint, No. 10-cv-2203-RLH, (D. Nev. Jan. 18, 2013), available at http://www.ftc.gov/os/caselist/1023015/130118iworkscmptexha.pdf

[85] *See, e.g.,* Brett Wolf, "FDIC SunFirst action a reminder of third-party processor risk to banks," January 7, 2011, http://blogs.reuters.com/financial-regulatory-forum/2011/01/07/fdic-sunfirst-action-a-reminder.... Viewed 6/24/13

[86] Automated systems may not be able to distinguish an imaged check that has a signature from one that does not. But visual inspection can.

fraudulent telemarketing were insufficient to show that the banks actually knew of the fraudulent activities and agreed to conspire with the telemarketers.[87]

Similarly, a district court upheld a claim against one bank but dismissed claims against others that allegedly knew or should have known that they were processing fraudulent payments, including RCCs, for telemarketers. The court was unconvinced by a pleading stating, among other indicia, that the banks transferred money to countries known as money laundering havens for fraudulent telemarketers and that the accounts had numerous consumer transactions that were challenged, refunded, or returned for insufficient funds.[88]

A complete ban on RCCs would also help address evasions that can mask the source of an RCC. Typically, the merchant using RCCs does not have a direct account with the originating bank but uses a payment processor. The payment processor may have a direct relationship with the telemarketer, payday lender or other scammer, or it may process payments received from other payment processors. But in either case, the payment processor can serve as a vehicle for laundering the identity of the payee and giving the originating bank deniability from claims that it is processing fraudulent payments.[89]

The current approach does not prohibit banks from processing RCCs for high risk merchants. Despite regulatory warnings about risks, some banks will decide that the rewards are worth the risks. The FTC's proposed TSR ban notes that payment processors have "perverse financial incentives" when it comes to scam artists.[90] The same is true of the banks that originate the payments. Small banks eager for fee income may be especially tempted by the high revenue paid by processors who handle high risk payments. Banks may also profit off of return fees when return rates are high.

As is evident from the hundreds of millions of dollars per year in fraudulent processing of RCCs, existing rules have not prevented payment processors and ODFIs from facilitating these dangerous payment mechanisms. A complete ban on RCCs would ensure that payment processors and ODFIs cannot hide behind claims of ignorance in processing unlawful payments. It will eliminate the gray zones, create clear black and white rules, and make it much harder for fraudsters to drain consumers' bank accounts.

D. The FRB Has the Authority to Ban RCCs

The Board has the authority to prohibit RCCs through Regulation CC and its power under the Expedited Funds Availability Act. The EFAA gives the Board the responsibility to regulate "(A) any aspect of the payment system, including the receipt, payment, collection or clearing of checks; and (B) any related function of the payment system with respect to checks."[91]

---

[87] Johnson v. US Nat' Bank Ass'n, 2012 WL 6200260, 508 Fed.Appx. 451 (6th Cir. Dec. 12, 2012).
[88] *See* Reyes v. Zion First Nat. Bank, 2012 WL 947139 (E.D. Pa. Mar. 21, 2012).
[89] FTC v. 3d Union Card Serv., doing business as Pharmacycards.com, Civ. Action No. CV-S-04-0712-RCJ-RJJ (D. Nev. 2004).
[90] Section II.A.2, Federal Trade Commission, Notice of Proposed Rulemaking, 16 CFR Part 310, Telemarketing Sales Rule. Available at http://www.ftc.gov/os/2013/05/130521telemarketingsalesrulefrn.pdf (*citing* United States v. First Bank of Delaware, Civ. No. 12-6500 (E.D. Pa. Nov. 19, 2012)).
[91] 12 U.S.C. § 4008(c)(1).

The Board has already used its Regulation CC authority to impose warranties on ODFIs who originate RCCs. But that liability has clearly not been sufficient to stop abuses. The time has come to eliminate RCCs from the payment system.

E. Until a Complete Ban Can Take Effect, Banks Should Have Greater Responsibility to Monitor Use of RCCs and to Avoid Processing Unlawful RCCs

If the Fed concludes that a complete ban on RCCs cannot be accomplished immediately, it should announce a plan to work toward a complete ban, to take effect on a later date, and a series of important interim measures. We urge the FRB, together with the other banking agencies, to undertake a number of measures to monitor the use of RCCs and to require banks to exercise greater scrutiny over the RCCs they process.

First, the FRB should ban use of RCCs as a back-up payment mechanism. A merchant should be prohibited from creating an RCC after an ACH payment is stopped, authorization is revoked, or the item is returned for lack of authorization. NACHA rules prohibit an originator from using a check as the source document for an ACH payment or otherwise initiating an ACH payment after a check has been stopped or otherwise revoked. But NACHA does not have the authority to impose the converse rule – to stop creation of an RCC after authority for an ACH fails. The FRB has that authority in its role over the check system.

Second, the FRB and other bank regulators should require ODFIs to identify which customers are using RCCs, monitor return rates, improve know-your-customer due diligence, and take action to stop inappropriate use of RCCs. ODFIs should be prohibited from processing RCCs for entities on NACHA's terminated operator list and required to conduct close scrutiny of those on the operator watch list or engaged in high-risk businesses. Banks that fail to conduct close oversight of customers who use RCCs should face supervisory or enforcement action.

Although distinguishing RCCs from conventional checks is difficult for RDFIs, it is not for ODFIs. As the FTC points out:

> *[I]ndividual* banks and payment processors, however, can detect remotely created checks, investigate the total return rates of their clients' check transactions, compare the percentage of returned remotely created checks to the return rate for all checks transacted through the national banking system (approximately one half of one percent or .5 percent), attempt to categorize the specific reasons for returns, compare their clients' return rates to industry average return rates for other payment mechanisms (such as credit card payments and ACH debits), and watch closely for other signs of suspicious or fraudulent merchant activity.[92]

Third, the FRB should consider requiring RCCs to be specially marked. If such a marking system can be implemented without undue delay, it should be. But if a marking system requires a substantial, time-consuming overhaul to the check clearing system, it may make more sense to simply work towards a complete ban without wasting time on this interim step. Even without a marking system, however, the Board could educate banks on how to identify RCCs so that they can

[92] FTC TSR Proposal, 78 Fed. Reg. at 41207.

be monitored. For example, we understand that the check numbers for RCCs have more digits than most consumer checks.

