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.