Comments
to the
Federal Trade Commission
16 CFR Parts 310
[RIN 3084-AA98]
Telemarketing Sales Rule
Project No. R411001
(Remotely Created Checks and Other Items)
78 Fed. Reg. 41200 (July 9, 2013)

by the National Consumer Law Center
on behalf of its low-income clients
and
Center for Responsible Lending
Consumer Action
Consumer Federation of America
Consumers Union, the Advocacy and Policy Arm of Consumer Reports
National Association of Consumer Advocates
National Consumers League
U.S. PIRG

Submitted August 2, 2013

I. Introduction

The National Consumer Law Center (on behalf of its low income clients), the Center for Responsible Lending, Consumer Action, Consumer Federation of America, Consumers Union, the Advocacy and Policy Arm of Consumer Reports, National Association of Consumer Advocates, National Consumers League and U.S. PIRG appreciate this opportunity to submit comments to the Federal Trade Commission (FTC) on the proposed amendments to the Telemarketing Sales Rules ("TSR").[1] We applaud the FTC for proposing well-documented and thoroughly justified proposed rule changes. The prefatory material to the Proposed Rule identifies and illustrates the necessity for these changes, which are essential to protect consumers from fraud.

We support all of the proposals, which address fraudulent transactions that plague numerous consumers whom our organizations represent or serve. The well-justified ban on use of remotely created checks, remotely created payment orders, cash-to-cash money transfers and prepaid card reload packs as payment mechanisms by telemarketers and sellers will have little to no impact on legitimate businesses. We agree that advance fees should not be charged for purportedly recovering lost money or prizes, regardless whether the consumer's initial loss was incurred in a telemarketing transaction or one on the internet. The clarifications of the TSR and rules governing the Do Not Call Registry will be helpful to prevent evasions of those important consumer protections.

[1] Organizational descriptions are attached as an appendix. These comments were written by Lauren Saunders, Margot Saunders and Andrew Pizor of the National Consumer Law Center and Susan Grant and Jean Ann Fox at the Consumer Federation of America.

We also recommend these enhancements to ensure that the ban on the four payment systems is effectively enforced:

- The FTC should work with other regulators to completely ban remotely created checks (RCCs) and remotely created payment orders (RPCOs) in all consumer transactions.
- Originating banks and payment processors should be strictly liable for processing RCCs or RCPOs; the FTC should not be required to prove knowledge of a violation.
- Strict liability may also be appropriate for money transmitters, and both money transmitters and cash reload systems should also be responsible when there are patterns of misuse.
- Scams initiated by email or other methods should also be covered by the ban on the four payment systems.

Finally, we ask the FTC to open up a broader rulemaking to address other improvements needed to the Telemarketing Sales Rule. The rule is in need of significant updates in other areas to stop fraudulent and unfair practices aimed at consumers. In particular:

- *Negative option billing.* Consumers are routinely defrauded when they do not realize that they have purportedly agreed to have goods or services (that they may not even want) sent to them automatically, placing the burden on them to either pay for the items or return them.
- *Selling personal financial information to third parties.* Businesses should be banned from selling personal financial account information to third parties.
- *Upselling.* The FTC should address a number of unscrupulous upselling practices that induce consumers to purchase items they do not want.
- *Debt relief***.** The FTC should strengthen the regulation of debt relief services to address abuses and evasions that have become problematic since the rules were issued.
- *Mandatory arbitration and class action bans.* The FTC should ban pre-dispute binding mandatory arbitration ("forced arbitration") clauses and class action bans in transactions under the TSR. Scammers routinely violate the law, consumers cannot get adequate relief through forced arbitration, and the FTC cannot protect every consumer.

Our comments focus on the principal proposed amendments banning the four payment mechanisms in telemarketing sales. We address the other items more briefly.

II. Consumers Need To Be Fully Protected From The Harms Caused By All Four Payment Mechanisms

A. RCCs and RCPOs Should be Banned for All Consumer Purposes

We strongly support the FTC's proposed prohibition of all four methods of payments for telemarketing transactions. (Proposed §§ 310.4(a)(9) and (10).) As the FTC extensively explained in this Proposed Rulemaking, all four payment systems -- remotely created checks (RCCs), remotely created payment orders (RCPOs), cash-to-cash transfers and cash reload systems -- are often used by scammers in telemarketing frauds.

However, the FTC's compelling case against RCCs and RCPOs is not limited to telemarketing sales. These payment mechanisms are also prime instruments for unauthorized withdrawals by purely internet-based scams, online and storefront payday lenders,[2] lead generators, and others. The FTC should work with the Consumer Financial Protection Bureau, the Federal Reserve Bank, and the other bank regulators to ban RCCs and RCPOs in all consumer transactions.[3]

Both RCCs and RCPOs work by obtaining the consumer's bank account number and routing number to create an item that is processed through the check clearing networks. The payee obtains or purports to obtain the consumer's advance permission to have money taken from the consumer's checking account to pay money to that payee. The payee need only be armed with the consumer's bank account number and the bank's routing number, which is included in the magnetic ink character recognition (MICR) numbers on the bottom of the check or is included in completed online loan applications from consumers seeking payday or installment loans directly from lenders or via marketing websites.

The RCC or RCPO may be created by the payee or anyone else with the right software. Once the payee obtains the relevant information, it can use desktop publishing technology to produce a check with the account information encoded on the bottom as though it were the customer's own check. Most commonly, the RCC or RCPO is created by a third party payment processor. The processor generates a draft bearing the MICR numbers and deposits the draft in the processor's bank.