Finally, if the Board concludes that it cannot institute a ban immediately, it should use the transition period to conduct an updated survey of the use of RCCs. Knowing more about the ways in which legitimate parties use RCCs will enable regulators to assist them in adapting to the ban.

Conclusion

The FTC set forth a compelling case for prohibiting the use of RCCs and RCPOs in telemarketing transactions. The *exact* same set of facts, analysis, and rationale justify prohibiting these payment mechanisms altogether in consumer transactions. There is nothing unique about transactions within the scope of the TSR; purely internet based transactions are just as subject to fraud, deception and illegality. RCCs are no longer a critical payment mechanism for legitimate uses, and their dangers far outweigh the benefits. A complete ban on RCCs and RCPOs will ensure compliance with the FTC's expected TSR rule; prevent originating banks and payment processers from being witting or unwitting accomplices to illegality; and ensure that scammers and questionable businesses operate in a system where their payments can be monitored.

Respectfully submitted,

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

Jean Ann Fox
Consumer Federation of America

Rebecca Borné
Center for Responsible Lending

Ruth Susswein
Consumer Action

Suzanne Martindale
Consumers Union

Ellen Taverna
National Association of Consumer Advocates

Sally Greenberg
National Consumers League

Ed Mierswinski
U.S. PIRG

APPENDIX

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.

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 **Center for Responsible Lending (CRL)** is a nonprofit, non-partisan research and policy organization dedicated to protecting homeownership and family wealth by working to eliminate abusive financial practices. CRL is an affiliate of Self-Help, a nonprofit community development financial institution. For 30 years, Self-Help has focused on creating asset building opportunities for low-income, rural, women-headed, and minority families, primarily through financing safe, affordable home loans.

Consumer Action has been a champion of underrepresented consumers nationwide since 1971. A nonprofit 501(c)3 organization, 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.

Consumers Union is the public policy and advocacy division of Consumer Reports. Consumers Union works for telecommunications reform, health reform, food and product safety, financial reform, and other consumer issues. Consumer Reports is the world's largest independent product-testing organization. Using its more than 50 labs, auto test center, and survey research center, the nonprofit rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 8 million subscribers to its magazine, website, and other publications.

The **National Association of Consumer Advocates** (NACA) is a non-profit corporation whose members are private and public sector attorneys, legal services attorneys, law professors, and law students, whose primary focus involves the protection and representation of consumers. NACA's mission is to promote justice for all consumers.

National Consumer's League, founded in 1899, is the nation's pioneering consumer organization. Our non-profit mission is to protect and promote social and economic justice for consumers and workers in the United States and abroad.

U.S. Public Interest Research Group (U.S. PIRG) serves as the Federation of State PIRGs, which are non-profit, non-partisan public interest advocacy organizations that take on powerful interests on behalf of their members. For years, U.S. PIRG's consumer program has designated a fair financial marketplace as a priority. Our advocacy work has focused on issues including credit and debit cards, deposit accounts, payday lending and rent-to-own, credit reporting and credit scoring and opposition to preemption of strong state laws and enforcement. On the web at uspirg.org.

September 18, 2013

Mr. Robert deV. Frierson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Ave., NW
Washington DC 20551

Ms. Monica Jackson
Office of the Executive Secretary
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

Re: Supplemental Comments, 12 CFR Part 229, Regulation CC: Docket No. R-1409, 76 Fed. Reg. 16862 (Mar. 25, 2011), Remotely Created Items, Funds Availability Schedule for Prepaid Cards and Mobile Deposits

Dear Mr. Frierson and Ms. Jackson,

We understand that finalizing the amendments to Regulation CC that were proposed in 2011 is on the regulatory agenda for the end of this year. That docket included questions about updates to the funds availability schedule to address modern check clearing methods, as well as the appropriate rules for certain forms of remotely created payment items. The National Consumer Law Center (on behalf of its low income clients), Consumer Action, Consumer Federation of America, Consumers Union, the nonprofit publisher of Consumer Reports, National Association of Consumer Advocates, and National Consumers League are writing to comment, or to update our earlier comments,[1] in that docket.[2] Although the comment period has closed, we hope that you will consider these comments in light of new developments that warrant further comment.

We urge the Consumer Financial Protection Bureau (CFPB) and Federal Reserve Board (FRB) to:

- Open a rulemaking to work towards the elimination of remotely created checks (RCCs) and remotely created payment orders (RCPOs) (called "electronically-created items" or "electronic image and information" by the FRB) in consumer transactions.
- In the interim, extend RCC warranties to RCPOs, clarify that RCPOs are covered by the protections of Regulation E, and improve monitoring of both RCCs and RCPOs.

[1] In June 2011 Consumers Union and Consumer Federation of America filed comments in the Regulation CC docket to address proposals regarding the hold period for nonproprietary ATM deposits, non "on us" checks and checks from consumers with repeated overdrafts.
[2] Organizational descriptions are attached as an appendix. These comments were written by Lauren Saunders of the National Consumer Law Center and Laura Udis and Jean Ann Fox at the Consumer Federation of America.

- Treat remotely created items that bear a handwritten electronic "signature" in the same fashion as RCCs and RCPOs.
- Clarify the application of the Expedited Funds Availability Act (EFAA) to ensure that consumers have prompt access to deposits made on mobile and other devices through remote deposit capture (RDC) and to deposits to prepaid cards.

