BILLING CODE: 6750-01-S

FEDERAL TRADE COMMISSION

16 CFR Part 310 Telemarketing Sales Rule

RIN 3084–AB19

AGENCY: Federal Trade Commission.

ACTION: Final Rule Amendments.

SUMMARY: In this document, the Commission adopts amendments to the Telemarketing Sales Rule ("TSR" or "Rule"). These amendments define and prohibit the use of certain payment methods in all telemarketing transactions; expand the scope of the advance fee ban for recovery services; and clarify certain provisions of the Rule. The amendments are necessary to protect consumers from deceptive or abusive practices in telemarketing.

DATES: The amendments published in this document are effective on **[insert date 60 days from date of publication]**, except for sections 310.4(a)(9) and (10), which are effective on **[insert date 180 days from date of publication]**.

ADDRESSES: This document is available on the Internet at the Commission's website at www.ftc.gov. The complete record of this proceeding, including the final amendments to the TSR and the Statement of Basis and Purpose ("SBP"), is available at www.ftc.gov.

FOR FURTHER INFORMATION CONTACT: Karen S. Hobbs or Craig Tregillus, Attorneys, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Room CC-8528, Washington, D.C. 20580, (202) 326-3587 or 2970.

SUPPLEMENTARY INFORMATION:

This document states the basis and purpose for the Commission's decision to adopt amendments to the TSR that were proposed and published for public comment in the Federal Register on July 9, 2013.[1] After careful review and consideration of the entire record on the issues presented in this rulemaking proceeding, including 43 public comments submitted by a variety of interested parties,[2] the Commission has decided to adopt, with several modifications, the proposed amendments to the TSR intended to curb deceptive or abusive practices in telemarketing and improve the effectiveness of the Rule.

Beginning on **[insert date 60 days from publication]**, sellers and telemarketers will be required to comply with the amended TSR requirements, except for sections 310.4(a)(9) and (10), the prohibitions against accepting remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms, which will be effective on **[insert date 180 days from publication]**.

I. Background

A. Overview of the TSR

Enacted in 1994, the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act" or "Act")[3] targets deceptive or abusive telemarketing practices.[4] The Act

[1] *Telemarketing Sales Rule Notice of Proposed Rulemaking*, 78 FR 41200 (July 9, 2013) (hereinafter *NPRM*). The text of the TSR is set forth at 16 CFR 310. Unless stated otherwise, references to specific provisions of the TSR refer to the current version of the Rule published in the Code of Federal Regulations, revised as of January 1, 2015.
[2] All of the public comments are available at http://ftc.gov/os/comments/tsrantifraudnprm/index.shtm. In addition, a list of commenters cited in this SBP, along with their short citation names or acronyms used throughout the SBP, is attached as Appendix A. Where a commenter submitted more than one comment, the comment is identified separately.
[3] 15 U.S.C. 6101-6108. Subsequently, the USA PATRIOT Act, Pub. L. 107–56, 115 Stat. 272 (Oct. 26, 2001), expanded the Telemarketing Act's definition of "telemarketing" to encompass calls soliciting charitable contributions, donations, or gifts of money or any other thing of value.
[4] Other statutes enacted by Congress to address telemarketing fraud during the early 1990's include the Telephone Consumer Protection Act of 1991, 47 U.S.C. 227 *et seq.*, which restricts the use of automated dialers, bans the sending of unsolicited commercial facsimile transmissions, and directs the Federal Communications Commission

specifically directed the Commission to issue a rule defining and prohibiting deceptive and abusive telemarketing practices.[5] In addition, the Act mandated that the rule address some specified practices, which the Act designated as "abusive."[6] The Act also authorized state attorneys general or other appropriate state officials, as well as private persons who meet stringent jurisdictional requirements, to bring civil enforcement actions in federal district court.[7]

Pursuant to the Act's directive, the Commission promulgated the original TSR in 1995 and subsequently amended it in 2003 and again in 2008 and 2010 to add, among other things, provisions establishing the National Do Not Call Registry and addressing the use of pre-recorded messages and debt relief offers.[8] The TSR applies to virtually all "telemarketing," defined to mean "a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call."[9] The Telemarketing Act, however, explicitly states that the jurisdiction of the Commission in enforcing the Rule is coextensive with its jurisdiction under Section 5 of the Federal Trade Commission Act ("FTC Act").[10] As a result, some entities and products fall outside the jurisdiction of the TSR.[11] Further, the Rule wholly or partially exempts

---

("FCC") to explore ways to protect residential telephone subscribers' privacy rights; and the Senior Citizens Against Marketing Scams Act of 1994, 18 U.S.C. 2325 *et seq*., which provides for enhanced prison sentences for certain telemarketing-related crimes.

[5] 15 U.S.C. 6102(a).

[6] 15 U.S.C. 6102(a)(3).

[7] 15 U.S.C. 6103, 6104.

[8] *Telemarketing Sales Rule Statement of Basis and Purpose and Final Rule,* 60 FR 43842 (Aug. 23, 1995) (hereinafter *TSR Final Rule 1995*); *Amended Telemarketing Sales Rule Statement of Basis and Purpose,* 68 FR 4580 (Jan. 29, 2003) (hereinafter *TSR Amended Rule 2003*); *Amended Telemarketing Sales Rule Statement of Basis and Purpose,* 73 FR 51164 (Aug. 29, 2008) (hereinafter *TSR Amended Rule 2008*); *Amended Telemarketing Sales Rule Statement of Basis and Purpose,* 75 FR 48458 (Aug. 10, 2010) (hereinafter *TSR Amended Rule 2010*).

[9] 16 CFR 310.2(cc) (using the same definition as the Telemarketing Act, 15 U.S.C. 6106).

[10] 15 U.S.C. 6105(b).

[11] 15 U.S.C. 45(a)(2) (setting forth certain limitations to the Commission's jurisdiction with regard to its authority to prohibit unfair or deceptive acts or practices). These entities include banks, savings and loan institutions, and certain federal credit unions. It should be noted, however, that although the Commission's jurisdiction is limited with respect to the entities exempted by the FTC Act, the Commission has made clear that the Rule does apply to any

from its coverage several types of calls.[12]

The TSR is fundamentally an anti-fraud rule that protects consumers from deceptive and abusive telemarketing practices. First, the Rule requires telemarketers to make certain disclosures to consumers, and it prohibits material misrepresentations.[13] Second, the TSR requires telemarketers to obtain consumers' "express informed consent" to be charged on a particular account before billing or collecting payment and, through a specified process, to obtain consumers' "express verifiable authorization" to be billed through any payment system other than a credit or debit card.[14] Third, the Rule prohibits telemarketers and sellers from requesting or receiving payment in advance of obtaining: credit repair services;[15] recovery services;[16] offers of a loan or other extension of credit, the granting of which is represented as "guaranteed" or having a high likelihood of success;[17] and debt relief services.[18] Fourth, the Rule prohibits credit card laundering[19] and other forms of assisting and facilitating sellers or telemarketers

---

third-party telemarketers those entities might use to conduct telemarketing activities on their behalf. *See TSR Proposed Rule*, 67 FR 4492, 4497 (Jan. 30, 2002) (citing *TSR Final Rule 1995*, 60 FR 43843) ("As the Commission stated when it promulgated the Rule, '[t]he Final Rule does not include special provisions regarding exemptions of parties acting on behalf of exempt organizations; where such a company would be subject to the FTC Act, it would be subject to the Final Rule as well.'").

[12] For example, Section 310.6(a) exempts telemarketing calls to induce charitable contributions from the Do Not Call Registry provisions of the Rule, but not from the Rule's other requirements. In addition, there are exceptions to some exemptions that limit their reach. *See, e.g.*, 16 CFR 310.6(b)(5)-(6).

[13] The TSR requires that telemarketers soliciting sales of goods or services promptly disclose several key pieces of information: (1) the identity of the seller; (2) the fact that the purpose of the call is to sell goods or services; (3) the nature of the goods or services being offered; and (4) in the case of prize promotions, that no purchase or payment is necessary to win. 16 CFR 310.4(d). Telemarketers also must disclose, in any telephone sales call, the cost of the goods or services and certain other material information. 16 CFR 310.3(a)(1).

In addition, the TSR prohibits misrepresentations about, among other things, the cost and quantity of the offered goods or services. 16 CFR 310.3(a)(2). It also prohibits making false or misleading statements to induce any person to pay for goods or services or to induce charitable contributions. 16 CFR 310.3(a)(4).

[14] 16 CFR 310.4(a)(7); 16 CFR 310.3(a)(3).

[15] 16 CFR 310.4(a)(2).

[16] 16 CFR 310.4(a)(3).

[17] 16 CFR 310.4(a)(4).

[18] 16 CFR 310.4(a)(5).

[19] 16 CFR 310.3(c).

engaged in violations of the TSR.[20]

The TSR also protects consumers from unwanted telephone calls. With narrow exceptions, it prohibits telemarketers from calling consumers whose numbers are on the National Do Not Call Registry or who have specifically requested not to receive calls from a particular entity.[21] Finally, the TSR requires that telemarketers transmit to consumers' telephones accurate Caller ID information[22] and places restrictions on calls made by predictive dialers[23] and those delivering pre-recorded messages.[24]

B. Overview of the Proposal to Amend the TSR

On July 9, 2013, the Commission proposed to amend the TSR to enhance its anti-fraud protections, as well as to clarify amendments that apply primarily, though not exclusively, to the provisions restricting unwanted calls. The Commission's Notice of Proposed Rulemaking ("NPRM") detailed the proposed amendments to the TSR ("proposed Rule"). The subsections I.B.1 and I.B.2 below describe the Commission's proposal with respect to its anti-fraud amendments, which would:

1. Define and prohibit the use of four types of payment methods by telemarketers and sellers: "remotely created check," "remotely created payment order," "cash-to-cash money transfer," and "cash reload mechanism."

2. Expand the prohibition against advanced fees for recovery services (now limited to recovery of losses sustained in prior telemarketing transactions) to include recovery of losses in any previous transaction.

[20] 16 CFR 310.3(b).
[21] 16 CFR 310.4(b).
[22] 16 CFR 310.4(a)(8).
[23] 16 CFR 310.4(b)(1)(iv).
[24] 16 CFR 310.4(b)(1)(v).

Section II sets forth the Commission's analysis of the comments received on the proposal, any modifications to the proposed language, and reasons for adopting the provisions of the Final Rule.