The payee may obtain the consumer's bank account information in a variety of ways. 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.[4] Some credit card finders use their service to discover the consumer's checking account number and then electronically take money out of that account.[5] The same is the case with credit repair organizations[6] and companies that promise, for a fee, to find the consumer unused scholarships and grants.[7]

Other scam operators ask for a checking account number to pay for specified services, but then take money out of the account without providing the services and without authorization.[8] A fraudulent company may obtain the consumer's authorization for one payment and use it to keep

---

[2] *See* Federal Trade Comm'n v. Direct Benefits Group, L.L.C. (M.D. Fla. July 18, 2011) (complaint filed), *available at* http://www.ftc.gov/os/caselist/1123114/. Storefront payday lenders may also include language in their agreements authorizing creation of an RCC in the event that the original check is stopped or rejected.

[3] The CFPB has authority to ban the devices under its authority to prevent unfair, deceptive and abusive practices. The FRB has the authority under its Regulation CC authority over the check system. Our experience is limited to consumer transactions, but we are unaware of any legitimate use of RCCs and RCPOs that justifies their risk, even for business purposes. Moreover, as the FTC has found in the context of the Do Not Call list, exceptions for business purposes have a tendency to be exploited and to result in impacts on consumers as well.

[4] *See, e.g.,* Proposed Consent Decree, Federal Trade Comm'n v. Windward Mktg., Ltd., 5 Trade Reg. Rep. (CCH) ¶ 24,223 (N.D. Ga. 1997); Consent Order, Windward Mktg., Inc., 5 Trade Reg. Rep. (CCH) ¶ 24,060 (June 21, 1996) (FTC File No. X96 0026).

[5] *See* Federal Trade Comm'n v. Mandy Enters., Inc., 5 Trade Reg. Rep. (CCH) ¶ 23,181 (D.S.C. 1992).

[6] *See* Proposed Consent Decree, Federal Trade Comm'n v. Ellis, 5 Trade Reg. Rep. (CCH) ¶ 24,179 (C.D. Cal. 1996).

[7] *See* Proposed Consent Decree, Federal Trade Comm'n v. Student Aid Inc., 5 Trade Reg. Rep. (CCH) ¶ 24,312 (S.D.N.Y. 1997).

[8] *See* Proposed Consent Decree, Federal Trade Comm'n v. Regency Serv., Inc., 5 Trade Reg. Rep. (CCH) ¶ 24,219 (M.D. Fla. 1997).

presenting drafts month after month. Alternatively, the company may use the draft to obtain more money than authorized.

These exact same scenarios also occur in purely internet-based transactions and others outside the current scope of the TSR. A telephone call is not a necessary element of the scams. Sometimes the authorization is buried in fine print; sometimes the consumer did not realize that she was agreeing to purchase an item or service; sometimes the consumer provided no authorization at all.

For example, one of the FTC's recent cases involving RCPOs involved consumers who applied online for a payday loan and whose information was used by another party to make unauthorized withdrawals.[9] Purely online payday loans are not covered by the TSR. And the scammer who makes an unauthorized debit after obtaining the consumer's account information may have had no contact whatsoever with the consumer, by telephone or otherwise.

RCCs are used by internet payday lenders who operate in states where their loans are illegal or where the lenders are unlicensed. There is also a growing problem of lenders who claim to be affiliated with Native American tribes and to be completely exempt from state and federal laws. The consumer's authorization for the payment or fees is questionable if the contract itself is unlawful, but the check clearing system does not provide a good way for the consumer to raise disputes or for the system to monitor lenders who are consistently operating in an illegal fashion.

All types of payday lenders also use RCCs to defeat the consumer's options and ensure control over the consumer's bank account. Storefront payday lenders may bury authorization to create an RCC in the fine print of the loan agreement, which enables the lender to create a new check if the consumer stops payment of the first one or if the lender wishes to charge the consumer a late fee or another amount not covered by the original check. Internet payday and installment lenders use RCCs if the consumer exercises her right to withdraw authorization for or stop payment of an electronic funds transfer.[10]

Whatever the context, the use of RCCs and RCPOs is popular for scammers because the consumer protections are weak and poorly enforced compared to the stronger protections for electronic fund transfers, debit cards and credit cards.[11] Compared to the protections of Regulations E and Z, the UCC does not provide the same caps on liability for unauthorized charges, right of recredit, or clear error resolution procedures. Disputing an unauthorized check takes much more

---

[9] *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.).

[10] www.GreatPlainsLending.com Consumer Loan Agreement, dated 8/24/12, "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." On file with CFA.

[11] *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.

time and expense than disputing an unauthorized electronic transaction or debit or credit card charge.

RCCs and RCPOs can also be used by scammers to exploit weaknesses in the check system that make it difficult for the consumer's bank to honor stop payment orders. 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 a check number for an RCC or RCPO, and scammers frequently manipulate the amount of the check – adding or subtracting a few cents or breaking up a transaction into more than one check.

In the current rulemaking, the FTC has articulated specifically and carefully why using RCCs and RCPOs is abusive and causes substantial consumer economic injury which cannot be reasonably avoided.[12] The Commission points out repeatedly 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,

> [t]hese alternatives offer both dispute resolution rights and protections against unlimited liability for unauthorized charge to consumers and are available to consumers who do not possess or do not wish to use credit cards.[13]

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 just issued a bulletin intended to prevent misuse of the ACH network by those who would re-present payments that have been stopped. The bulletin makes clear that, 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.[14] Any modification of the amount of the payment or any other change in an attempt to make the payment appear as a new entry is also a violation of the NACHA Rules.[15] There are no similar rules that prevent a scammer from creating an RCC or RCPO if a check or ACH payment has been stopped or rejected. The consumer would have to contest the authorization using common law contract and agency law principles and the outcome might be uncertain.