We also support, but will not further comment on, the FRB's proposal to amend Regulation CC to:

- Eliminate nonlocal checks and extend the local check available schedule to all checks.
- Reduce the maximum hold period for nonproprietary ATM deposits.
- Exclude declined debit card transactions from the exception that allows banks to extend hold times for consumers who have had "repeated overdrafts."
- Reduce the reasonable hold extension period for non "on us" checks to two business days.

We appreciate these efforts to give consumers faster access to funds that they deposit by check, which is especially important for families who are struggling to make ends meet without incurring overdraft fees.

1. RCCs and RCPOs Should Be Banned Entirely

Remotely created checks (RCCs) and remotely created payment orders (RCPOs) (termed "electronically-created items" or "electronic image and information" by the FRB) should be banned entirely in consumer transactions (and possibly all transactions). We will address this subject briefly in these comments and will also soon send you a separate letter addressing the topic at greater length. You may also wish to review our recent comments to the Federal Trade Commission (FTC) in connection with the FTC's proposal to ban use of RCCs and RCPOs in telemarketing sales.[3]

An RCC is "a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn." 12 C.F.R. § 229.2(fff). Any merchant that obtains a consumer's bank routing and account number can create and print an RCC with the proper software or the help of a third-party payment processor. The payee or payment processor then deposits the RCC into its bank account for collection. Once an RCC is introduced into the check clearing system, it is virtually indistinguishable from a traditional paper check.

An RCPO is the all-electronic version of an RCC. An RCPO never existed in printed paper form but is nonetheless deposited into and cleared through the check clearing system. A merchant or payment processor simply enters a bank account number and bank routing number into an

[3] Comments of NCLC et al. to the Federal Trade Commission, 16 CFR Parts 310 [RIN 3084-AA98], Telemarketing Sales Rule, Project No. R411001 (Remotely Created Checks and Other Items) (submitted August 2, 2013), available at http://www.nclc.org/images/pdf/rulemaking/ftc-telemarketing-rcc-comments-822013.pdf.

electronic file that is transmitted to a financial institution for processing via the check clearing system. Like an RCC, an RCPO is indistinguishable from traditional paper checks that have been imaged. However, whether an RCPO is covered by the laws that protect checks, electronic transactions, both, or neither is unclear.

RCCs and RCPOs are used by payday lenders (storefront, internet and tribal), internet scammers, and merchants in high-risk industries such as gambling advice, psychic readings, pyramid sales, terminated merchants, pawn brokers, bail bondsmen, debt reduction services, and loan modifications. Our organizations have seen widespread use of RCCs and RCPOs to evade consumer protections, to compromise consumers' control over their bank accounts, and to facilitate unlawful, fraudulent, unfair, deceptive and abusive practices.

We recognize that RCCs, and possibly RCPOs, are used for some legitimate purposes. However, we believe that much of the continuing use of these payment devices is due to inertia and that safer electronic payment systems can substitute in these situations with lower risks.

We support the FTC's proposal to ban the use of RCCs and RCPOs in transactions covered by the Telemarketing Sales Rule (TSR). The FTC has outlined a compelling case describing the pervasive misuses of RCCs and RCPOs that justify a ban in telemarketing sales.

However, the TSR rule will not be effective without a ban that applies to depository institutions, which are outside the FTC's jurisdiction. Moreover, the FTC's rule will not apply to transactions that do not involve a telephone call and do not fall under the TSR. Yet the reasons to ban RCCs and RCPOs in those transactions are just as compelling.

RCCs and RCPOs should be banned because:

- They are too easy to use to debit bank accounts without consumer consent.
- They lack the consumer protections available for other electronic payment methods.
- They operate through the check clearing system, which lacks the systemic controls to police fraudulent and unlawful use.
- They are widely used to facilitate fraudulent and unlawful payments and to evade consumer protections and oversight.
- They are unnecessary in light of the wide availability of modern electronic payment systems.
- Their usefulness for a handful of legitimate uses is outweighed by their risks.
- A clean, complete ban will facilitate legal compliance.

Canada banned RCCs (calling them "tele-cheques") in 2004.[4] The National Association of Attorneys General called for their abolition in 2005.[5] In the last few years, the case for abolishing

[4] While there is no specific rule or law barring them, the Canadian Payments Authority, which operates Canada's payment clearing system, prohibits their use. Canadian Payments Authority, "Prohibition of Tele-Cheques in the Automated Clearing Settlement System" (June 1, 2003), *available at*

RCCs and RCPOs has become even more compelling as automated clearinghouse transactions are now available in situations where RCCs/RCPOs were being used, and the evidence of abuses of RCCs and RCPOs has become overwhelming. The FTC has compiled an impressive case against RCCs and RCPOs in its proposed TSR rule,[6] and we will elaborate further in a separate letter shortly.

2. In the Interim, RCC Warranties Should Be Extended to RCPOs, Regulation E Coverage Should Be Clarified, and Both RCCs and RCPOs Should be More Carefully Monitored,

While we believe that RCCs and RCPOs should be banned, we recognize that completely eliminating them from the payment system will take some time. In the interim, we support the proposal in this docket to amend Regulation CC to require originating banks to warrant the validity of RCPOs in the same manner as currently required for RCCs. We urge the CFPB to dispel any doubt that RCPOs are covered by Regulation E. The FRB should also require more monitoring of RCCs and RCPOs.

RCPOs are subject to all of the same dangers as RCCs, and originating banks should have the same responsibility to determine their validity. An originating bank that submits an RCPO to a receiving bank should be required to warrant the validity of the instrument and to indemnify the receiving bank if the item is unauthorized. Originating banks are in the best position to conduct due diligence as to their clients', and their clients' clients', use of RCPOs and to monitor return rates to ensure that the items are not being used for fraudulent or unlawful purposes.