The clarifying amendments, discussed in Section III, serve three main functions. First, they specify that a description of the goods or services purchased must be included in the verification recording of a consumer's agreement to purchase them. Second, they clarify that the business-to-business exemption extends only to calls to induce a sale to or contribution from a business entity, and not to calls to induce sales to or contributions from individuals employed by the business. Finally, these amendments address the TSR's Do Not Call requirements to:

- State expressly that a seller or telemarketer bears the burden of demonstrating that the seller has an existing business relationship with, or has obtained an express written agreement from, a person whose number is listed on the Do Not Call Registry;
- Illustrate the types of impermissible burdens that deny or interfere with a consumer's right to be placed on a seller's or telemarketer's entity-specific do-not-call list;
- Specify that a seller's or telemarketer's failure to obtain the information necessary to honor a consumer's request to be placed on a seller's entity-specific do-not-call list pursuant to section 310.4(b)(1)(ii) disqualifies it from relying on the safe harbor for isolated or inadvertent violations in section 310.4(b)(3); and
- Emphasize that the prohibition against sellers sharing the cost of Do Not Call Registry fees, which are non-transferrable, is absolute.

1. Proposed Prohibition on Novel Payment Methods in Telemarketing

The NPRM proposed to prohibit the use of four types of "novel payment methods" in telemarketing, namely: remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms.[25] The Commission distinguishes these four payment methods from "conventional payment methods," such as credit cards, and electronic fund transfers, such as debit cards. The conventional payment methods are processed or cleared electronically through networks that can be monitored systematically for fraud. Further enhancing the security of conventional payment methods is the fact that they are subject to federal laws that provide statutory limitations on a consumer's liability for unauthorized transactions and standard procedures for resolving errors. The NPRM contrasted and compared the features and vulnerabilities of the four types of novel payment methods, especially when used in telemarketing.[26]

a. Remotely Created Checks and Remotely Created Payment Orders

Traditional checks require the signature of the account holder and instruct a financial institution to pay money from the account of the check writer ("payor") to the check recipient ("payee"). As originally defined in the NPRM, a remotely created check ("RCC") is a type of check which is created by the payee (typically a merchant, seller, or telemarketer) using the consumer's personal and financial account information and which is not actually signed by the payor.[27] In place of the payor's actual signature, the remotely created check usually bears a

[25] *NPRM*, *supra* note 1, at 41200.
[26] *Id.* at 41202-07.
[27] For the reasons raised by certain commenters, and discussed in detail in Section II.A.4 below, the Final Rule adopts a revised definition of "remotely created payment order" that deletes the reference to the absence of the

statement indicating that the account holder authorized the check, such as "Authorized by Account Holder" or "Signature Not Required." A remotely created check is deposited into the check clearing system like any other check. As defined in the NPRM, a remotely created payment order ("RCPO") is an electronic version of a remotely created check. The electronic image looks and functions like a remotely created check, but it never exists in paper form. Using remote deposit capture – a system that allows a depositor to scan checks remotely and transmit the check images to a bank for deposit – a merchant, seller, or telemarketer can deposit a remotely created payment order into the check clearing system in the same way as traditional paper checks and remotely created checks.

Electronic payment alternatives to remotely created checks and remotely created payment orders include conventional payment methods, such as Automated Clearinghouse ("ACH")[28] debits and traditional debit card transactions – both of which involve consumer bank accounts – as well as credit card transactions.[29] These alternatives are processed through different payment networks. Payment methods cleared through the ACH network are subject to regular oversight and scrutiny by NACHA – The Electronic Payments Association ("NACHA"), a private self-regulatory trade association that enforces a system of rules, monitoring, and penalties for

---

payor's signature and eliminates the need for a separate definition of "remotely created check." The revised definition of "remotely created payment order" includes any payment instruction or order drawn on a person's account that is created by the payee and deposited into or cleared through the check clearing system. The definition is broad enough to include a "remotely created check," as defined in Regulation CC.

[28] ACH transactions are electronic payment instructions to either credit or debit a bank account. ACH credit transactions push funds into an account, while ACH debit transactions pull funds from an account. NACHA, *What is ACH?: Quick Facts About the Automated Clearing House (ACH) Network* (Jul. 1, 2013), *available at* https://www.nacha.org/news/what-ach-quick-facts-about-automated-clearing-house-ach-network. ACH credits include payroll direct deposits, Social Security benefits, and interest payments. Examples of ACH debit transactions include mortgage, loan, and insurance premium payments. FFIEC, *Bank Secrecy Act/Anti-Money Laundering Examination Manual, Automated Clearing House Transactions—Overview* 217 (Feb. 27, 2015) *available at* http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_059.htm.

[29] Unlike most general-purpose reloadable cards and other prepaid cards, traditional debit cards (also referred to as "check cards") are linked to consumer checking accounts at a financial institution. *See infra* notes 176-178; Electronic Funds Transfer Act ("EFTA"), 15 U.S.C. 1693; Regulation E, 12 CFR 1005.

noncompliance. Among other things, NACHA monitors the levels at which all ACH debits are returned (or rejected) by consumers or consumers' banks because high rates of returned transactions ("return rates") can be indicative of unlawful practices, such as unauthorized debiting of consumer accounts. NACHA also monitors and categorizes specific types of returned transactions, based on the reason for the return, such as "unauthorized," "non-sufficient funds," or "invalid account numbers." For many years, NACHA's rules have required banks to report and investigate any merchant with a monthly return rate of 1 percent or more for returns categorized as unauthorized,[30] a threshold that NACHA recently reduced to 0.5 percent.[31]

Likewise, the payment card networks, such as American Express, Discover, MasterCard, and Visa, impose on participants (*e.g.*, merchants, banks, and third party payment processors) a system of rules, monitoring, and penalties for noncompliance. Transactions processed through the payment card networks, including certain types of debit and general-purpose reloadable debit card ("GPR card") transactions, are subject to systemic monitoring to identify unusual activity associated with fraud.[32] Among other things, payment card networks monitor whether a merchant's monthly number of chargebacks[33] and chargeback rate (*i.e.*, the percentage of transactions that are "charged back" out of the total number of sales transactions submitted by a

[30] NACHA, 2013 Operating Rules, Art. 2, Subsection 2.17.2.1, Additional ODFI Action and Reporting When the Return Threshold is Exceeded (Mar. 15, 2013) (describing the actions that originating financial institutions ("ODFIs") must take when an originator's unauthorized return rate exceeds 1 percent).

[31] In September 2015, amendments to NACHA's Operating Rules will take effect. Among other things, these amendments reduce the threshold for unauthorized returns from one percent to 0.5 percent. Press Release, NACHA, *NACHA Membership Approves New Rules to Further Improve ACH Network Quality* (Aug. 26, 2014), *available at* https://www.nacha.org/rules/updates. NACHA also adopted new monthly return rate thresholds for other types of ACH debit returns, including a three percent threshold for returns based on "account data issues" (*i.e.*, debits returned for invalid account numbers or an inability to locate the account) and a total return rate of 15 percent.

[32] Network-branded debit cards and GPR cards can be used like credit cards to make purchases at a variety of stores, online, or over the telephone. These so-called "signature" debit card purchases (*i.e.*, without the use of a PIN) are processed through and, thus, subject to the operating rules and anti-fraud monitoring of the payment card networks.

[33] "Chargeback" is a payments industry term used to describe the process through which a disputed charge to a consumer's credit card is refunded to the consumer and charged back to the entity, often a merchant, that placed the charge on the consumer's account. *See NPRM*, *supra* note 1, at 41203 & nn.47-48.

specific merchant) exceed certain parameters – for example, 100 chargebacks and a 1 percent chargeback rate in a given month.[34]

In contrast to the transactions processed by the ACH and payment card networks, remotely created checks and remotely created payment orders are not subject to such centralized and systemic monitoring. This is due to the decentralized nature of the check clearing system and the inability of banks to distinguish these items from other checks deposited for clearing.[35]

In addition to these operational differences between conventional and novel payment mechanisms, different laws govern each type of payment. As described in detail in section II.A.3.a(3) below, electronic fund transfers such as ACH debits and traditional debit card transactions are governed by Regulation E and the EFTA, which provide consumers with specific rights, including liability limits for unauthorized transactions, the right to a prompt re-credit of funds, specified deadlines for completing investigations of unauthorized transactions, and the right to notification of the results of such investigations.[36] Under Regulation E and the

---

[34] For example, Visa's operating rules state:

> Visa monitors the total volume of US Domestic Interchange, International Interchange, and Chargebacks for a single Merchant Outlet and identifies US Merchants that experience all of the following activity levels during any month:
> • 100 or more interchange transactions
> • 100 or more Chargebacks
> • A 1% or higher ratio of overall Chargeback-to-Interchange volume

Visa, U.S.A, *Visa Core Rules and Visa Product Service Rules*, 479 (Oct. 15, 2014), *available at* http://usa.visa.com/download/about_visa/15-October-2014-Visa-Rules-Public.pdf. MasterCard maintains similar, but not identical, thresholds for its excessive chargeback monitoring programs (at least 100 chargebacks and a chargeback ratio of 1.5 percent). MasterCard, *Security Rules and Procedures: Merchant Edition*, 8-13 (July 31, 2014), *available at* http://www mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf.

[35] *NPRM*, *supra* note 1, at 41206-07.

[36] *See infra* notes 176-178; EFTA, 15 U.S.C. 1693; Regulation E, 12 CFR 1005. With certain exceptions, most GPR cards are not subject to the EFTA or Regulation E. However, payment card networks voluntarily extend their same zero liability protection to GPR purchases as they apply to credit and traditional debit cards processed through their networks. Federal Reserve Bank of Atlanta, Retail Payments Risk Forum, *Dispelling prepaid card myths: Not all cards are created equal* (July 5, 2011), available at http://portalsandrails.frbatlanta.org/2011/07/dispelling-prepaid-card-myths-not-all-cards-created-equal html; *see also infra* note 178. The CFPB recently published a proposed rule that would extend to "prepaid accounts," including GPR cards, the protections of Regulation E and the EFTA, with certain important modifications. *Notice of Proposed Rulemaking Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z)* (hereinafter "Prepaid Account Rule"), 79

EFTA, the financial institution has the burden of proof for showing the transaction was "authorized" or "unauthorized."[37] For ACH transactions, consumers also benefit from NACHA's systemic oversight and enforcement of operating rules governing participants in the ACH Network.[38]

Credit card transactions also are governed by federal law – Regulation Z and the Truth in Lending Act ("TILA").[39] This regulation provides protections for consumers using credit cards that are similar to, but more robust than, those for ACH debits under EFTA and Regulation E. These rights include error and dispute resolution rights, as well as limited liability for unauthorized transactions. In addition, consumers are protected by the operators of the payment card networks that enforce compliance with operating rules designed to detect and deter fraud.[40]

In contrast, remotely created checks are governed principally by Articles 3 and 4 of the Uniform Commercial Code ("UCC"), a series of state laws applicable to negotiable instruments and commercial contracts.[41] As described in section II.A.3.a(3) below, the UCC provides that consumers are not liable for a check unless it is "properly payable."[42] Unlike the defined rights of consumers under Regulation E and the EFTA, however, provisions of the UCC applicable to unauthorized checks (including remotely created checks) do not set forth specific timeframes for investigations and provide no right to the re-credit of funds during a bank's investigation. Moreover, the permissible timeframe for consumers to report unauthorized checks, and many other provisions of the UCC, can be varied by agreement or contract. These variations often

---

FR 77102 (Dec. 23, 2014). At this time, the CFPB has not taken further action on the proposal.
[37] 15 U.S.C. 1693g.
[38] *See supra* notes 30-31.
[39] *See infra* notes 172-1173 and accompanying text; TILA, 15 U.S.C. 1601 *et seq.*; Regulation Z, 12 CFR 1026.
[40] *See supra* notes 32-34 and accompanying text.
[41] Currently, the UCC (in whole or in part) has been enacted, with some local variation, in all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands.
[42] UCC 4-401 cmt. 1 ("An item is properly payable from a customer's account if the customer has authorized the payment and the payment does not violate any agreement that may exist between the bank and its customer.").

appear in the fine print of take-it-or-leave-it bank deposit agreements.[43] Technically, the UCC does not cover remotely created payment orders. As a practical matter, however, banks process remotely created payment orders the same as remotely created checks because they cannot distinguish between the two during the check clearing process.