Indeed, some payment processors promote their RCC services for the very purpose of evading the strong legal protections for other payment methods. For example, CheckWriter states that a benefit of using its check drafting software program is not being covered by "strict ACH regulations published by N.A.C.H.A."[16] ACH Check Solutions lists as a benefit of accepting echecks

---

[12] *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.

[13] 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.

[14] NACHA, ACH Operations Bulletin #3-2013, "Reinitiation of Returned Debit Entries" (July 15, 2013), available at https://www.nacha.org/OpsBulletins.

[15] *Id.*

[16] 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."

that "ACH Rules do not apply – Echeck Services are not governed by NACHA!"[17] The extensive list of eCheck Merchant Accounts business types accepted by this company include gambling advice, psychic readings, pyramid sales, terminated merchants, pawn brokers, bail bondsmen, debt reduction, and loan modification.[18] 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."[19]

RCCs and RCPOs are also used by entities who wish to escape scrutiny by the systems used to detect fraud in other payment systems. Scammers may use RCCs and RCPOs after NACHA has banned them from the ACH system or in order to avoid NACHA's enforcement mechanisms.[20] The networks that handle credit and debit cards also have much more robust fraud detection mechanisms than the check system.

Consumers cannot protect themselves from the dangers of RCCs and RCPOs. The same information -- bank account and routing number – is used to create an electronic fund transfer, RCC or RCPO, but the consumer has no way of knowing how the payment will be processed and no effective control over how the payee processes the payments. Consumers also do not understand the different levels of protection for different types of payments.

For almost a decade, many regulators and advocates have called for the banning of RCCs, arguing 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.[21] Amid concerns over the high potential for fraud, Canada prohibited RCCs (calling them "tele-cheques") in 2004.[22] In 2005, the attorneys general of thirty-five states, the District of Columbia, and American Samoa asked regulators to ban RCCs.[23]

---

[17] www.echeck-merchantaccount.com/ viewed 7/23/13

[18] www.echeck-merchantaccount.com/eChecklist.html viewed 7/23/13

[19] 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.

[20] *See* NACHA, ACH Operations Bulletin #2-2013, "High-Risk Originators and Questionable Debit Activity at 1 n.2 (March 14, 2013), *available at* https://www.nacha.org/sites/default/files/files/ACH_Rules/ACH_Operations_Bulletins/ACH%20Operations%20Bulletin%20-%20High-Risk%20Originators%20and%20Questionable%20Debit%20Activity%20-%20March%2014%202013(1).pdf. 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.

[21] *See* George Thomas, "Viewpoint: Remote Checks Pose High Risk," American Banker (Feb. 17, 2010).

[22] 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.

[23] 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.gpo.gov/fdsys/pkg/CHRG-110shrg75784/html/CHRG-110shrg75784.htm.

The reasons to ban RCCs (and the electronic equivalent, RCPOs) are even more compelling today. With the availability of modern electronic payment methods, there are no longer any legitimate reasons to use either payment mechanism that can justify their risks.

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.[24] But even back in 2010, NACHA concluded that the safeguards of ACH debit transactions outweighed the conveniences RCCs, given their risks.[25]

Since 2010, changes in NACHA rules, along with other ACH or debit card options, have all but eliminated even those few legitimate advantages. Either an ACH or a debit card payment is as or nearly as fast as depositing a paper check. 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.

A discussion paper presented to the Atlanta Federal Reserve Board lists other legitimate uses of RCCs, though ACH or debit card payments could substitute for most if not all of them.[26] We understand that one of the prime legitimate uses of RCCs is for consumers who wish to make same day payments on their mortgage or insurance policy, a situation in which taking an ACH authorization is more difficult. We believe that, given the time to adjust, ACH payments could be used in that situation and that the minor advantages of RCCs and RCPOs are heavily outweighed by the significant consumer injury from their use.

The Commission has set forth a compelling case for prohibiting the use of RCCs and RCPOs in telemarketing transactions. However, the *exact* same set of facts, analysis, and rationale can be used by the FTC to prohibit the use of these payment mechanisms altogether under its unfairness authority. Moreover, it will be easier for originating banks and payment processers to avoid processing unlawful RCCs and RCPOs if all such instruments are banned. We encourage the FTC to work with the CFPB, FRB and other bank regulators to extend the scope of the excellent work evident in this rulemaking to prohibit remotely created checks and remotely created payment orders in all contexts applicable to consumers.

B. The FTC Should Hold Payment Processors and Originating Banks Strictly Liable for Facilitating Use of RCCs and RCPOs

A ban on RCCs and RCPOs that only applies to telemarketers and the sellers for which they work will be ignored by many scammers, who are already consciously violating the law. But users of RCCs and RCPOs normally require the assistance of at least two third parties: a payment processor and the originating bank (sometimes called the originating depository financial institution or ODFI). The best way to stop RCCs and RCPOs from entering into the system and reaching consumers'

---

[24] 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.
[25] Id. at 12.
[26] *See* Ana R. Cavazos-Wright, "An Examination of Remotely Created Checks," available at http://www.frbatlanta.org/documents/rprf/rprf_resources/RPRF_wp_0510.pdf.

accounts is to tighten up the rules governing those who assist or facilitate TSR violations and hold payment processors and ODFIs strictly liable for accepting RCCs or RCPOs that violate the TSR.[27]

Payment processors and ODFIs play critical roles in the misuse of RCCs and RCPOs. Although in theory anyone with the right software can create an RCC or RCPO, telemarketers and others usually engage the services of a third party payment processor, who actually creates the instrument and deposits as its bank, the ODFI. The payment processor acts as an intermediary between the payee (i.e., a telemarketer, payday lender or other merchant) and the ODFI that submits the item to the check clearing system. In the case of a remotely created check, the telemarketer transmits data that the payment processor uses to generate paper checks that the processor deposits into its account at the ODFI.[28] In the case of a remotely created payment order, the processor transmits electronic files to the ODFI bank for processing through the check clearing system.[29] The telemarketer or other merchant is a customer of the payment processor.