It is essential, however, to make clear that such an amendment will not cast doubt on court or regulator determinations that RCPOs are also covered by the Electronic Fund Transfer Act (EFTA) and Regulation E.[7] That is, consumers should be permitted to exercise their rights under Regulation E, and the consumer's bank should be required to honor those rights and follow Regulation E, regardless of how the warranties operate among the banks that process the RCPO. Regulation E protections are especially important given that the UCC likely does not apply to items that were never in paper form.

---

http://www.cdnpay.ca/imis15/eng/Act_Rules/Automated_Clearing_Settlement_System_ACSS_Rules/eng/rul/policy_statement_telecheques.aspx.

[5] National Association of Attorneys General, Comment to the FRB Docket No. R-1226 (Proposed Amendment to Regulation CC/Remotely Created Checks) (May 9, 2005), available at http://www.federalreserve.gov/SECRS/2005/May/20050512/R-1226/R-1226_264_1.pdf; *see also* Oversight of Telemarketing Practices and the Credit Repair Organizations Act: Hearing Before the Senate Commerce, Science & Transp. Comm. (July 31, 2007) (testimony of Richard Johnson, Member of the Board of Directors, AARP, available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=b8655fb6-b7a3-457b-b675-69830dbea5ee

[6] Federal Trade Commission, Telemarketing Sales Rule Notice of Proposed Rulemaking, 16 CFR Part 310, RIN: 3084-AA98, 78 Fed. Reg. 41200 (July 9, 2013) ("FTC 2013 TSR Proposal").

[7] *See, e.g.,* Fed. Trade Comm'n v. Johnson, 2013 WL 800257 (D. Nev. Mar. 1, 2013) ("Persuasive is a notice issued by the Retail Payments Office of the Federal Reserve to financial institutions that it views transactions like the ones authorized by Elite Debit's protocol as 'electronically originated consumer payments [that] fall under the requirements of the Electronic Fund Transfer Act and Regulation E, not under check law.' (See dkt. no. 585–1 at 2.)").

We appreciate the FRB's statement in the proposal that coverage under Regulation CC does not preclude a determination that RCPOs are also "electronic fund transfers" (EFTs) covered under Regulation E.[8] We also support the way in which the FRB's proposal handled the issue – not by including RCPOs in the definition of remotely created check, but instead by including commentary stating that items that purport to be RCCs are subject to RCC warranties as if they were checks.[9]

In order to avoid any confusion, especially by courts that may not read the discussion in the proposed rule, we suggested that the Commentary be further amended to state explicitly that treating RCPOs as RCCs for warranty purposes does not preclude a finding that they are also subject to Regulation E. That is, at the end of Proposed Commentary Section 229.34-1, we propose the following additional language:

> The fact that an electronic image and information transferred as an electronic collection item is treated as a check for these purposes does not preclude a finding that an item that was not derived from a paper check is an electronic fund transfer subject to Regulation E.

Similarly, at the end of Proposed Commentary Section 229.34(c)-5, we propose the following additional language:

> The fact that an electronic image and information transferred as an electronic collection item is subject to the warranties for a remotely created check does not preclude a finding that an item that was not derived from a paper check is an electronic fund transfer subject to Regulation E.

Alternatively, commentary could be added to the definition of RCCs to make clear that RCPOs are not checks or RCCs. We fear that, absent such clear language in the Commentary, a court might mistakenly conclude that RCPOs should be treated as checks not only for warranty purposes but for Regulation E purposes as well. This clarification is especially important because it may not be obvious to all courts that the definition of "remotely created checks" in Regulation CC requires that the check be reduced to paper form.[10]

More directly, the CFPB should make clear – through a Bulletin, revised Commentary, or in some other fashion – that RCPOs are covered by Regulation E. An examination of Regulation E plainly leads to that conclusion. RCPOs are a transfer of funds initiated through a computer. 12 C.F.R. § 1005.3(b)(1). Because they were never reduced to paper form, they do not fall under the

[8] 76 Fed. Reg. at 16866.

[9] Proposed Commentary Sections 229.34-1, 229.34(c)-5.

[10] Regulation CC defines a "remotely created check" as "a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn." 12 C.F.R. § 229.2(fff). "Check," in turn, is defined to include a "demand draft" – a term that is not defined in Regulation CC – including a demand draft that is not negotiable. 12 C.F.R. § 229.2(k), (k)(7).

Regulation E exclusion for payments that originated "by check, draft, or similar paper instrument." *Id.* § 1005.3(c)(1). One court has already held that RCPOs are covered by Regulation E.[11]

Nonetheless, regulators have expressed uncertainty about Regulation E coverage.[12] RCPOs are processed through the check system and are indistinguishable from RCCs, leading to potential confusion about their treatment.

While a CFPB determination is not necessary to Regulation E coverage where an item clearly falls within the scope of the regulation, to avoid any misunderstanding, the CFPB should state explicitly that RCPOs are covered by Regulation E. Entities that take advantage of the efficiencies of electronically processed payments should be required to provide the consumer protections adopted for electronic fund transfers, especially as the UCC likely does not cover electronic items.

Pending eventual action to eliminate RCCs and RCPOs from the payment system, the FRB should also take more concrete steps to require payees and originating banks to monitor the use of RCCs and RCPOs. The Federal Reserve Bank of Atlanta, for example, has suggested requiring "every bank to collect and report to its primary federal regulator on a frequent basis each instance in which any of its customers deposited significant numbers of checks that resulted in an abnormal number or rate of returns."[13] Methods could also be developed to distinguish RCCs and RCPOs from traditional paper checks. More extensive monitoring of RCCs and RCPOs will both reduce misuse and also yield information crucial to further regulatory efforts.

3. Electronically "Signed" Images Should Be Treated the Same as RCCs and RCPOs

The 2011 proposal describes a new form of RCC or RCPO:

> [T]he drawer's bank (the paying bank) might supply a smart-phone application through which the drawer is able to execute a "handwritten" signature on the phone's screen, and through which the signature is attached to an electronic "check" that the drawer sends via the Internet to the payee, for the payee's subsequent electronic deposit with its bank.[14]

This possibility is even more likely two years later with the spread of tablets, laptops and desktop computers that have touch screens.