Unscrupulous telemarketers use remotely created checks and remotely created payment orders to exploit vulnerabilities in the check clearing system, enabling them to siphon "hundreds of millions of dollars" in telemarketing transactions from consumers' bank accounts.[44] In past TSR rulemaking proceedings, the Commission was concerned with providing protection in telemarketing transactions "when consumers are unaware that they may be billed via a particular method, when that method lacks legal protection against unlimited unauthorized charges, and when the method fails to provide dispute resolution rights," as with novel payment methods like remotely created checks and payment orders.[45] In response to the original TSR rulemaking proceedings in which the Commission proposed to prohibit remotely created checks by requiring written authorization, the Commission received numerous, detailed comments from representatives of the automated payments industry and businesses demonstrating the widespread use of remotely created checks by legitimate telemarketers and sellers, as well as the lack of effective payment alternatives.[46] Based on the 1995 rulemaking record, the Commission revised its proposal and adopted the basic "express verifiable authorization" requirement for transactions involving such payment methods in section 310.3(a)(3).[47] In the most recent NPRM, however,

---

[43] *See infra* note 189 (citing bank deposit agreements shortening timeframe to 14 days).
[44] *NPRM, supra* note 1, at 41202 (citing injury estimates from law enforcement cases).
[45] *TSR Final Rule 2003, supra* note 8, at 4606.
[46] *TSR Final Rule 1995, supra* note 8, at 43850 & n.80 (noting examples of businesses, such as "two of the baby Bells, GEICO, Citicorp, Telecheck, Equifax, Bank of America, Discovery Card, Dunn and Bradstreet, and First of America Bank."); *see also TSR Revised Notice of Proposed Rulemaking*, 60 FR 30406, 30413 (June 8, 1995) (hereinafter *TSR RNPRM*).
[47] *TSR Final Rule 1995, supra* note 8, at 43850-51. Under section 310.3(a)(3), a consumer's authorization is

the Commission amassed evidence from its own enforcement actions, and those of other federal and state agencies, demonstrating that the express verifiable authorization requirement is manifestly ineffective at preventing massive consumer losses in fraudulent telemarketing transactions involving remotely created checks and remotely created payment orders. The NPRM accordingly proposed to prohibit the use of these payment methods in telemarketing transactions.

b. Cash-to-Cash Money Transfers and Cash Reload Mechanisms

Money transfer providers enable individuals to send (or "remit") money quickly and conveniently to distant friends and family, using a network of agents in various locations in the U.S. and abroad. As used in the NPRM and this Statement of Basis and Purpose ("SBP"), the term "cash-to-cash money transfer" describes a specific type of money transfer in which a consumer brings cash or currency to a money transfer provider that transfers the value to another person who can pick up cash in person.

As the NPRM described, the perpetrators of telemarketing scams frequently instruct consumers to use cash-to-cash money transfers because this method of payment is a fast way to anonymously and irrevocably extract money from the victims of fraud. Once a cash-to-cash money transfer is picked up, there is no recourse for the consumer to obtain a refund after the fraud is discovered. Cash-to-cash transfers to locations outside of the U.S. are governed by the Remittance Transfer Rule ("Remittance Rule"), part of the EFTA and Regulation E. Among other things, the Remittance Rule mandates disclosures to customers of money transfer

---

considered verifiable if it is obtained in one of three ways: advance written authorization signed by the consumer; an audio recording of the consumer giving express oral authorization; or written confirmation of the transaction mailed to the consumer before submitting the charge for payment.

providers, error resolution for mistakes, limited cancellation rights, and other protections.[48] However, the Remittance Rule provides no similar rights for consumers using other types of cash-to-cash transfers.

Cash reload mechanisms are similarly problematic. Cash reload mechanisms act as a virtual deposit slip for consumers to load funds onto a GPR card without a bank intermediary. A consumer simply pays cash, plus a small fee, to a retailer that sells cash reload mechanisms, such as MoneyPaks, Vanilla Reloads, or Reloadit packs. In exchange, the consumer receives a unique access or personal identification number ("PIN") authorization code. The consumer can use the PIN code over the telephone or Internet to transfer the funds onto any existing GPR card within the same prepaid network, apply the funds to a "digital wallet" with a payment intermediary (*e.g.*, PayPal), or pay a utility or other bill owed to an approved partner of the cash reload mechanism provider.[49] Perpetrators of telemarketing scams increasingly are instructing consumers to pay with a cash reload mechanism that the perpetrator can quickly use to offload the funds onto their own prepaid cards and thereby anonymously and irrevocably extract money from victims. As with a cash-to-cash money transfer, once a cash reload mechanism is transmitted to an anonymous con artist, the money is gone and cannot be recovered. In response to concerns about the misuse of its cash reload mechanism by perpetrators of fraud, Green Dot Corporation ("Green Dot") announced it would discontinue its MoneyPak cash reload mechanism in favor of a swipe-reload process – where a consumer presents her existing GPR

[48] 15 U.S.C. 1693*o*-1; 12 CFR 1005, subpt. B (effective October 28, 2013); *NPRM*, *supra* note 1, at 41211 & n.129.
[49] For reasons discussed in section II.B.3.c below, legitimate merchants and billers typically do not accept cash reload mechanisms directly from consumers. Instead, merchants and most billers accept as payment the GPR card itself. In the past, Green Dot Corporation permitted certain approved billing partners to accept its MoneyPak cash reload mechanisms directly from customers. Unlike perpetrators of telemarketing fraud, however, these approved billers did not use the PIN-based cash reload mechanisms to add the funds onto existing GPR cards. *See infra* note 414 and accompanying text (describing the operation of MoneyPak and other cash reload mechanisms).

card at the register and loads funds directly to the card.[50] The providers of two other cash reload mechanisms, Vanilla Reload Network and Reloadit, have made similar announcements.[51]

Like remotely created checks and payment orders, cash-to-cash money transfers and cash reload mechanisms are categorized herein as "novel" telemarketing payment methods because they lack the same error resolution rights and liability limits provided by the TILA and Regulation Z (for credit card payments) or the EFTA and Regulation E (for electronic fund transfers, ACH debits, and traditional debit card transactions). Thus, the use of cash-to-cash money transfers and cash reload mechanisms expose consumers to the risk of unrecoverable losses from telemarketing fraud. Because it appeared from the Commission's law enforcement experience that all these novel payment methods are used almost exclusively by perpetrators of telemarketing fraud, who typically ignore the TSR's "express verifiable authorization" requirement, the NPRM proposed to prohibit their use in all telemarketing transactions.

2. Proposed Expansion of Prohibition on Telemarketing Recovery Services

Telemarketers pitching "recovery services" contact victims of prior scams promising to recover the money they lost or the prize or merchandise they never received, in exchange for a fee paid in advance. Once the fee is paid, consumers rarely receive any benefit from the promised recovery services. To protect consumers from this abusive practice, section

[50] Written Statement of Green Dot Corporation For U.S. Senate Special Committee on Aging Hearing "Hanging Up on Phone Scams: Progress and Potential Solutions to this Scourge," 2 (July 16, 2014) (hereinafter "Written Statement of Green Dot"), *available at* http://www.aging.senate.gov/imo/media/doc/Green_Dot_7_16_14.pdf. *See infra* section II.B for a detailed discussion.

[51] Press Release, InComm, *InComm Expands Vanilla Reload Network, Plans to Add Swipe Reload at Over 15,000 More Retail Locations: InComm removes reload packs from stores to help prevent victim assisted fraud* (Oct. 24, 2014) (hereinafter "InComm Press Release"), *available at* http://www.incomm.com/news-events/Pages/Press%20Releases/InComm-Expands-Vanilla-Reload-Network-Plans-to-Add-Swipe-Reload-to-Over-15000-More-Retail-Locations.aspx; Testimony of William Tauscher Chairman and Chief Executive Officer Blackhawk Network Holdings, Inc. Before United States Senate Special Committee on Aging Hearing "Private Industry's Role in Stemming the Tide of Phone Scams," at 3 (Nov. 19, 2014) (hereinafter "Testimony of Blackhawk Network"), *available at* http://www.aging.senate.gov/imo/media/doc/Tauscher_11_19_14.pdf (describing Blackhawk's "elimination of quick load with the scratch-off PIN" for its Reloadit Pack product).

310.4(a)(3) of the TSR prohibits any telemarketer or seller from requesting or receiving payment for recovery services for losses in a previous telemarketing transaction "until seven (7) business days after such money or other item is delivered to that person." The Commission is eliminating the requirement that the prior loss was the result of a telemarketing transaction. This will ensure that consumers who have incurred fraud losses in non-telemarketing transactions receive the same protection against recovery services fraud.

3. Other Proposed Clarifying Amendments

The NPRM also proposed a number of technical amendments to the TSR that are designed to clarify existing provisions, as noted in the introduction. They are discussed fully in section III.

C. Overview of Comments Received in Response to the NPRM

In response to the NPRM, the Commission received more than 40 comments representing the views of state and federal agencies,[52] consumer groups,[53] consumers,[54] industry trade associations,[55] businesses,[56] a U.S. Senator;[57] and an academic.[58] The commenters generally

[52] N.J. Acting Att'y Gen. and Vt. Att'y Gen.'s Office (on behalf of 24 states and the District of Columbia) (collectively, "AGO"); Consumer Fin. Prot. Bureau ("CFPB"); Consumer Prot. Branch, U.S. Dep't of Justice ("DOJ-CPB"); Criminal Div., U.S. Dep't of Justice ("DOJ-Criminal"); and Fed. Reserve Bank of Atlanta ("FRBA").