The payment processor deposits the RCC or RCPO into it's the account at its bank, the ODFI. The ODFI 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 ODFI 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.

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. In either case, the payment processor can serve as a vehicle for laundering the identity of the payee and giving the ODFI deniability from claims that it is processing fraudulent payments.[30] However, ODFIs should be aware that payment processors who process payments for other payment processors pose special risks.

The TSR already 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.[31] That is a difficult standard to prove and insulates third parties who are essential to a fraudulent scheme.

For example, the Sixth Circuit recently upheld the dismissal of claims against two banks that maintained accounts for and conspired with telemarketers to process payments for various telemarketers engaged in fraudulent activities. The court held that significant red flags of fraudulent

---

[27] Although the FTC does not have authority over financial institutions, it can work with the other regulators to adopt a complementary rule. Of course, a complete ban on RCCs and RCPOs would make it even easier for payment processors and originating banks to prevent misuse of those instruments.

[28] *See* Ana R. Cavazos-Wright, "An Examination of Remotely Created Checks," available at http://www.frbatlanta.org/documents/rprf/rprf_resources/RPRF_wp_0510.pdf.

[29] *See id.*

[30] *See* Reyes v. Zion First Nat. Bank, 2012 WL 947139 (E.D. Pa. Mar. 21, 2012); *In re* Wachovia Bank, 2008-027 (OCC Consent Order for a Civil Penalty, Apr., 24, 2008) (stating that bank engaged in unsafe, unsound, and unfair banking by debiting consumer accounts for payment processors acting on behalf of telemarketers, despite allegations of consumer fraud from other banks and consumers, and implementing a policy having effect of minimizing consumer complaints and bank's scrutiny of its relationship with payment processors and telemarketers.); FTC v. 3d Union Card Serv., doing business as Pharmacycards.com, Civ. Action No. CV-S-04-0712-RCJ-RJJ (D. Nev. 2004).

[31] 16 C.F.R. § 310.3(b).

telemarketing were insufficient to show that the banks actually knew of the fraudulent activities and agreed to conspire with the telemarketers.[32]

Nonetheless, under NACHA guidelines and bank regulator requirements, participants in payment systems are expected to know their customers and their customers' customers.[33] In the banking and payment processing industries, the monitoring of merchant return rates is a well-established component of risk management practices.[34] NACHA rules impose a duty on those who process ACH payments to monitor returns and to take action when there is a pattern of suspicious activity. NACHA maintains an Originator Watch List and a Terminated Originator Database to assist ODFIs in fulfilling their duty to avoid handling fraudulent items.

Such a systemic monitoring system is lacking for the check system. However, the FTC, together with the bank regulators, is in the position to create such a monitoring system. Although distinguishing RCCs and RCPOs from conventional checks is difficult on the receiving end, it is not difficult on the originating end. As the Commission 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.[35]

Moreover, the same lists of questionable originators and terminated originators that NACHA has created for the ACH system can be used to screen out or scrutinize originators that might be processing fraudulent RCCs and RCPOs.

The best way to give ODFIs and payment processors the incentive to conduct such monitoring is to hold them strictly liable for processing any improper RCCs and RCPOs, without the need to prove knowledge. Even if the ban on RCCs and RCPOs is limited to transactions under the TSR, ODFIs and payment processors can conduct due diligence about the business of the merchants for whom they process payments. Their job will be even easier if RCCs and RCPOs are banned entirely.

Strict liability for ODFIs and payment processors is consistent with the trend among regulators to impose greater responsibilities on those who process RCCs and RCPOs. Historically, liability for forged checks fell to the payor's bank (the consumer's bank, in the current context), rather than the payee's bank (the bank of the payment processor or telemarketer).[36] The payor bank, it was believed, would best know its customers and their signatures, and would thus be in the best position to verify whether a given check was legitimate or not. RCCs—which, by definition, do not

---

[32] Johnson v. US Nat' Bank Ass'n, 2012 WL 6200260, 508 Fed.Appx. 451 (6th Cir. Dec. 12, 2012).
[33] *Id.*
[34] *See* Complaint for Injunctive and Other Equitable Relief, FTC v. Landmark Clearing, Inc., et al, No. 4:11-cv-00826 (E.D. Tex. Dec. 15, 2011), available at http://www.ftc.gov/os/caselist/1123117/index.shtm.
[35] Proposed Rule, 78 Fed. Reg. at 41207 (original emphasis).
[36] This dates back to principles set forth in English common law. *See* Price v. Neal, 97 Eng. Rep. 871 (K.B. 1762).

have the consumer's signature, and do not originate with the consumer—cannot be verified by the consumer's bank at all. Recognizing this, the Federal Reserve Board transferred loss liability for unauthorized RCCs from the consumer's bank to the originating bank in a 2006 amendment to Regulation CC.[37] Once an RCC is determined to be inauthentic, the payee's bank can pass it back to previous parties, who are liable for warranting the instrument.[38]

Federal bank regulators have also issued guidance to the banks they supervise to address the problems posed by payment processors, RCCs and RCPOs. 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.[39] 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.[40] In addition, as the FTC details in these proposed regulations, regulators have taken actions against payment processors and originating banks arising out of RCCs.