An item with such a "handwritten" signature might arguably fall outside the Regulation CC definition of "remotely created check." One could argue that the item does "bear a signature

---

[11] *See* Fed. Trade Comm'n v. Johnson, 2013 WL 800257 (D. Nev. Mar. 1, 2013).

[12] The FRB's 2011 Regulation CC proposal referred to a possible "future" determination that RCPOs are subject to Regulation E. 76 Fed. Reg. at 16866; *see also* FTC 2013 TSR Proposal, 78 Fed. Reg. at 41205 & n. 61(noting that the CFPB "has not yet determined whether such electronically-created items not derived from checks are electronic fund transfers subject to Regulation E"); Comments of Federal Reserve Bank of Atlanta to FTC re Telemarketing Sales Rule at 2 (Aug. 8, 2013) ("FRB of Atlanta TSR Comments") ("We, similar to the Commission, recognize the lack of clarity around the legal framework governing RCPOs and the various implications that result should consumer RCPOs definitively become subject to the EFTA.")

[13] FRB of Atlanta TSR Comments at 4.

[14] 76 Fed. Reg. at 16865.

applied, or purported to be applied" by the drawer. Although the creator of the check, not the consumer, applied the printed electronic signature to the original paper check, once the item is imaged, it may appear to have a signature that purports to have been applied by the drawer. However, like a traditional remotely created check, the original check does not have an original signature.

It would be tempting to conclude that an item that was created after the consumer supplied a handwritten signature, albeit electronically, does not bear the same dangers as RCCs and RCPOs. But with advancing technology, obtaining that electronic signature, and applying it repeatedly to new items, could be as easy and deceptive as obtaining authorization (or purported authorization) to create an RCC or RCPO. As the Federal Reserve Bank of Atlanta recently commented: "Defrauders might evade the coverage of the [Federal Trade] Commission's prohibition on RCCs simply by issuing payment orders that bear a signature instead of a printed legend."[15] A consumer could be required to sign a payday loan agreement or other agreement, or to upload a handwritten signature, as part of an electronic transaction. Then the fine print of the contract would permit the lender to use that signature to create a RCC or RCPO. A consumer could be induced to "sign" in much the same way that consumers are induced to click "I agree" when they do not understand the full scope of the agreement. Any items that are created remotely using that signature by an entity other than the paying bank are subject to the same abuses and dangers of RCCs and RCPOs.

Moreover, it is hard to envision situations in which such electronically signed checks would be any more necessary or useful than RCCs or RCPOs. The ACH system and the card networks can substitute for RCCs and RCPOs, with much lower risks, in virtually every circumstance where those items are legitimately used today. The same is likely to be true of any new situation in which electronically signed checks might be used. PayPal, various P2P systems, and other newer payment systems can be used to transmit funds to persons and small businesses that are not equipped to accept electronic payments or cards directly.[16] It would defeat the purpose of banning or regulating RCCs and RCPOs if those rules could be evaded by substituting another item that escapes the scrutiny and protections of the electronic payment system as well as the rules that govern RCCs and RCPOs.

Similarly, as the FTC explained in its proposed TSR rule, the consumer protections and systemic monitoring of items transmitted through the check system are inferior to those for electronic payments processed through the ACH system and card networks. Merchants who wish to take advantage of the speed and convenience of electronic payments should have to extend the consumer protections that electronic payments receive. They should not have it both ways, benefiting from electronic processes but depriving consumers of appropriate protections.

Consequently, we believe that items that contain an electronically handwritten signature should be treated the same as RCCs and RCPOs – ideally banned, and in the interim, subject to the

[15] FRB of Atlanta TSR Comments at 2.

[16] Checks generated by a consumer when bills are paid through a bank bill payment feature are created by the consumer's bank and thus do not meet the definition of an RCC or RCPO.

same warranties. Just as the FRB explained with RCPOs, originating banks are in the best position to monitor returns and to ensure that their clients do not misuse such items.

In order to ensure that electronically signed, remotely created items are subject to the RCC warranties, either the definition of "remotely created check" in Regulation CC, or the Commentary to that definition or elsewhere, should be amended to make clear that an item that holds an electronic rather than an original signature falls within the definition of an RCC. If the item was never reduced to paper, then it should fall within the treatment of electronically created items discussed elsewhere in these comments.

If there is any question that electronically signed items deserve different treatment from RCCs, we ask for the opportunity for further discussion and comment, along with consideration of how to ensure that such items are not used to replicate the problems of RCCs and RCPOs.

4. Consumers Should Have Prompt Access to Funds Deposited By Remote Deposit Capture

The FRB proposes to amend the definition of "automated teller machine" to exclude mobile devices or computers at which consumers may take or upload a picture of the check through a process known as "remote deposit capture" (RDC). The proposal requires that an ATM be able to accept deposits of actual paper checks and cash in order to be considered an ATM.

The FRB did not explain the purpose of this amendment or its implications. But excluding RDC from the ATM definition creates an ambiguity as to whether and how the funds availability schedule applies to RDC deposits. Thus, it is not clear when those funds must be made available to consumers.

Whether by including RDC in the definition of ATM, or by clarifying the treatment of RDC separately, the CFPB and FRB must ensure that consumers who deposit funds by RDC have prompt access to those funds. Consumers are being hit with a barrage of advertising promoting RDC. They should not be steered to a method that results in a delay in access to their money.

We generally believe that consumers should have access to funds deposited by RDC on the same schedule as for deposits at the bank's ATMs. A check deposited by RDC is done so through an app or website provided by the consumer's bank and is transmitted immediately.