[53] AARP; Ams. for Fin. Reform ("AFR") (on behalf of itself and Arkansans against Abusive Payday Lending; Chicago Consumer Coal.; Consumer Action; Consumer Fed'n of Am.; Consumers Union, the Advocacy and Policy Arm of Consumer Reports; Maryland Consumer Rights Coal.; Nat'l Consumer Law Ctr.; National Ass'n of Consumer Advocates; Pub. Citizen; Pub. Justice Ctr.; Florida Consumer Action Network; U.S. PIRG; and Utah Coal. of Religious Cmtys.); and the Nat'l Consumer Law Ctr. ("NCLC") (on behalf of its low-income clients and the Ctr. For Responsible Lending; Consumer Action; Consumer Fed'n of Am.; Consumers Union, the Advocacy and Policy Arm of Consumer Reports; Nat'l Ass'n of Consumer Advocates; the Nat'l Consumers League; and U.S. PIRG).

[54] Three supported all or part of the proposed amendments: Michalik, Cordero, and Frankfield. Five did not specifically address the proposed amendments: Burden, Bailey-Waddell, Manness, Seaman, and Farrington.

[55] Amer. Bankers Ass'n ("ABA"); The Clearing House and Fin. Servs. Roundtable ("The Associations"); Credit Union Nat'l Ass'n. ("CUNA"); Elec. Check Clearing House Org. ("ECCHO"); Elec. Transactions Ass'n. ("ETA"); NACHA – The Elec. Payments Ass'n. ("NACHA"); The Money Servs. Roundtable ("TMSRT"); and Nat'l Ass'n. of Fed. Credit Unions ("NAFCU").

[56] Blue Diamond Remodeling, Inc. ("Blue Diamond"); DCS Holdings Group, LLC ("DCS Holdings"); G3 Assocs.; Green Dot Corp. ("Green Dot"); InfoCision Mgmt. Corp. ("InfoCision"); Interactive Commc'ns Int'l, Inc.

supported the Commission's efforts to combat telemarketing fraud and enforce the existing provisions of the TSR. The vast majority of commenters discussed the amendments to prohibit the use of novel payment methods in telemarketing transactions. Most financial services industry and business commenters opposed all or part of the amendments curtailing novel payment methods. Law enforcement and regulators, consumer advocates, and individual consumers expressed support for the amendments, with some commenters urging the Commission to expand the prohibitions to other industries and marketing methods. Several commenters expressed their views on the amendments to the recovery services, express verifiable consent, or Do Not Call related provisions of the Rule. The comments and the basis for the Commission's adoption or rejection of the commenters' suggested modifications to the proposed amendments are analyzed in detail in sections II and III below.

II. Final Amended Rule Pertaining to the Anti-Fraud Amendments

The Commission has carefully reviewed and analyzed the entire record developed in this proceeding.[59] The record, as well as the Commission's own law enforcement experience and that of its state and federal counterparts, supports the Commission's view that the anti-fraud amendments to the TSR are necessary and appropriate to protect consumers from significant financial harm.[60] In some instances, the Commission has made modifications to its original proposal. The Final Rule addresses deceptive and abusive practices in telemarketing by:

("InComm"); Michael; NetSpend; PPA - Biondi; PPA - Frank; Samuel ("First Data"); Thayer Gate Advisors ("Thayer"); and Transp. FCU.

[57] The Hon. Bill Nelson.

[58] Prof. Sarah Jane Hughes ("Hughes").

[59] The record includes the NPRM, and the law enforcement cases and experience referenced therein, which are hereby incorporated by reference.

[60] The Commission's decision to amend the Rule is made pursuant to the rulemaking authority granted by the Telemarketing Act to protect consumers from deceptive and abusive practices. 15 U.S.C. 6102(a)(1) and (a)(3).

- Prohibiting the use of remotely created payment orders in outbound and inbound telemarketing transactions;
    - Adopting a modified definition of the term "remotely created payment order" that broadly includes checks (including "remotely created checks") and payments that are: (1) created by the payee; and (2) sent through the check clearing system;
    - Eliminating the proposed definition of the term "remotely created check;"
- Prohibiting the use of cash-to-cash money transfers and cash reload mechanisms in outbound and inbound telemarketing transactions;
    - Adopting the proposed definition of "cash-to-cash money transfer;"
    - Adopting a revised definition of the term "cash reload mechanism" to clarify the exclusion of swipe reload methods of loading funds to GPR cards; and
- Expanding the advance fee ban on recovery services to include recovery of losses incurred in previous telemarketing and non-telemarketing transactions.

A. Final Rule and Comments Received on Remotely Created Checks and Remotely Created Payment Orders

Based on its review of the entire record, the Commission concludes that the use of remotely created checks and remotely created payment orders in telemarketing is an abusive practice. In reaching this conclusion, the Commission has applied the unfairness analysis set forth in Section 5(n) of the FTC Act,[61] finding that this practice causes or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or

[61] The Telemarketing Act authorizes the Commission to promulgate Rules "prohibiting deceptive telemarketing acts or practices and other abusive telemarketing acts or practices." 15 U.S.C. 6102(a)(1). In determining whether a practice is "abusive," the Commission has used the Section 5(n) unfairness standard where appropriate. *See TSR Amended Rule 2003*, *supra* note 8, at 4614.

competition and is not reasonably avoidable.[62] In the following sections, the Commission separately: (1) reviews comments supporting the prohibition against each of the two novel payment methods, (2) reviews comments opposing the prohibition against each of them, (3) sets forth its legal analysis, and (4) describes the operation of the amended provisions, and related definitions, in the Final Rule.

1. Comments Supporting the Prohibition on Remotely Created Checks and Remotely Created Payment Orders

Numerous commenters, including members of the financial services industry, a federal credit union, small businesses, an academic, consumer advocacy groups, individual consumers, staff from federal agencies, and Offices of Attorneys General in 24 states and the District of Columbia supported the prohibition on the use of remotely created checks and remotely created payment orders in telemarketing transactions.[63] Commenters expressed support for every aspect of the Commission's proposal, specifically described reasons why it is necessary and appropriate, and some suggested that the Commission's proposal should be applied to non-telemarketing transactions.

In general, commenters in support of the prohibition argued that these payment methods are highly susceptible to fraud in telemarketing and cause significant harm to consumers in the form of unauthorized and fraudulent withdrawals from their financial accounts.[64] Commenters agreed that perpetrators of fraud frequently use remotely created checks and remotely created

[62] *See* 15 U.S.C. 45(n) (codifying the Commission's unfairness analysis, set forth in a letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction, *reprinted in In re Int'l Harvester Co*., 104 F.T.C. 949, 95-101 (1984)) (hereinafter "Unfairness Policy Statement").
[63] The states are: Arizona, Arkansas, Delaware, Hawaii, Illinois, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Nevada, New Hampshire, New Jersey (joined via separate comment letter), New Mexico, Oregon, Pennsylvania, Rhode Island, Tennessee, Utah, Vermont, and Washington. AGO at 1.
[64] DOJ-CPB at 2; AFR at 1; AARP at 3; AGO at 11; CFPB at 1; NCLC at 2-3; DOJ-Criminal at 3; Transp. FCU.

payment orders to extract money from consumer victims and inflict significant harm.[65] One small business owner suggested that businesses should never receive direct access to a consumer's account, describing it as "a perfect scenario for fraud and other deceitful actions to occur."[66] The DOJ-CPB stated that a prohibition on remotely created checks and remotely created payment orders and other novel payment methods "would prevent hundreds of millions of dollars in consumer loss each year while, at the same time, leaving open safer mechanisms for legitimate marketers to accept consumer payments."[67] In addition, the DOJ-CPB noted, "[t]he serious risks posed by RCCs are well documented in and outside of the FTC's [NPRM]," including in guidance documents published by bank regulators and public comments filed in other rulemaking proceedings.[68]

Several commenters emphasized that consumers who provide their account numbers to a telemarketer have no effective control over how that payment is processed, little understanding of the different levels of protection afforded different types of payments, and no realization that the information they provide can be used to initiate additional unauthorized debits.[69] Many commenters pointed out how the consumer protections for remotely created checks and remotely

[65] AARP at 3; AGO at 11 (reaffirming the views expressed by the Attorneys General of 34 states, the District of Columbia, and American Samoa in 2005 comment letter filed by National Association of Attorneys General, Proposed Amendment to Regulation CC Remotely Created Checks, FRB Docket No. R-1226 (May 9, 2005), *available at* http://www.federalreserve.gov/SECRS/2005/May/20050512/R-1226/R-1226_264_1.pdf); NACHA at 1; NCLC at 1, 5; Michael; DOJ-CPB at 1-2; DOJ-Criminal at 1& 3.

[66] Michael.

[67] DOJ-CPB at 1.

[68] *Id.* at 2 (citing Financial Crimes Enforcement Network, Advisory FIN-2012-A010, Risk Associated with Third-Party Payment Processors (Oct. 22, 2012); NACHA, Remotely Created Checks and ACH Transactions: Analyzing the Differentiators (March 2010); FFIEC, Bank Secrecy Act Anti-Money Laundering Examination Manual: Third-Party Payment Processors B Overview (2010); Federal Reserve Bank of Atlanta, 2008 Risk & Fraud in Retail Payments: Detection & Mitigation Conference Summary (Oct. 6-7, 2008); Public Comment filed with the Federal Reserve by the National Association of Attorneys General, the National Consumer Law Center, Consumer Federation of America, Consumers Union, the National Association of Consumer Advocates, and U.S. Public Interest Research Group in Docket No. R-1226 (May 9, 2005)).

[69] AGO at 11 (citing a "lack of consumer awareness of how strangers can debit their bank accounts without authorization"); Trans. FCU (noting that consumers do not realize their account information "can easily be used to generate additional unauthorized payments"); NCLC at 6 ("Consumers cannot protect themselves from the dangers of RCCs and RCPOs"); Michael.

created payment orders are less robust and more burdensome for consumers than those provided for credit cards and ACH debits.[70] Commenters also explained how protections for consumers whose accounts are debited via remotely created checks and remotely created payment orders are further diminished due to the lack of a systemic, centralized monitoring and identification of these payment types in the check clearing system.[71] Many commenters described how a telemarketer's choice to use a consumer's bank account information to create a remotely created check, instead of originating an ACH debit or accepting a payment card, determines the level of scrutiny and monitoring applied to the transaction and the telemarketer or seller.[72] These commenters pointed out that telemarketers and sellers using remotely created checks and remotely created payment orders are often deliberately exploiting these regulatory and operational weaknesses to escape the heightened scrutiny and monitoring of the ACH and payment card networks.

Virtually all of the commenters in support of the prohibition focused on the harm inflicted on consumers when unauthorized and fraudulent debits are withdrawn using remotely created checks and remotely created payment orders.[73] Commenters opined that the legitimate

[70] AGO at 11 (noting "the hurdles that consumers often encounter in trying to obtain a recredit to their bank account when – if at all – they discover an unauthorized debit"); NCLC at 4-5 (noting that "the use of RCCs and RCPOs is popular for scammers because the consumer protections are weak and poorly enforced . . ." and explaining how RCCs and RCPOs can make it difficult for consumers to initiate stop payment orders).

[71] AGO at 11 (highlighting "the difficulty, if not impossibility, of tracking remotely created checks"); NACHA at 3 ("RCCs are difficult, if not impossible, for individual financial institutions to monitor as a class"); NCLC at 9 ("a systemic monitoring system is lacking for the check system.").