However, as is evident from the hundreds of millions of dollars per year in fraudulent processing of both RCCs and RCPOs, the problems are still significant. While the change in the TSR proposed by the FTC will help, there is still a high likelihood that both payment processors and originating banks will be able to avoid liability and continue helping the processing of these dangerous payment mechanisms. These third parties can avoid liability under the existing TSR standard unless the FTC can prove that they knew or consciously avoided knowing that their involvement furthered the violation of the rules. The FTC's actions in this proposed rule, even accompanied by its litigation enforcement, may not be sufficient to stop the profitable market of processing fraudulent and illegal payments.[41] The FTC's actions were based, in part, on a payment study issued by the Federal Reserve System in 2011 that, among other issues, reported on the number of checks that were returned unpaid.[42] Existing rules have not prevented payment

---

[37] 12 C.F.R. §229.34(d)(1).

[38] Federal Fin'l Inst'ns Exam'n Council, IT Examination Handbook InfoBase – Remotely Created Checks, available at http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/payment-instruments,-clearing,-and-settlement/check-based-payments/remotely-created-checks.aspx?prev=1.

[39] 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.

[40] *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.

[41] The FTC has sued payment processors for unfair and deceptive practices when the processor used remotely created instruments to debit consumer accounts on behalf of merchant clients, ignoring high return rates and other warning signs that the payments were unauthorized. *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.). The complaint alleged that the processor ignored return rates of 50% to 80% when industry average return rates were closer to 1%. *Also see* Jessica Silver-Greenberg, *A Vulnerable Age – Fraud Against Seniors Often is Routed Through Banks.* New York Times, June 10, 2013. Available at http://www.nytimes.com/2013/06/11/business/fraud-against-seniors-often-is-routed-through-banks.html?emc=eta1&_r=1&.

[42] Federal Reserve System, "The 2010 Federal Reserve Payments Study: Noncash Payment Trends in the United States: 2006 – 2009 (Apr. 5, 2011), available at http://www.frbservices.org/files/communications/pdf/research/2010_payments_study.pdf. The Federal Reserve plans to update the study in 2013 to provide additional data including, for the first time, limited third-party fraud information.

processors and ODFIs from facilitating these dangerous payment mechanisms, even when the return rates on the transactions are alarmingly high.[43]

Payment processors and ODFIs rake in transaction fees from the scammers and the scammed alike. The FTC's proposal itself notes that payment processors have "perverse financial incentives" when it comes to scam artists.[44] The same is true of the banks that originate the payments. Some small banks in particular that are starved for fee income may be lured by the high revenue paid by processors who handle high risk payments.

To correct those incentives, the FTC and bank regulators must ensure that payment processors and ODFIs that enable misuse of RCCs and RCPOs cannot hide behind claims that they did not realize that they were processing unlawful payments. If strict liability is imposed on payment processors and ODFIs that process the banned form of payments in telemarketing, they will develop healthy mechanisms to ensure they are not processing these banned payments. The Commission and bank regulators must raise the stakes to ensure full responsibility by third parties who are essential to telemarketing and other consumer frauds.

C. The FTC Should Ban Cash-to-Cash Money Transfers and Cash Reload Systems for TSR-applicable Transactions.

As the FTC has documented in its proposal, cash-to-cash money transfers and cash reload systems have also been used with growing frequency to enable fraudulent transactions. Cash-to-cash money transfers are systems under which consumers use remittance providers, such as Western Union and Money Gram, to send cash to another individual. Cash reload systems are vehicles to load cash onto a prepaid card, such as the Green Dot MoneyPak. Though both have legitimate uses, cash-to-cash money transfers have been used by scammers for decades, and if past history is any indicator, cash reload systems will become just as popular.

Both vehicles allow scammers to remain practically anonymous when retrieving their victim's money, as quickly as minutes after the initial deposit is made. Although cash reload packs are typically used in connection with a prepaid card that has an identified account holder, scammers often use cards opened in the name of an identity theft victim and then immediately withdraw the cash. Once a cash transfer is retrieved or a prepaid card is emptied, the money is gone—and the scammer with it.

Federal Reserve Board, Press Release, "Federal Reserve Banks Announce New Study to Examine Nation's Payments Usage" (Jan. 17, 2013), available at http://www.federalreserve.gov/newsevents/press/other/20130117a.htm.

[43] Consider the 2006 proceeding by the Office of the Comptroller of the Currency in which it was alleged that telemarketers victimized more than 740,000 consumers using remotely created checks processed by three payment processors through Wachovia accounts. OCC Press Release, OCC, Wachovia Enter Revised Agreement to Reimburse Consumers Directly (Dec. 11, 2008), available at http://www.occ.gov/news-issuances/news-releases/2008/nr-occ-2008-143.html. 2 All three of these payment processors allegedly knew their clients had return rates well above accepted industry standards. *Also see,* cases noted Notes 104 -108 in 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.

[44] 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)).

Statistics from the National Consumers League's (NCL) Fraud Center, which takes complaints from consumers about telemarketing and Internet fraud and transmits that information to a variety of law enforcement agencies, confirm that these are scammers' payment methods of choice. In 2012, cash-to-cash money transfers were the top method of payment in telemarketing fraud reported to NCL's Fraud Center, accounting for nearly 63 percent of all telemarketing payments (up from 49 percent in 2009).

Since the Fraud Center does not have a payment category for cash reload systems, those payments are recorded in the "other credit card" category. In 2012, that was the second most common method of payment in telemarketing fraud reported to NCL's Fraud Center, at 8 percent of all telemarketing payments (up from 1 percent in 2009). According to NCL, most of the payments in the "other credit card" category appear to be situations in which cash reload systems were used.