However, we recognize that RDC deposits present fraud concerns. If – and only if – necessary to address serious fraud risks, RDC deposits could be subject to a one day delay in funds availability from the schedule required for deposits at proprietary ATMs. As experience with RDC grows and fraud prevention techniques improve, hopefully any delay can be eliminated.

5. Checks Deposited to Prepaid Cards Should be Covered under the Expedited Funds Availability Act

In order to maintain the integrity of the expedited funds schedule and to reflect other technological developments, we also urge the FRB to amend Regulation CC to clarify that the expedited funds schedule applies to checks deposited onto prepaid cards. The consumers who use prepaid cards tend to be lower income or credit-challenged consumers who especially need prompt access to their funds.

It is presently unclear whether prepaid card accounts are considered to be "accounts" within the meaning of Regulation CC.[17] Regulation CC relies on Regulation D's definition of "transaction account."[18] The wording of that definition appears broad enough to encompass prepaid cards, even if the funds are held in subaccounts under a master account that is not in the consumer's name. However, Regulation D has broader purposes, such as determining capitalization requirements, which could lead to double counting if both the master account and subaccount were considered to be accounts. Moreover, Regulation CC applies to "banks,"[19] and not all prepaid cards are issued by depository institutions.

At least one prepaid card issuer, American Express, applies a lengthy 10-day hold time to checks deposited onto its Bluebird prepaid cards. JP Morgan Chase, on the other hand, appears to apply the regular EFAA hold times to checks deposited onto its Liquid card. Whether such differences are due to the fact that Bluebird is not offered through American Express's bank, or that its deposits are entirely through RDC rather than through ATMs, is not clear. This distinction creates an unlevel playing field and unequal protections for users of different cards.

While RDC deposits may warrant slightly different treatment from ATM deposits, as discussed above, we do not believe that holders of prepaid card accounts should be treated any differently from consumers who hold traditional bank accounts. Hold times for deposited funds should be determined by the type and manner of deposit as set forth in Regulation CC, not by the type of underlying account. We see no regulatory or practical reason to treat deposits to prepaid cards any differently than deposits to bank accounts, and the policy reasons for giving prepaid card consumers prompt access to their funds are compelling. We ask that the FRB and CFPB clarify Regulation CC to include prepaid card accounts in the "accounts" protected by the EFAA and implementing regulations.

6. Consumers Should Receive Better Information to Prevent Check Scams

We appreciate the effort to improve the notices that consumers receive about funds availability policies. However, the proposed notices fail to address a crucial issue about the distinction between funds availability and check clearing. We ask that the CFPB and the FRB study

[17] 12 C.F.R. § 220.2(a).
[18] 12 C.F.R. § 204.2(e).
[19] 12 C.F.R. § 229.2(e).

ways to inform consumers that a check may still bounce even after the funds are made available, and that, if the check is returned, the consumer will be responsible for any funds that have been withdrawn.

Fake check scams were the top consumer scam reported in 2012 to the National Consumer League's fraud complaint site.[20] The scams rely on the distinction between fund availability and the full clearing of a check to induce consumers to cash and draw on fraudulent checks that are subsequently returned. Common examples of these scams are the Nigerian check scam and the counterfeit check scam involving an overpayment for an item the consumer is selling.[21] These scams also take advantage of the fact that many consumers are unaware that they can be held liable for funds that they are permitted to withdraw against checks that later bounce.

In 2008, to support a public education campaign about fake check scams, Consumer Federation of America commissioned a consumer survey on understanding of check cashing rules. The study revealed that 59 percent of the respondents believed that financial institutions confirm that a check is good before allowing the funds to be withdrawn, and 39 percent thought that if they deposited a check and withdrew some of the funds, and it was later discovered that the check was phony, the person who gave it to them would be responsible to pay the money back to their financial institution.[22]

The funds availability notices should inform consumers that a check could still be returned even if funds are made available. Consumers should be told how to determine when a check will have fully cleared. Furthermore, the notice should make clear that consumers will be responsible for any funds that are withdrawn against a deposit that is reversed.

Better information about the distinction between check hold times and the full clearing of a check should be communicated not only in notices to consumers but also through improved teller information and training. For example, one of the writers of these comments recently attempted to determine if a deposited check had fully cleared. Neither the bank's customer service representatives, nor a supervisor, understood the distinction between funds availability and check clearing and could not answer if or when the check had been paid by the originating bank.

Fake check scams continue to be a problem for consumers. Improving consumer understanding of the check clearing process could help avoid some of these scams. It would also make consumers more cautious about other situations in which they might be asked to cash a check, such as when a friend or acquaintance asks them to do so as a favor.

---

[20] National Consumers League, "Familiar Faces in 2012 Top Scams Report," available at http://www.nclnet.org/personal-finance/64-fraud/769-familiar-faces-in-2012-top-ten-scams-report.

[21] These scams are described in the recent comments of Vermont Assistant Attorney General Eliot Burg, on behalf of several attorneys general, to the Federal Trade Commission on the Telemarketing Sales Rule, 16 CFR Part 10, Project No. R411001 (Aug. 8, 2013), available at http://ftc.gov/os/comments/tsrantifraudnprm/00035-86301.pdf

[22] *See* Consumer Federation of America, "Tear Up" Fake Check Scams (May 2009), available at http://www.consumerfed.org/elements/www.consumerfed.org/file/CFA%20Fake%20Check%20Scams%20Fact%20Sheet.pdf.

* * *

Thank you for the opportunity to submit these comments. Please contact Lauren Saunders at lsaunders@nclc.org, (202) 595-7845, or Laura Udis at ludis@consumerfed.org, 202-939-1004, if you have any questions.

Yours very truly,

National Consumer Law Center (on behalf of its low income clients)
Consumer Action
Consumer Federation of America
Consumers Union, the policy and advocacy arm of *Consumer Reports*
National Association of Consumer Advocates
National Consumers League

Attachment: Descriptions of Commenters

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. A nonprofit 501(c)3 organization, 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.