[72] AFR at 1 ("RCCs and RCPOs are heavily used by scammers and others who wish to avoid the consumer protections and fraud prevention mechanisms associated with modern electronic payment devices"); DOJ-CPB at 2 ("we have seen third party payment processors that promote their use of RCCs as a means to process transactions for merchants that have been blacklisted from credit card and ACH transactions"); Trans. FCU ("[w]e have seen these types of payment mechanisms used by scammers, often targeting elderly or financially distressed members"); NACHA at 3 ("Because RCCs are not monitored systemically . . . fraudsters are able to use RCCs to evade the authorization requirements and strong protections that NACHA has implemented through the ACH system"); NCLC at 6 ("RCCs and RCPOs are also used by entities who wish to escape scrutiny by the systems used to detect fraud in other payment systems.").

[73] One commenter from the financial services industry, NetSpend, described the significant adverse impact that

use of remotely created checks and payment orders in telemarketing transactions, if any, is significantly outweighed by the considerable evidence of harm inflicted on consumers.[74] Citing the existence of safer modern alternatives to remotely created checks and remotely created payment orders in telemarketing transactions, such as debit cards and ACH debits, commenters argued that the reasons to prohibit their use are even more compelling today than in the past.[75] As a result, they maintained, the proposed Rule would not adversely affect legitimate telemarketers, who already accept more conventional payment methods.

Two commenters responded to the Commission's specific request for comment regarding the proposed definitions of remotely created check and remotely created payment order by proposing discrete changes that would eliminate the requirement that the check or payment order be "unsigned."[76] These commenters explained that the definition proposed in the NPRM was too narrow and technical to be fully effective, because a telemarketer engaged in fraud could

---

remotely created checks have on its prepaid Visa and MasterCard debit card business and the banks that issue its cards. Netspend at 1. NetSpend explained that its debit cards do not have checking account functionality, so any remotely created checks drawn on the card account number are automatically returned unpaid by the issuing bank. NetSpend states that "some financial institutions and their third-party vendors choose to ignore the 100% return-rate" and continue to submit remotely created checks each month against its prepaid debit cards that lack checking privileges. As a result, NetSpend reports, it pays about $75,000 per year in bank fees to just one of its card issuing banks for processing thousands of remotely created check images before the bank can automatically reject them. *Id.* NetSpend also stated that it suffered significant losses from remotely created checks originated by First Bank of Delaware – a bank that the Department of Justice sued for processing remotely created payments for "fraudulent merchants and telemarketers wishing to skirt the rules of the electronic funds transfers networks." *Id.*; *see also U.S. v. First Bank of Delaware*, Civ. No. 12-6500 (E.D. Pa. Nov. 19, 2012).

[74] AARP at 3 (concluding that "the benefit to consumers of the proposed rule outweighs the burden to businesses in complying with this rule"); Hughes at 1 ("I find the cost-benefit analysis articulated in the [NPRM] to be persuasive"); NACHA at 3 (explaining that "[i]n 2010, NACHA adopted rules (that became effective in 2011) allowing for recurring payments to be authorized over the telephone" thereby eliminating the few advantages for legitimate businesses of remotely created checks over ACH).

[75] AARP at 3 (concluding that "legitimate businesses have access to a variety of other payment methods"); AFR at 1 (noting that remotely created checks and remotely created payment orders "have few legitimate uses for which other payment systems could not substitute"); DOJ-CPB at 3 ("The FTC's proposed rule change will not adversely affect legitimate telemarketers" that can "use a variety of other payment means"); NCLC at 7 ("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.").

[76] CFPB at 2 ("The Bureau believes that the RCC and RCPO definitions ultimately adopted by the Commission should not hinge on the presence or absence of the consumer's signature"); FRBA-2 at 2 (stating that "this broader prohibition will better serve the Commission's purposes . . .").

instead insert "a graphical image of a signature into the signature block of each check or remotely created payment order" to circumvent the prohibition.[77] Instead, the commenters suggested that the Commission revise the definitions of remotely created check and remotely created payment order to make clear that both are a payment order or instruction: (1) created or initiated by the payee and (2) deposited into or cleared through the check clearing system.

Several commenters supporting the proposed Rule urged the Commission to expand the prohibition on remotely created checks and remotely created payment orders to non-telemarketing transactions.[78] These commenters argued for a complete prohibition on these payment methods in all consumer transactions, noting the existence of abuse of remotely created checks and payment orders in connection with scams perpetrated via email and other media.[79] Two of these commenters urged the Commission to work closely with the CFPB, Federal Reserve Bank, and other regulators to implement such a prohibition.[80]

Some commenters also emphasized the essential assistance provided by payment processors and merchant banks to telemarketers and sellers that use remotely created checks and remotely created payment orders to debit consumer accounts without authorization.[81] NCLC expressed the view that the Rule's existing knowledge standard for assisting and facilitating is too burdensome, and would insulate payment processors from liability for processing prohibited

[77] FRBA-2 at 2.
[78] AFR at 1; NCLC at 2; *see also* NACHA at 4 (noting that "it seems likely that bad actors would attempt to move activity online, as e-commerce is not covered by the telemarketing sales rule."). In addition, two individuals went so far as to suggest either banning all telemarketing or requiring "everything in writing." Seaman (adding, "[i]f consumers want something, they will call the company themselves"); G3 Assocs. ("It's real simple.. make them put it in writing (either snail mail or e-mail)...if they are legit they will if they won't, hang up!").
[79] AFR at 1 (urging the Commission to apply the proposed ban to "sales initiated by email or other methods that do not use a telephone"); NCLC at 4 (noting the use of these payments by internet payday lenders that provide loans to consumer in states where payday lending is illegal or where they are not licensed).
[80] AFR at 1; NCLC at 7.
[81] DOJ-CPB at 2 (noting that payment processors market the use of remotely created checks to process transactions for merchants that have been kicked out of payment card networks and ACH network); NCLC at 8 ("Payment processors and ODFIs play critical roles in the misuse of RCCs and RCPOs.").

payments for telemarketers.[82] NCLC and AFR urged the Commission to adopt a strict liability standard that would incentivize payment processors to develop robust mechanisms to ensure they are not processing these prohibited payments.[83]

2. Comments Opposing the Prohibition on Remotely Created Checks and Remotely Created Payment Orders

In stark contrast to the 1995 rulemaking proceedings in which a number of specific entities described in detail their legitimate use of and dependence on remotely created checks, in response to the current NPRM, the Commission received only one comment from a telemarketing firm covered by the amended Rule – InfoCision. InfoCision asserted generally that the amended Rule would increase the burdens on legitimate businesses and charities that rely on novel payment methods.[84] The remaining comments were submitted primarily by financial services industry members and associations.[85] Comments from the financial services industry contended that prohibiting telemarketers and sellers from using remotely created checks and remotely created payment orders would be a direct and impermissible regulation of banks, an action that exceeds the Commission's jurisdiction.[86] Overall, commenters opposed to the prohibition raised similar concerns. As described in detail below, commenters challenged the FTC's unfairness analysis, including the significance of the injury to consumers and the relative

[82] NCLC at 8.
[83] AFR at 1 ("Payment processors and the banks that originate RCCs and RCPOs should be strictly liable for processing unlawful payments"); NCLC at 7-8 ("The best way to stop RCCs and RCPOs from entering into the system and reaching consumers' accounts is to . . . hold payment processors and ODFIs strictly liable for accepting RCCs or RCPOs that violate the TSR.").
[84] InfoCision at 2.
[85] *See generally*, ABA; The Associations; CUNA; ECCHO; ETA; First Data; FRBA; NAFCU; PPA - Biondi; PPA - Frank.
[86] ABA at 7 (stating the prohibition exceeds "the FTC's mission, jurisdiction, and authority"); *see also* ECCHO at 3; The Associations at 2. Other comments acknowledged the amended Rule would not apply to financial institutions, but raised concerns about potential negative effects on the broader payment system. ABA at 7; CUNA at 1; FRBA-1 at 2; The Associations at 10. To minimize these effects, commenters encouraged the Commission to coordinate closely with the Federal Reserve Board, CFPB, bank regulators, and other stakeholders. CUNA at 1; FRBA-1 at 4; NAFCU at 1.

burdens on consumers and businesses; argued that the reach of the proposal was too broad; and suggested alternative courses of action.

While many commenters challenged the FTC's assertion that the use of these payment methods in telemarketing causes or is likely to cause substantial harm to consumers,[87] no commenter specified how or to what extent remotely created checks and remotely created payment orders are used in lawful telemarketing of legitimate products and services. For example, InfoCision claimed that novel payment methods are "extremely important" to legitimate businesses and charities that "need to offer customers multiple means of accepting payments or charitable donations" and that the amended Rule would increase the cost of collecting payments and donations but did not provide support for these claims.[88] Commenters from the financial services industry also did not provide specific support or evidence.[89]

The commenters in opposition took issue with other aspects of the unfairness analysis the Commission articulated in the NPRM.[90] According to some commenters, the Commission failed to demonstrate that the regulatory framework applicable to remotely created checks and remotely created payment orders is a source of significant harm to consumers or a sufficient justification for the amendment.[91] To buttress that argument, commenters favorably compared the consumer

[87] ABA at 2; ETA at 2; The Associations at 2; ECCHO at 13.
[88] InfoCision at 2.
[89] ABA at 1 ("we do not speak extensively in this comment letter of all of the potential legitimate uses of RCCs by telemarketing and other merchants"); DCS Holdings ("we do not have quantifiable data concerning how many businesses depend on one or more of these [payment] methods"); ECCHO at 12-13 (estimating the total number of remotely created checks cleared and returned as unauthorized in 2010 without identifying the number related to telemarketing); First Data at 7 (estimating that "thousands" of small businesses in its system accept RCCs and RCPOs, "some" of which "may be used via telemarketing transactions"); Thayer ("[the prohibition] will make business far more difficult for legitimate telemarketing firms . . ."). Furthermore, First Data, itself a credit card payment processor, described its use of remotely created checks to withdraw money from the bank accounts of start-up merchants that have yet to obtain corporate credit or debit cards. First Data at 7. First Data did not provide estimates of the number of such transactions. *Id.*
[90] ABA at 1, 3; ECCHO at 4; The Associations at 5.
[91] ECCHO suggested that the Commission "should undertake additional primary research to validate the statements in the Proposal regarding the relative burdens associated with a consumer obtaining a credit of funds to his/her

protections that the UCC affords consumers who use remotely created checks and remotely created payment orders with those afforded by the EFTA (for ACH debits and traditional debit cards) and the TILA (for credit cards).[92] Further, many argued that the Commission overstated the operational weaknesses of the check clearing system in detecting and deterring fraudulent telemarketers and unauthorized transactions.[93]

At least one commenter argued that the Commission failed to demonstrate that remotely created payment orders, themselves, caused unavoidable harm to consumers.[94] Indeed, some commenters asserted that the prohibition would do little to protect consumers when unscrupulous telemarketers thwart the Rule's existing express verifiable authorization requirements, regardless of the payment method used.[95]

Most commenters, however, aimed their critique at the final cost-benefit prong of the Commission's unfairness analysis. These commenters expressed the view that the harm, if any, inflicted on consumers is outweighed by the benefits of using remotely created checks and remotely created payment orders in telemarketing transactions.[96] Because of the inability of

---

account when making a claim of an unauthorized payment of any type (card, ACH or check)." ECCHO at 7.