Cash reload systems, while relatively new, already cause headaches for investigators. As the statistics from NCL's Fraud Center illustrate, more and more criminals across the country have turned to this method of payment as an effective way to anonymously bilk consumers out of their cash.[45] In 2011, Consumer Federation of America (CFA) released new tips and a video to help educate consumers about the growing use of cash reload systems in fraudulent transactions.[46] Scams that in past years would use the increasingly regulated money transfers are switching over to the largely unregulated cash reload systems.

For example, last November, the Federal Bureau of Investigations acknowledged that a computer scam was spreading across the country impersonating the bureau's Internet Crime Complaint Center.[47] This scam seizes the user's computer, displays an official-looking FBI notice accusing the user of accessing felonious content online, and offers to settle the charge with a "fine," payable through MoneyPak cards.[48]

As the FTC's proposal explains, the laws that govern cash-to-cash transfers and cash reload systems are inadequate to protect consumers. Both systems are typically governed by state money transmitter laws. Those laws primarily require state licenses and bonding to ensure the solvency of the company. But they are not set up to protect consumers from liability when the systems are misused, and they certainly do not have the robust consumer remedies and fraud prevention systems that the ACH system and card networks do.

Consequently, the FTC's proposal to ban use of cash-to-cash transfers and cash reload systems in TSR transactions is well justified. Neither payment system has any legitimate use in that context and both are merely vehicles for evading consumer protections and liability for fraud. Legitimate actors can easily use electronic payments or debit or credit cards and have no need to use payment systems that are designed for entirely different purposes.

---

[45] See notes 157-158 of the FTC's Notice of Proposed Rulemaking for examples of fraudulent transactions across the country using cash reload systems to bilk consumers.

[46] See Scam Artists Target New Payment Methods under Consumer Information at www.consumerfed.org/fraud.

[47] http://www.fbi.gov/scams-safety/e-scams (accessed June 19, 2013).

[48] One victim of the virus, David Wismer, documented his experience with the scam earlier this year, available at http://www.forbes.com/sites/davidwismer/2013/02/06/hand-to-hand-combat-with-the-insidious-fbi-moneypak-ransomware-virus/.

D. The FTC Should Extend the Payment Systems Ban to Internet and Other Types of Sales

The proposed ban on the four payment systems should apply not only to transactions that involve a telephone but also to sales initiated by email, over the internet or through other methods that are not covered by the TSR. For example, just in the past few days a court issued a permanent injunction requested by the FTC against an online operation that illegally debited consumers' bank accounts using RCPOs when consumers visited the defendants' websites seeking payday loans.[49] As the FTC described in connection with recovery services scams, modern scams may take place entirely over the internet or through email without using a telephone. The consumers that our organizations represent have been frequently victimized by scams that are outside the scope of the TSR protections.

RCCs and RCPOs are unnecessary and inappropriate in any context, and there is no legitimate need for any business to use a cash-to-cash transfer or cash reload system as a method of receiving payment from a consumer. The anonymity and lack of consumer protections for those systems are totally inappropriate for sales transactions. The compelling case that the FTC has made for the TSR rule applies equally to internet sales.

Though the FTC may not have the same rulewriting authority over transactions outside the TSR rule, it can issue a strong statement that it is unfair and deceptive to use the four payment systems described in *any* sales context. The FTC can also take enforcement actions against persons who commit unfair or deceptive practices by misusing those payment systems even if the transactions are not covered by the TSR rule. The FTC should put everyone on notice that the Commission's view of the unfair and deceptive nature of RCCs, RCPOs, cash-to-cash transfers and cash reload systems as a device for receiving payments from consumers is not limited to telemarketing transactions.

E. The FTC Should Increase Responsibility for Those Who Assist or Facilitate Improper use of Cash-to-Cash Transfers and Cash Reload Systems

Unlike RCCs and RCPOs, both cash-to-cash transfers and cash reload systems have legitimate purposes and should not be banned entirely. But the operators of those systems still have a role to play in ensuring that the systems are not misused for fraudulent purposes. The FTC should consider imposing strict liability on money transmitters for violations of the proposed TSR ban and should explore patterns of misuse that would trigger responsibilities for cash reload system operators.

Studies have shown a shocking correlation between cash-to-cash money transfers and telemarketing fraud. An FTC survey showed that 79 percent or more of all Money Gram transfers of $1,000 or more from the United States to Canada over four months in 2007 were fraud-induced. Several attorneys general who surveyed Western Union customers in 2003 found that about one-third of the person-to person transfers over $300 to Canada were fraud-induced. Western Union's

[49] See FTC, Press Release, "Judge Agrees With FTC: Scammers Debited Payday Loan Applicants' Bank Accounts Without Their Consent; Consumers Entitled to More Than $9.5 Million in Refunds" (July 30, 2013), available at http://www.ftc.gov/opa/2013/07/directbenefits.shtm.

own survey found that 58% of the total dollars transferred by the surveyed customers were fraud-induced and that the average transfer by a defrauded customer was $1,500.