Consumers Union is the public policy and advocacy division of Consumer Reports. Consumers Union works for telecommunications reform, health reform, food and product safety, financial reform, and other consumer issues. Consumer Reports is the world's largest independent product-testing organization. Using its more than 50 labs, auto test center, and survey research center, the nonprofit rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 8 million subscribers to its magazine, website, and other publications.

The **National Association of Consumer Advocates** (NACA) is a non-profit corporation whose members are private and public sector attorneys, legal services attorneys, law professors, and law students, whose primary focus involves the protection and representation of consumers. NACA's mission is to promote justice for all consumers.

National Consumers League, founded in 1899, is the nation's pioneering consumer organization. Our non-profit mission is to protect and promote social and economic justice for consumers and workers in the United States and abroad.

Exhibit 4

Comments of NCLC et al. to Federal Reserve Board on Regulatory Publication and Review Under the Economic Growth and Regulatory Paperwork Reduction Act of 1996, FRB Docket No. R–1510, Regulation II (March 22, 2016)

Comments of

Americans for Financial Reform
Arkansans Against Abusive Payday Lending
Consumer Action
Consumer Federation of America
Mark Budnitz, Professor of Law, emeritus, Georgia State College of Law
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low income clients)
Public Justice Center (Baltimore)
Reinvestment Partners
Woodstock Institute

submitted to the
Federal Reserve Board

Regulatory Publication and Review
Under the Economic Growth and
Regulatory Paperwork Reduction Act of 1996

FRB Docket No. R–1510

Regulation II (interchange fees and prepaid cards)
12 CFR Part 235

March 22, 2016

The undersigned consumer organizations and legal experts submit these comments on improvements needed to modernize Regulation II regarding debit card interchange fees.[1] We urge the Federal Reserve Board (FRB) to revisit the unnecessary limitations on the prepaid card accounts that are eligible for an exemption from Regulation II. As a result of Regulation II, many prepaid card accounts offered by larger financial institutions do not permit links to savings accounts or access to the bank's online bill payment page, features that are especially important for consumers who lack access to safe bank accounts. With the CFPB about to finalize rules to define prepaid accounts and cover those accounts under Regulation E, the FRB should adopt the CFPB's definition and eliminate the Regulation II limitations that restrict prepaid cards to second class accounts.

Regulation II implements the "Durbin Amendment" to the Dodd-Frank Wall Street Reform and Consumer Protection Act. The Durbin Amendment caps the interchange fees that may be charged on debit cards issued by financial institutions with assets over $10 billion. However, in order to protect the availability of prepaid cards for lower income consumers, the statute has an exemption for prepaid cards. That is, the interchange fees on prepaid cards are not limited as long as they meet two conditions in the statute: They may not charge overdraft fees, and they must provide at least one free ATM withdrawal per month.

[1] Organizational descriptions are attached at the end of these comments.

Like the statute, Regulation II exempts prepaid cards that meet certain conditions. Two of these conditions are in the statute: no overdraft fees and one free ATM withdrawal. However, the regulation adds another condition not in the statute: the card must be the sole means of accessing the account. That is, the funds on the prepaid account may not be accessible in any other way, such as by transferring funds to a savings account, by using the bank's online bill payment feature, or through money orders or pre-funded checks that come with the account.[2] These limitations were not in the proposed rule and were adopted in the final rule without any opportunity for notice or comment.

The Regulation II conditions on the prepaid card exemption inhibit the functionality of accounts intended for consumers who need that functionality the most. These consumers are not allowed to link savings accounts to their prepaid cards or to participate in automated savings programs. They cannot use a prepaid card's online bill payment feature or a pre-funded check to pay landlords who do not accept cards. They also cannot use their prepaid accounts to send money to family members.

The FRB adopted these limitations in order to prevent evasions of the interchange fee rules. However, the limitations are not necessary to prevent evasions, because none of the prohibited functions (bill payment, transfers to savings, person-to-person transfers) generates interchange fees. Ironically, Regulation II permits banks to allow consumers to transfer funds from an interchange fee-capped debit card account and spend those funds through an uncapped prepaid card – which could be a form of evasion. Yet banks cannot permit consumers to spend or access prepaid card funds through methods that would be very useful for lower income consumers and that do ***not*** generate interchange fees.

Because of the perverse incentives created by Regulation II, many major banks do not offer fully featured prepaid card accounts. The prepaid cards offered by larger banks mostly have limited functionality. For example, the BBVA Compass ClearSpend Card, the Commerce Bank mySpending Card, the PNC SmartAccess Prepaid Visa Card, the Regions Now Visa prepaid Card, the TD Bank Connect Reloadable Card, the U.S. Bank Convenient Cash Card, and the Wells Fargo Prepaid Card all lack online bill payment on the bank's website or the capacity to make transfers to a savings account.[3]

These accounts lack the features that smaller banks like Green Dot Bank and MetaBank can offer. The Regulation II limitations may become even more problematic if major prepaid card issuing banks grow large enough to be covered by the regulation.

The profit margins on general use reloadable prepaid cards are quite thin. Prepaid card users who use the prepaid accounts as checking account substitutes have lower incomes than the general population and are more likely than checking account holders to earn less than $25,000.[4] Prepaid accounts tend to

[2] A pre-funded check is a check that may not be used until the consumer contacts the financial institution and segregates the funds necessary to cover that check. Once activated, a pre-funded check is essentially a money order.

[3] Source: Survey by the Center for Financial Services Innovation (CFSI), conducted for Thea Garon, James Latta, CFSI, 2016 Prepaid Industry Scorecard (March 15, 2016), available at http://www.cfsinnovation.com/Document-Library/2016-Prepaid-Scorecard.