[92] ABA at 8-9 (noting that, despite differences in "details and the technical legal process," the protections for consumers "are, as a practical matter, comparable . . ."); ECCHO at 6 ("the UCC and other check law protections against unauthorized RCCs are arguably better for consumers than Regulation E and Regulation Z."); The Associations at 4-5 (expressing disagreement that consumer protections for unauthorized remotely created checks and remotely created payment orders are inadequate); PPA-Biondi (same); PPA-Frank (same).

[93] PPA-Biondi; PPA-Frank.

[94] ABA at 6 (opining that the unavoidability must be connected to the cause of the harm, which is the telemarketer's initial deception, not the choice of payment system routing); *see also* ECCHO at 5 (suggesting the Commission should focus "on the actions of the telemarketer that give rise to unfair or abusive practices and not on the use of a particular payment instrument."); ETA at 1 ("it is not the payment methods themselves that are fraudulent, but rather the actors that are attempting to sell goods and services in a fraudulent manner that constitute the problem"); PPA – Frank ("The change here is just like blaming the gun and not the person who pulls the trigger . . .").

[95] ABA at 5 (stating that fraudulent telemarketers will shift to other payment mechanisms); CUNA at 2 (same); PPA-Biondi (same); *see also* ECCHO at 4 (opining that the proposed Rule will have no deterrent effect on a "telemarketer who is already violating the TSR by not obtaining customer authorization for a debit transaction of any type – ACH, card, or RCC.").

[96] ABA at 7 (noting that not all consumers have or are eligible for the conventional payment methods described in the NPRM); First Data at 3 (stating that the prohibition will result in delayed receipt of goods or services purchased over the telephone); PPA-Biondi (stating that RCCs and RCPOs benefit consumers because "there is more space

banks to distinguish remotely created checks and remotely created payment orders from traditional checks, some argued that the prohibition would have a "*per se* application beyond telemarketing" that would cause banks to refuse to accept any remotely created checks and remotely created payment orders.[97] As a result, commenters emphasized, the amended Rule would cause substantial harm to all consumers and businesses that rely on these payment methods in non-telemarketing transactions (*e.g.*, last minute payments of credit card bills, insurance premiums, and mortgages).[98] As evidence of the responsible use of remotely created checks and remotely created payment orders by legitimate businesses, ECCHO provided estimates that they asserted showed relatively low overall rates of unauthorized remotely created check adjustment claims, compared with the overall volume of such transactions.[99] In addition to their concern over curtailing currently accepted payment mechanisms, several commenters opined that any action to restrict remotely created checks and, more importantly, remotely created payment orders would stifle future innovation in payments.[100]

Some commenters opposing the prohibition offered alternatives to the Commission's proposal. These suggestions included voluntary or mandatory reporting of remotely created check and remotely created payment order return rates to the Commission by telemarketers or their non-depository payment processors;[101] requiring financial institutions to disclose to bank

---

available for providing information about the transaction to the consumer"); PPA-Frank (same).

[97] ABA at 6; *see also* DCS Holdings; ECCHO at 3; FRBA-1 at 2; PPA-Frank; The Associations at 2.

[98] ABA at 2; ECCHO at 4; ETA at 2; PPA-Biondi The Associations at 9.

[99] ECCHO estimated that banks processed approximately 2.04 million remotely created checks per day in 2009. ECCHO at 13-14. Based on a survey of three large financial institutions, ECCHO estimated the percentages and numbers of the unauthorized RCC adjustment claims to be .01264% or approximately "258 unauthorized RCCs per day industry wide." *Id.*

[100] CUNA at 1; ECCHO at 3-4; FRBA-1 at 2; NAFCU at 1.

[101] The Associations at 2, 10-11 ("Rather than prohibiting the use of RCCs and RCPOs by telemarketers altogether, we believe the FTC should impose return reporting requirements on telemarketers and their [non-depository] processors that use RCCs and RCPOs"); *compare* DCS Holdings (proposing that the Commission "require monitoring and quantifying all payment types processed for returns, volumes, velocity patterns etc.").

regulators each instance of "abnormal" or "significant" remotely created check and remotely created payment order transaction or returns activity by their customers;[102] mandating that all banks and payment processors only do business with telemarketers on a registry of telemarketers;"[103] and implementing a magnetic ink character recognition ("MICR") line[104] identifier for remotely created checks and remotely created payment orders.[105]

3. The Commission Concludes that the Use of Remotely Created Checks and Remotely Created Payment Orders in Telemarketing Meets the Test for Unfairness

In the context of TSR rulemaking proceedings, the Commission has determined to apply the unfairness test to evaluate whether certain acts and practices qualify as "other abusive telemarketing acts or practices"[106] under the Telemarketing Act.[107] As set forth in Section 5(n) of the FTC Act, an act or practice is unfair if: (a) it causes or is likely to cause[108] substantial injury to consumers, (b) the injury is not reasonably avoidable by consumers, and (c) the injury is not outweighed by countervailing benefits to consumers or competition. Based on the entire record in this proceeding, the Commission concludes that the use of remotely created checks and remotely created payment orders in telemarketing transactions meets the unfairness test and, thus, is an abusive practice.

---

[102] FRBA-1 at 4.
[103] PPA-Frank ("How about requiring alk (sic) telemarketers to register providing all product and fulfillment details for what they are selling"); DCS Holdings ("Require all banks and third party processors only do business with 'Registered' telemarketers . . .").
[104] The MICR information appears at the bottom of each check, and contains numbers that identify the bank branch, bank routing number, check number, and account number at the payor bank.
[105] ECCHO at 10; First Data at 8.
[106] 15 U.S.C. 6102(a)(1) ("The Commission shall prescribe rules prohibiting deceptive telemarketing acts or practices and other abusive telemarketing acts or practices.").
[107] *TSR Amended Rule 2003*, *supra* note 8, at 4614.
[108] Thus, the Commission need not demonstrate *actual* consumer injury, but only the *likelihood* of substantial injury. In this proceeding, however, there is sufficient evidence that the use of remotely created checks and remotely created payment orders in telemarketing causes actual injury.

a. The Use of Remotely Created Checks and Remotely Created Payment Orders in Telemarketing Causes Substantial Harm to Consumers

(1) Law Enforcement Record

The rulemaking record demonstrates the persistent, ongoing, and substantial harm caused by the use of remotely created checks and remotely created payment orders in telemarketing transactions. For nearly two decades, the Commission and its state and federal law enforcement partners have used every available tool at their disposal to combat the abuse of remotely created checks in unlawful telemarketing transactions. In many of these cases, the Commission has sought and courts have granted extraordinary equitable and monetary relief, including *ex parte* temporary restraining orders and asset freezes aimed at immediately halting the perpetrators of widespread telemarketing fraud.[109] These fraudulent schemes have victimized consumers nationwide with pitches for a variety of products, such as phony medical discount products, advance fee loans, credit card interest rate reduction services, and magazine subscriptions.

[109] Since 1995, the Commission has filed more than 300 cases involving violations of the TSR, many of which have included fraudulent or unauthorized remotely created checks. *See, e.g., FTC v. Sun Bright Ventures, LLC,* Civ. No. 14-02153-JDW-EAJ (M.D. Fla. July 20, 2015) (Stip. Perm. Inj.); *FTC v. First Consumers, LLC,* Civ. No. 14-1608 (E.D. Pa. Feb. 19, 2015) (Summ. J.); *FTC v. AFD Advisors,* Civ. No. 13-6420 (N.D. Ill. Aug. 26, 2014) (Stip. Perm. Inj.); *FTC v. Ideal Financial Solutions, Inc.*, Civ. No. 13-00143-MMD-GFW (D. Nev. Feb. 15, 2013) (Prelim. Inj.); *FTC v. Group One Networks, Inc*., Civ. No. 09-0352 (M.D. Fla. Mar. 19, 2010) (Stip. Perm. Inj.); *FTC v. FTN Promotions, Inc.*, Civ. No. 07-1279-T-30TGW (M.D. Fla. Dec. 30, 2008) (Stip. Perm. Inj.); *FTC v. 3d Union*, Civ. No. 04-0712-RCJ-RJJ (D. Nev. July 19, 2005) (default judgment); *FTC v. 4086465 Canada, Inc. d/b/a International Protection Center*, Civ. No. 04-1351 (N.D. Ohio Nov. 14, 2005) (Stip. Perm. Inj.); *FTC v. Win USA Services, Ltd.*, Civ No. 98-1614Z (W.D. Wash. Apr. 13, 2000) (Summ. J.); *FTC v. Consumer Money Markets, Inc.*, Civ. No. 00-1071-PMP-RJJ (Sept. 6, 2000) (Stip. Perm. Inj.); *FTC v. National Credit Management Group*, Civ. No. 98-936(ALJ) (D.N.J. May 4, 1999) (Stip. Perm. Inj.); *FTC v. SureCheK Systems, Inc.*, No. 1-97-CV-2015 (JTC) (N.D. Ga. June 11, 1998) (Stip. Perm. Inj.); *FTC v. National Credit Foundation, Inc.*, Civ. No. 96-2374-PHX-ROS (Apr. 10, 1997) (Stip. Perm. Inj.); *FTC v. Universal Credit Corporation*, Civ. No. 96-0114-LHM(EEx) (C.D. Cal. Dec. 6, 1996) (Stip. Perm. Inj.); *FTC v. Diversified Marketing Service Corp*., Civ. No. 96-0388M (Oct. 18, 1996) (Stip. Perm. Inj.); *FTC v. Windward Marketing, Ltd*, Civ. No. 96-0615-FMH (N.D. Ga. Oct. 10, 1996).

States have brought additional cases against telemarketers and sellers that used remotely created checks to withdraw money from consumer bank accounts without authorization. *See e.g*., *State of Ohio ex rel. v. Simplistic Advertising, Inc.*, Civ. No. 08-7232 (Franklin County, OH Ct. Com. Pl. filed May 16, 2008); *State of Ohio ex rel. v. 6450903 Canada, Inc.*, Civ. No. 05CVH7233 (Franklin County, OH Ct. Com. Pl. May 8, 2009) (default judgment).

Despite aggressive and active law enforcement actions, telemarketers and sellers continue to abuse remotely created checks and, increasingly, remotely created payment orders, to defraud consumers, as exemplified by recent cases filed by the Commission.