Regulators have had lengthy experience with cash-to-cash money transfers. The FTC,[50] the U.S. Attorney for the Middle District of Pennsylvania,[51] and the attorneys general of forty-six different states[52] have taken action against MoneyGram, the second largest cash-to-cash money transfer company, in the last decade for sloppy practices, including a lack of money laundering prevention programs, poor-to-no oversight of agents committing fraud, and failure to protect consumers from fraudulent transactions. Western Union, the industry leader, also settled with most of the attorneys general in 2005 for failure to protect consumers from fraud.[53]

Money transmitters do not currently have sufficient incentives to set up systems to detect misuse. Every money transfer earns them a fee. In 2012, $4.2 billion – nearly 75% of Western Union's revenues – came from transaction fees.[54] MoneyGram has 85% of revenue, about $1.2 billion, from money transfer fees.[55] Whether or not money transmitters are knowing parties to fraudulent transactions, every fraudulent transfer coming through their services earns them more profit at the expense of the scammers' victims.

Moreover, many fraudulent transactions are operated by agents of the companies themselves, who use their position from within the company to rob consumers.[56] For years, MoneyGram was well aware that its agents were defrauding consumers and did little to stop it. In fact, MoneyGram encouraged these fraudsters with parties and gifts, all the while profiting from the fraudulent transactions' fees.[57] Despite flagging the most egregious scam agent's outlet as processing high levels of fraudulent transactions as early as 2004, MoneyGram let him operate unhindered for nearly five years, with senior executives overruling their own fraud department's recommendation that they be shut down in 2007.[58] All told, the fraudster took nearly $28 million from Americans.[59]

Money transmitters are in a position to police their system, and they will do so if they have strict liability for violations. Money transmitters already have obligations to prevent money

---

[50] FTC v. MoneyGram Int'l., Inc., Civ. No. 1:09-06576 (N.D. Ill. Oct. 19, 2009) (Stip. Perm. Inj.).
[51] *United States v. MoneyGram Int'l, Inc.,* Cr. No. 1:12-291 (M.D. Pa. Nov. 9, 2012).
[52] This action resulted in an assurance of voluntary compliance, available at https://www.oag.state.tx.us/newspubs/releases/2008/070208moneygram_avc.pdf.
[53] A press release detailing the settlement with 47 states and the District of Columbia is available at http://www.law.state.ak.us/press/releases/2005/111405-WesternUnion.html.
[54] Western Union 2012 10-K filing with the SEC, p. 53, available at http://www.sec.gov/Archives/edgar/data/1365135/000136513513000008/wu-12312012x10k.htm.
[55] MoneyGram 2012 10-K filing with the SEC, pp. 5, 31, available at http://www.sec.gov/Archives/edgar/data/1273931/000119312513089758/d440705d10k.htm.
[56] *See, e.g.,* Department of Justice Press Release, "Three Receive Prison Sentences, Nine Indicted in Continuing Federal Prosecution of Mass-Marketing Schemes," available at http://www.justice.gov/usao/pam/news/2012/MoneyGram_3_1_2012.htm (three MoneyGram agents sentenced to up to 11 years in prison for defrauding Americans, while nine other Western Union and MoneyGram agents were indicted for similar frauds); United States v. MoneyGram Int'l, Cr. No. 1:12-cv-00291 (M.D. Pa. Nov. 9, 2012), available at http://lib.law.virginia.edu/Garrett/prosecution_agreements/pdf/MoneyGram.pdf.
[57] US v. MoneyGram (MoneyGram rewarded and encouraged agents with the highest levels of fraudulent activity, including giving one such agent a MoneyGram-sponsored party, a $70,000 re-signing bonus, and permission to expand from one store to twelve).
[58] Id.
[59] Id.

laundering. They can look for patterns of large amounts of funds being transmitted to particular persons or locations or other suspicious patterns. They can post prominent notices about scams, ask the sender why he is sending the money, and stop common scams like grandparent scams[60].

The Commission need look no further than to the credit card industry for an example of how creating strict liability for fraud is workable and leads to better protections for consumers. The Truth in Lending Act as amended by the Fair Credit Billing Act creates limits on the amount owed by cardholders for unauthorized transactions, generally capping their liability at $50.[61] In response to this heightened liability for fraud, the credit card industry has robust anti-fraud technologies.[62] Similarly, banks and other financial institutions have created systems to guard against losses covered by the Electronic Fund Transfer Act. Both laws place liability on the institutions for losses. As a result, both laws have provided strong financial incentives for the industry to limit those losses by creating new systems to protect themselves.

Cash reload systems operate somewhat differently from cash-to-cash money transfers, but the FTC should still consider imposing greater obligations on the operators of those systems. Cash reload systems are often sold at unaffiliated retail stores, and the system operator may not have the same face-to-face interaction with the defrauded consumer as a money transmitter does. But the reload operator may still be able to detect patterns or scrutinize suspicious transactions, such as withdrawals in foreign countries, cash reloads followed by immediate cash withdrawals, or high volume withdrawals by different customers at an unusual ATM.

The cash-to-cash money transfer and cash reload system industries are capable of creating internal systems to minimize fraudulent transactions. They are in a much better position than consumers themselves to root out systemic problems. The FTC must provide the necessary incentives to encourage fraud detection regimes and ensure that consumers can use these systems with confidence.

III. We Support the Other Proposed Amendments Governing Recovery Services and Evasions of the TSR and Do Not Call Registry

We support the proposal to ban advance fees charged for purported help in recovering losses in connection with prior scams of all types. The existing recovery services rule addresses only scams under which a consumer is promised help in recovering lost money, prizes or merchandise in connection with prior telemarketing sales. But as these scams increasingly take place over the internet, the advance fee ban should apply to all offers of recovery services regardless how the original loss occurred. There is no reason to make a distinction based on the circumstances of the loss.

We support the proposed amendment to require that the goods or services being purchased in a telemarketing transaction be verified in the recording of the consumer's consent. Telemarketers

[60] In the grandparent scam, a senior receives a call from a person purporting to be a grandson or granddaughter, saying that the grandchild has gotten into trouble and needs the grandparent to wire money immediately. The scam takes advantage of the fact that some seniors may not remember the names of all of their grandchildren or their voices. The scammer asks the grandparent not to tell the parent about the incident.