[4] Pew Charitable Trusts, "Why Americans Use Prepaid Cards" at 3-4 (Feb. 2014), http://www.pewstates.org/uploadedFiles/PCS_Assets/2014/Prepaid-Cards-Survey-Report.pdf. The vast majority of new Chase Liquid customers had no bureau score or a score below 660 when they opened their Chase Liquid accounts. Presentation by Jon Wilk, Chase, to FDIC Committee on Economic Inclusion, http://www.fdic.gov/about/comein/2013/2013-05-16_presentation_wilk.pdf.

have a shorter life than checking accounts. Full interchange revenue may be critical to making these accounts viable and to encourage more banks to offer them.

Banks' inability to generate more interchange revenue on fully functional prepaid accounts may be contributing to the lack of those accounts or banks' failure to aggressively market them.[5] In a recent review by the Consumer Financial Protection Bureau of the top retail banking websites, the CFPB found that nearly half do not appear to offer any deposit account that ensures consumers cannot overdraft.[6] The CFPB also expressed concerned that, even when banks have no-overdraft accounts available, the accounts are not marketed prominently and consumers may not know about them.[7]

The only functionality limits that a prepaid card account should have in order to be exempt from Regulation II are those directly related to the inherent nature of a prepaid card and the overdraft fee ban in the statute. In other words, the account should not have overdraft fees, nonsufficient funds fees, or checks that can bounce. However, pre-funded checks (which effectively become money orders) should be permitted. Distinguishing prepaid cards from checking accounts based on the presence or lack of checks and overdraft fees is consistent with the statute as well as the defining difference between checking and prepaid card accounts.

Thus, the FRB should re-define "prepaid card" in Regulation II as any account that:

- Is offered through a master-subaccount arrangement;
- Is covered by the CFPB's prepaid card rules;
- Lacks overdraft and nonsufficient funds fees; and
- Does not have un-funded checks.

If the FRB still fears evasions, it could put a cap on the amount of regular direct deposits or average balance that an exempt prepaid card account may have in order to prevent the exemption from covering accounts used as bank accounts by wealthier individuals.[8] The FRB could also prevent evasions by prohibiting financial institutions that allow funds to be transferred from an account with capped interchange from offering rewards for spending on prepaid accounts.

Policymakers across the country are working to promote financial inclusion of the millions of underserved consumers. The FRB should eliminate the outdated and burdensome restrictions on prepaid accounts that hinder those efforts at inclusion.

---

[5] While Chase recently gave up its Durbin exemption in order to offer more features on its Liquid Card, the bank suffered a heavy cost when doing so. Chase may be less likely to promote its prepaid card account when it can make so much more money off putting a subprime consumer into a traditional checking account where the consumer may incur overdraft fees.

[6] CFPB, Press Release, "Consumer Financial Protection Bureau Takes Steps To Improve Checking Account Access" (Feb. 3, 2016), http://www.consumerfinance.gov/newsroom/cfpb-takes-steps-to-improve-checking-account-access/.

[7] *Id.*

[8] The FRB should permit occasional exceptions in order to permit lower income consumers to receive tax refunds, back payments of public benefits, and other one-time payments. The consumer could be required to spend those funds or transfer them to another account within a reasonable period of time.

If you have any questions, please contact Lauren Saunders at the National Consumer Law Center, (202) 595-7845, lsaunders@nclc.org. Thank you for considering these comments.

Respectfully submitted,

Americans for Financial Reform
Arkansans Against Abusive Payday Lending
Consumer Action
Consumer Federation of America
Mark Budnitz, Professor of Law, emeritus, Georgia State College of Law
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low income clients)
Public Justice Center (Baltimore)
Reinvestment Partners
Woodstock Institute

Attachment: Organizational Descriptions

Americans for Financial Reform is an unprecedented coalition of over 250 national, state and local groups who have come together to reform the financial industry. Members of our coalition include consumer, civil rights, investor, retiree, community, labor, faith based and business groups.

Arkansans Against Abusive Payday Lending is a broad-based coalition of non-profit, consumer, community, civic, military and faith-based organizations dedicated to ridding our community of the abuses of payday lending. Payday lending tends to prey on low-to-moderate income families, college students, military personnel and the elderly.

Consumer Action has been a champion of underrepresented consumers since 1971. A national, nonprofit 501(c)3 organization, 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 particularly in the fields of consumer protection, credit, banking, housing, privacy, insurance and utilities. www.consumer-action.org

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.

Since 1969, the nonprofit **National Consumer Law Center® (NCLC®)** has worked for consumer justice and economic security for low-income and other disadvantaged people, including older adults, in the U.S. through its expertise in policy analysis and advocacy, publications, litigation, expert witness services, and training.

The **Public Justice Center** works with people and communities to confront the laws, practices, and institutions that cause injustice, poverty, and discrimination. We advocate in the courts, legislatures, and government agencies, educate the public, and build coalitions, all to advance our mission of "pursuing systemic change to build a just society."

The **Reinvestment Partners'** mission is to advocate for economic justice and opportunity. We advocate for change in the lending practices of financial institutions to promote wealth building of underserved communities and to end predatory lending practices that strip wealth.

Woodstock Institute is a leading nonprofit research and policy organization in the areas of fair lending, wealth creation, and financial systems reform. Woodstock Institute works locally and nationally to create a financial system in which lower-wealth persons and communities of color can safely borrow, save, and build wealth so that they can achieve economic security and community prosperity. Our key tools include: applied research; policy development; coalition building; and technical assistance. Woodstock Institute has been a recognized economic justice leader and bridge-builder between communities and policymakers in this field since it was founded in 1973 near Woodstock, Illinois. Now based in Chicago, we work with community and philanthropic groups, financial institutions, and policymakers. Funded by foundation grants, consulting fees, and charitable donations, we conduct research on financial products and practices, promote effective state and federal policies, convene a coalition of community investment stakeholders working to improve access to credit, and help people use our work to understand the issues and develop and implement solutions.