In the past two years alone, the Commission halted three separate telemarketing operations that were charged with using remotely created checks or remotely created payment orders to defraud thousands of consumers out of tens of millions of dollars.[110] In September 2014, the Commission sued Sun Bright Ventures, LLC, its principals, and related entities for operating a telemarketing scheme that allegedly deceived consumers into divulging their bank account information by pretending to be part of Medicare. Using consumer bank account information, the defendants allegedly used remotely created checks (and remotely created payment orders) to extract money from thousands of seniors and used tape-recorded "authorizations" to defeat consumers' disputes with their banks.[111] The Commission alleged these tape recordings were faulty, as they failed to show that the defendants obtained consumers' authorization to be debited.[112] The rates at which consumers and banks returned these transactions were grossly outside comparable industry norms for debits from consumer bank accounts.[113] For example, the defendants allegedly generated overall return rates of

[110] *See FTC v. Sun Bright Ventures, supra* note 109 (entry of stipulated monetary judgment order for $1.418,981) million); *FTC v. First Consumers, supra* note 109 (entry of $10,734,255.81 monetary judgment); *FTC v. AFD Advisors, supra* note 109 (entry of stipulated monetary judgment of $1,091,450.68).
[111] Pl.'s Mot. and Memo. In Supp. of TRO at 8-9, *Sun Bright Ventures*, Civ. No. 14-02153.
[112] Compl. ¶ 23, *Sun Bright Ventures, supra* note 109. On June 5, 2015, an FBI Special Agent filed a criminal complaint and arrest warrant charging Glenn Erikson with wire fraud in connection with his part in the *SunBright Ventures* telemarketing scheme. *U.S. v. Glenn Erikson*, Cr. No. 15-0520-MPK (W.D. Pa. June 5, 2015).
[113] Due to the decentralized nature of the check clearing system and the inability to track remotely created checks and remotely created payment orders, neither the banking industry nor the Federal Reserve maintain data on average industry return rates. Therefore, the Commission's cases have referenced NACHA return rate statistics for ACH debits as a benchmark for return rates of remotely created check and remotely created payment order transactions. *See* Pl.'s Summ. J. Ex. 50, Dec. Professor Amelia Helen Boss, ¶ 16 (Oct. 21, 2014) (hereinafter "Dec. Prof. Amelia Helen Boss"), filed in *First Consumers, supra* note 109 ("The strong similarities between RCCs and ACH transactions make comparisons of system data particularly appropriate, and, as will be discussed below, such comparisons are extremely important in the analysis of returns.").

approximately 68 percent and an unauthorized return rate of 28 percent.[114] By comparison, in 2013 NACHA reported that overall return rates for ACH debit transactions averaged just 1.42 percent, while unauthorized return rates averaged .03 percent.[115]

In March 2014, the Commission sued the perpetrators of a similar scheme targeting senior citizens: First Consumers, LLC, its principals, and related entities. The Commission charged the defendants with cold-calling tens of thousands of seniors claiming to sell fraud protection, legal protection, and pharmaceutical benefit services. In some instances, the telemarketers who carried out the fraud impersonated government and bank officials, and enticed consumers to disclose their confidential bank account information. From 2010 through 2013, the defendants used consumers' bank account information to create and deposit $18,856,360.56 in remotely created checks at various banks – $8,122,104.75 of which were returned by consumers or their banks.[116] The defendants' rate of unauthorized returns ranged from at least 1.61 percent to 9.18 percent,[117] alarmingly high in light of the 0.03 percent average industry unauthorized return rate for ACH debits and NACHA's maximum threshold of 1 percent (currently 0.5 percent) for unauthorized returns.[118] The defendants' overall return rates were similarly

[114] Compl. ¶ 37, *Sun Bright Ventures, supra* note109.
[115] *Id.* at ¶ 36; *see also* NACHA, 2013 ACH Network Return Rate Statistics (on file with the Commission); *NACHA RFC, supra* note 31, at 3-5 (citing 2012 statistics evidencing an overall ACH debit return rate of 1.5 percent and an unauthorized return rate of 0.03 percent).
[116] Pl.'s Summ. J. Ex. 75, Summary of Deposits and Returns (hereinafter "Summary of Deposits and Returns"), filed in *First Consumers, supra* note 109. These return rates vastly exceed NACHA's recently established overall return rate threshold of 15 percent for ACH debit transactions.
[117] *Id.* To calculate return rates under NACHA's rules, NACHA divides the number of ACH debit transactions by the number of returned debit transactions. Due to incomplete information on the number of remotely created checks cleared and returned from the five banks used most heavily by the defendants, it was not possible for the FTC's expert witness, Professor Amelia Helen Boss, to calculate return rates by the number of items deposited and returned. Dec. Prof. Amelia Helen Boss, *supra* note 113, at ¶ 32 & n.1, filed in *First Consumers, supra* note 109. Instead, Professor Boss calculated the defendants' return rates using the value of the deposits and returns, yielding even higher overall return rates. When calculated by value, defendants' overall return rates ranged from 8.57 percent to 46.23 percent, with unauthorized return rates between 6 percent and 16.9 percent. Summary of Deposits and Returns, *supra* note 116.
[118] *See supra* notes 30-31 and accompanying text describing NACHA's return rate thresholds and network statistics.

excessive, ranging from at least 7.79 percent to 32.13 percent.[119] On February 19, 2015, the Court granted the Commission's motion for summary judgment, and entered a final order against the individual defendant, including a permanent injunction and monetary relief in the amount of $10,734,255.81 – the total amount consumers lost.[120]

In September 2013, the Commission sued AFD Advisors and its principal, Fawaz Sebai, for operating a telemarketing enterprise that allegedly pitched a prescription drug discount card that, victims were told, would provide substantially discounted or even free prescription drugs.[121] According to the complaint, in less than a year, the Montreal-based defendants deposited nearly $2 million in remotely created checks from consumer victims, and caused additional harm in the form of non-sufficient funds ("NSF") fees resulting from defendants' unexpected withdrawals. As part of the scheme, the defendants allegedly coached their elderly victims through purported recorded authorizations that the defendants used to defeat consumers' attempts to reverse the withdrawals as unauthorized.[122] In July 2014, a federal grand jury indicted Fawaz Sebai and two other Canadian citizens on eight counts of mail and wire fraud in connection with the alleged scheme.[123] Arrest warrants have been issued, and the United States Attorney for the Southern District of Illinois will seek extradition of the defendants from Canada.[124]

---

[119] Summary of Deposits and Returns, *supra* note 116.
[120] The permanent injunction bans the defendants from all telemarketing and from accepting or depositing remotely created checks or remotely created payment orders. On the same date, the court entered default judgments (and a similar permanent injunction) against the corporate defendants in the case.
[121] Compl. ¶ 18, *AFD Advisors, supra* note 109.
[122] The Commission described to the Court how the defendants would stop the recording process if the consumer did not answer "correctly," and start a new recording. Pl.'s Mot. and Memo. In Supp. of TRO at 7, *AFD Advisors, supra* note 109. The defendants would repeat this process until they obtained a "clean" recording that purported to demonstrate the consumer's authorization.
[123] Press Release, U.S. Attorney for the Southern District of Illinois, *U.S. Seniors Deceived By Foreign Scammers In Medicare Hoax* (July 24, 2014), *available at* http://www.justice.gov/usao/ils/News/2014/Jul/07242014_Sebai%20Press%20Release html.
[124] *Id.*

The Commission's record of law enforcement cases amply demonstrates that the harm resulting from the use of remotely created checks and remotely created payment orders in telemarketing is significant.[125] Several opponents of the proposed Rule amendment questioned the significance and prevalence of injury, noting that consumers who complain to their banks obtain reversals of unauthorized remotely created checks and remotely created payment orders.[126] Declarations from consumer victims in cases brought by the Commission, however, illustrate how banks can frustrate consumers' efforts to obtain reversals of such remotely created checks. For example, when one 74-year old victim in *FTC v. Sun Bright Ventures* attempted to reverse the defendants' unauthorized remotely created check, a bank teller told her the bank could not refund the money because the victim had not reported the issue within 24 hours.[127] Only after the victim reported the matter to a police officer, who instructed her to return to the bank to demand a reversal, did the bank agree to refund the $448 that the defendants withdrew from her account.[128]

Other *Sun Bright Ventures* victims unsuccessfully attempted to reverse unauthorized remotely created checks drawn on their bank accounts.[129] For example, an 86-year-old widow's bank refused to reverse the $448 remotely created check drawn on her account because she failed to dispute it within 30 days, ignoring the fact that she had been hospitalized during the 30 days

[125] *See supra* note 109 (citing FTC and state cases).
[126] ABA at 8-9; ECCHO at 8-9; The Associations at 6.
[127] Pl.'s TRO Ex. 15 ¶ 5, filed in *Sun Bright Ventures, supra* note 111.
[128] *Id.* at ¶ 7.
[129] Pl.'s TRO Ex. 8 ¶ 3, filed in *Sun Bright Ventures, supra* note 109 (bank refused to reverse the $448 remotely created check). Other victims in the *Sun Bright Ventures* case complained that banks made it difficult to reverse the transactions. *See, e.g.*, Pl.'s TRO Ex. 7 ¶ 6-8 (only after a consumer visited her credit union a second time, and spoke to a different representative, did the credit union reverse the $399 unauthorized remotely created check); Pl.'s TRO Ex. 13 ¶ 3 (bank was "not convinced" the remotely created check was unauthorized by declarant's mother, who was diagnosed with dementia, and refused to reverse $448 withdrawal).

before she noticed the unauthorized withdrawal.[130] An 82-year old victim filed an affidavit with his bank, contesting two remotely created checks made out to the defendants for $448.52 each.[131] Initially, the bank reversed the charges and returned the money to his account. However, a few months later, the bank revoked the credit to his account because it received a voice recording of the consumer answering the defendants' "yes" or "no" questions purportedly authorizing the debits.[132] The bank revoked the refund despite the consumer's allegations that the tape was fraudulent, noting several discrepancies including the fact that he never verified his age as between 18-75, when he was in fact 82 years old, and that the representative's voice on the recording was a woman's, instead of the man with whom he had spoken.[133]

In another case, *FTC v. Handicapped & Disabled Workshops,* a declarant described how the defendants bilked his elderly mother-in-law out of thousands of dollars, including a remotely created check for $654.95.[134] Despite his existing legal power of attorney over his mother-in-law's financial affairs due to the fact she suffers from Alzheimer's disease, her bank refused to initiate a return, supposedly because she had "authorized" the withdrawal.[135]

Even when consumers can obtain reversals of the original transactions, significant consumer injury also results from collateral consequences stemming from the unauthorized bank debit, such as overdraft or NSF fees. For example, one consumer victimized by the fake IRS refund pitch used by the defendants in *FTC v. NHS Systems* grew suspicious shortly after he