[61] 15 USC § 1602.

[62] National Consumer Law Center, "Truth in Lending Act, Eighth Edition" §§ 7.9-7.11, 2012.

often confuse consumers about exactly what they are selling. Requiring that the seller repeat an exact description of the item being purchased, recorded in a fashion that the FTC can verify and scrutinize, will help to ensure that consumer consent is genuine.

Better yet, we recommend that the FTC require telemarketers to record the entire conversation. Providing the entire context will ensure that other parts of the conversation and not unfair or deceptive and do not undercut the consumer's understanding of the product they are purchasing.

We also support the proposed amendments intended to prevent evasions of the Do Not Call Registry. We agree with the Commission's rationale for amendments that put the burden on the telemarketer to prove that the call is exempt from the Do Not Call ban; clarify coverage of calls to individual employees of a business; prohibit all sharing of DNC registry fees; and provide examples of impermissible efforts to block consumers from getting on a company's specific do-not-call list. The Do Not Call list is vitally important to consumers nationwide. But unfortunately, the consumers we represent are still plagued with unwanted calls, some of which are exploiting purported exemptions and other weaknesses in the existing rule. The proposed rules will help to close some of those loopholes and strengthen enforcement of existing rules.

IV. Additional Reforms Needed

We appreciate the important amendments that the FTC has proposed to the TSR. But more is needed to address unscrupulous telemarketing and sales practices. The rule is antiquated and in drastic need of improvement in other areas. We request that the Commission open a broader rulemaking, and convene a meeting to discuss other necessary changes. This is only a partial list, but other needed reforms include:

- *Negative option billing*: Negative option billing is a business practice in which a customer purportedly agrees to have goods or services provided automatically, and the customer must either pay for the service or specifically decline it in advance of billing. Consumers who sign up for a trial offer or a free giveaway often do not realize that they have given consent to have their credit or debit card or bank account charged on an ongoing basis. They then incur the hassle and expense of returning items and trying to figure out how to stop future items or bills. Companies also often make it difficult to cancel these agreements, hiding the procedure or requiring traditional mail rather than internet or telephone options. Another variation of this practice is magazine subscriptions that require automatic renewals and do not permit the consumer to simply pay for a single year's subscription, or that pre-check the renewal box. The TSR currently requires a few basic disclosures and prohibits certain deceptive statements for negative option sales. Negative option sales are a growing problem, as the FTC's action in just the last few days has shown.[63]

[63] See FTC, Press Release, "FTC Seeks Contempt Ruling Against Suntasia Telemarketing Defendants Defendants Ordered to Pay Over $11 Million" (Aug. 1, 2013) (involving defendants who defrauded consumers and charged their bank accounts without consent for various negative option programs, including memberships in discount buyer's and travel clubs), available at http://www.ftc.gov/opa/2013/08/suntasia.shtm.

- *Upselling practices.* The FTC should address a number of other unscrupulous upselling practices that induce consumers to purchase items they do not want. Add-ons can include insurance products, clubs and memberships, or other items. The protections against upselling in the current rule are insufficient.

- *Sales by lead generators and others of personal financial information to third parties.* The FTC has brought important cases against debt collectors who attempted to collect payday loan debts from consumers who never took out the loans. Consumers who thought they were applying for loans entered their bank account information in the website of a lead generator, who then sold that information to third parties who used it for improper purposes. Consumers have been defrauded into providing their financial information to other parties who sell it to the highest bidder. The FTC should ban businesses from selling personal financial information to third parties or providing it to anyone who is not a necessary party to the immediate transaction.

- *Debt relief services.* The FTC should strengthen the regulation of debt relief services to address abuses and evasions that have become problematic since the rules were last issued. In particular, the FTC should eliminate the exemption for agreements consummated in face-to-face meetings and should require payment for installment settlements to be made in proportion to each installment made as the creditor is paid.

- *Mandatory arbitration clauses and class action bans.* The FTC knows from experience that unfair and abusive practices and other legal violations are rampant in the telemarketing and debt relief areas. Public enforcement actions are time consuming and the FTC cannot possibly stop every violation. Yet consumers are often frustrated in their quest for relief by forced arbitration clauses and class action bans. Forced arbitration pushes consumers into a biased, lawless and secretive system. Mandatory arbitration also prevents consumers from getting the information needed to prove their cases. Class action bans promote relief for all victims of a violation and prohibit consumers from banding together when individual claims do not justify the expense of hiring a lawyer and investigating a case. The effect of the forced arbitration clause and class action waiver is to insulate businesses from the legal consequences of their misconduct, including violations of consumer protection statutes. Unfortunately, a series of recent decisions by the U.S. Supreme Court have made it significantly more difficult for consumers to vindicate their rights and challenge even the most abusive forced arbitration and class action ban clauses. Forced arbitration clauses and class action waivers shield telemarketing scammers from liability for their fraud, and the clauses and waivers should be banned in all transactions covered by the TSR.

V. Conclusion

The FTC has done much to protect consumers in the Proposed Rule. We support all of the proposed amendments. We also urge the FTC to work for a complete ban on RCCs and RCPOs; strengthen the liability of third parties who facilitate use of unusual payment systems; extend the ban to sales on the internet and through other methods; and open a rulemaking to address other unfair and deceptive sales practices. We appreciate the important work of the Commission to stamp out fraud against consumers. We would welcome the opportunity to meet with you to discuss additional reforms needed.

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.

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.

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.

The **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.

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,