---

[130] Pl.'s TRO Ex. 1 ¶¶ 4-6, filed in *Sun Bright Ventures, supra* note109.
[131] Pl.'s TRO Ex. 18 ¶¶ 4-5, filed in *Sun Bright Ventures, supra* note 109
[132] *Id.* at ¶¶ 5-6.
[133] *Id.*
[134] Pl.'s TRO Ex. 24 ¶ 21, filed in *FTC v. Handicapped & Disabled Workshops, Inc*., Civ. No. 08-0908-PHX-DGC (D. Ariz. Dec. 9, 2008) (Stip. Perm. Inj.). Another victim similarly failed to obtain reversals for approximately $1,800 of $5,500 worth of unauthorized remotely created checks initiated by the *Handicapped & Disabled Workshops* defendants from May through November 2007. Pl.'s TRO Exs. 21 & 22.
[135] Pl.'s TRO Ex. 24 ¶ 21, filed in *Handicapped & Disabled Workshops, supra* note 134.

revealed his bank account number over the telephone.[136] Despite putting a hold on his bank account and warning his bank that a fraud-induced withdrawal was going to be posted to his account, the consumer's bank charged him NSF fees resulting from the unauthorized remotely created checks initiated by the defendants. After another *NHS Systems* victim reported the unauthorized remotely created checks to his bank, the bank threatened to report his overdrawn account to a credit reporting agency. The bank ultimately agreed to waive some, but not all, of the NSF fees caused by the numerous unauthorized remotely created checks posted against his account, but still required him to bring the account to a zero balance before he could close it.[137]

Still other consumers simply never dispute such transactions with their bank in the first place.[138] As the FTC's expert witness observed in *FTC v. First Consumers,* "the victim may encounter roadblocks in attempting to achieve redress from the merchant, or simply may be embarrassed at his or her vulnerability."[139] Evidence of such underreporting can be inferred from the overall return rates generated by perpetrators of fraud. For example, the fact that a thoroughly fraudulent telemarketing scheme generates a 68 percent overall return rate implies that 32 percent of the transactions were never challenged by consumer victims.[140] Some of these consumers overlook the unauthorized or fraudulent charge altogether, fail to notice it in time to make a claim under the terms of the account agreements with their banks, or may be unaware of their option to pursue the matter with their own bank. Other consumers frequently try in vain to

[136] Pl.'s TRO Ex. 13 ¶¶ 3-5, 9, 13, filed in *FTC v. NHS Systems,* Civ. No. 08-2215-JS (E.D. Pa. Mar. 28, 2013) (Stip. Perm. Inj.).
[137] Pl.'s TRO Ex. 5 ¶¶ 8, 18, filed in *NHS Systems, supra* note 136.
[138] *See* Dec. Prof. Amelia Helen Boss, *supra* note 113, at ¶ 36, filed in *First Consumers, supra* note 109 ("many fraudulent debits go undetected by the consumer victim and, even if discovered, the victim may not assert its claim against the bank in time, or the bank may refuse to re-credit the account and return the check.").
[139] *Id.*
[140] Compl. ¶ 37, *Sun Bright Ventures, supra* note109.

pursue a refund directly from businesses on their own.[141] For example, after the defendants in *FTC v. Sun Bright Ventures* initiated a $448 unauthorized remotely created check charge to his account, one elderly victim tried for six months to resolve the matter with the defendants directly – he never received a refund.[142] In *FTC v. First Consumers*, a consumer thought she was talking to a representative of her bank, Wells Fargo, when she provided her bank account information to authorize a one-time payment of $38 for a theft protection plan from her account.[143] When she called the real Wells Fargo to inquire about the product, the representative told her that the defendants' company had no affiliation with the bank. Wells Fargo also apparently failed to advise her that, as the victim of an imposter scam, she could dispute the transaction. Instead of a $38 charge, the defendants initiated a remotely created check in the unauthorized amount of $387 against her account. The consumer tried for months to obtain a refund directly from the defendants, and never received her money back from the defendants or her bank.

Even the most aggressive and highly coordinated law enforcement cases have not been able to make consumer victims whole.[144] Consider the series of actions taken by the Commission, federal prosecutors, and bank regulators against Wachovia Bank, N.A., two of its

---

[141] *See, e.g.*, Pl.'s TRO Ex. 8 ¶¶ 8-12, filed in *FTC v. Instant Response Systems*, Civ. No. 13-0976-ILG-VMS (E.D.N.Y. Apr. 14, 2015) (Summ. J.) (describing how she spent many months trying in vain to obtain a refund from defendants after being pressured and harassed into providing her bank account information to the defendant for a home medical alert device, which cost her $840).

[142] Pl.'s TRO Ex. 6 ¶¶ 7-9, filed in *Sun Bright Ventures*, *supra* note109.

[143] Pl.'s TRO Ex. 2 ¶ 5, filed in *First Consumers*, *supra* note 109.

[144] The most recent example includes the simultaneous criminal and civil actions initiated by DOJ-Criminal and DOJ-CPB against CommerceWest Bank, of Irvine, California, for allegedly "allow[ing] one of its clients to facilitate the theft of tens of millions of dollars from the bank accounts of unsuspecting, innocent consumers." Compl. ¶ 2, *U.S. v. CommerceWest Bank*, Civ. No. 15-0379 (C.D. Cal. filed Mar. 10, 2015). Under the terms of the settlement, the bank agreed to pay $4.9 million to resolve civil and criminal complaints alleging the bank facilitated consumer telemarketing fraud schemes and violated the Bank Secrecy Act ("BSA") while processing remotely created check transactions for V Internet Corp LLC., a third-party payment processor based in Las Vegas. Press Release, DOJ, *CommerceWest Bank Admits Bank Secrecy Act Violation and Reaches $4.9 Million Settlement with Justice Department* (Mar. 20, 2015), *available at* http://www.justice.gov/opa/pr/commercewest-bank-admits-bank-secrecy-act-violation-and-reaches-49-million-settlement-justice. *See also, U.S. v. CommerceWest Bank*, Civ. No. 15-0379 (C.D. Cal. Mar. 10, 2015) (No. 3-1) (consent decree for permanent injunction and civil penalty); *U.S. v. CommerceWest Bank*, Cr. No. 15-0025 (C.D. Cal. Mar. 10, 2015) (deferred prosecution agreement and information).

payment processing customers, and one massive telemarketing enterprise.[145] In separate actions, the Office of the Comptroller of the Currency ("OCC") and the U.S. Department of Justice alleged that Wachovia Bank maintained account relationships with certain payment processors[146] responsible for depositing more than $418 million in remotely created checks on behalf of fraudulent telemarketers,[147] including the defendants in *FTC v. FTN Promotions, Inc.* ("Suntasia").[148] In 2007, the Commission charged the *Suntasia* defendants with deceptively telemarketing a variety of memberships in buyers' and travel clubs, resulting in $172 million in injury to nearly one million consumers. In settlement, the Commission and the OCC received approximately $50 million to be used for restitution; however, due to the extensive amount of injury caused by the defendants, the consumer victims were not made whole.[149]

---

[145] *U.S. v. Wachovia, N.A.*, Cr. No. 10-20165 (S.D. Fla. Mar. 16, 2010); *In the Matter of Wachovia Bank, N.A.*, AA-EC-10-16 (Mar. 10, 2010). In 2010, Wachovia agreed to pay more than $150 million in restitution to resolve the matters, and entered into a deferred prosecution agreement with the U.S. Attorney for the Southern District of Florida. *See* Press Release, United States Department of Justice, *Wachovia Enters Into Deferred Prosecution Agreement: Bank Agrees to Pay $160 Million* (Mar. 17, 2010), *available at* http://www.justice.gov/dea/divisions/hq/2010/pr031710p.html; Press Release, OCC, *OCC, Wachovia Enter Revised Agreement to Reimburse Consumers Directly* (Dec. 11, 2008), *available at* http://www.occ.gov/ftp/release/2008-143.htm.

[146] *U.S. v. Payment Processing Ctr., LLC*, Civ. No. 06-0725 (E.D. Pa. Aug. 12, 2010) (Stip. Perm. Inj.); *FTC v. Your Money Access ("YMA")*, Civ. No. 07-5147-ECR (E.D. Pa. Oct. 22, 2010) (Stip. Perm. Inj.). The FTC also brought cases against many of the telemarketers that worked with the processors.

[147] *See, e.g., Universal Premium Servs.*, Civ. No. 06-0849 (C.D. Cal. Apr. 17, 2008) (Summ. J.); *FTC v. Sun Spectrum Commc'ns. Org., Inc.*, Civ. No. 03-81105 (S.D. Fla. Oct. 3, 2004) (Stip. Perm. Inj.); *FTC v. Xtel Marketing, Inc.*, Civ. No. 04-7238 (N.D. Ill. July 22, 2005) (Stip. Perm. Inj.); *FTC v. 120194 Canada, Ltd.*, Civ. No. 1:04-07204 (N.D. Ill. Mar. 8, 2007) (Summ. J.); *FTC v. Oks*, Civ. No. 05-5389 (N.D. Ill. Mar. 18, 2008) (permanent injunction); *FTC v. Frankly Speaking, Inc.*, Civ. No. 1:05-60 (M.D. Ga. May 14, 2005) (Stip. Perm. Inj.).

[148] *FTC v. FTN Promotions, Inc. ("Suntasia")*, Civ. No. 07-1279-T30TGW (M.D. Fla. Dec. 30, 2008) (Stip. Perm. Inj.).

[149] In 2008, the *Suntasia* defendants agreed to pay more than $16 million to settle Federal Trade Commission charges, and as part of its settlement with the OCC, Wachovia paid an additional $33 million to *Suntasia* victims. *Id.;* Press Release, FTC, *Suntasia Marketing Defendants Pay More Than $16 Million to Settle FTC Charges* (Jan. 13, 2009), *available at* https://www ftc.gov/news-events/press-releases/2009/01/suntasia-marketing-defendants-pay-more-16-million-settle-ftc. Subsequently, the court found the individual defendants in the original *Suntasia* case (Byron Wolf and Roy Eliasson) in contempt of the permanent injunction, and imposed a judgment of $14.75 million against the defendants. The judgment represented the amount they illegally took from consumers in a second scheme in which they debited consumers' accounts without their consent for membership in a continuity program. *See* Press Release, FTC, *Court Finds Telemarketers in Contempt; Imposes $14.75 Million Judgment* (Jan. 31, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/court-finds-telemarketers-contempt-imposes-1475-million-judgment.

(2) Operational Weaknesses Make It Difficult to Detect and Stop Consumer Injury

Operational weaknesses in the check clearing system incentivize unscrupulous telemarketers to use remotely created checks and remotely created payment orders to initiate unauthorized and fraudulent debits to consumer accounts.[150] The check clearing system lacks the ability to distinguish remotely created checks and remotely created payment orders from other checks in the collection process. In addition, the check clearing system lacks the centralized, systemic monitoring necessary to analyze transaction trends and root out fraudulent actors. As a result, perpetrators of telemarketing fraud and unscrupulous payment processors continue to exploit these payment methods to siphon money from victims of fraud.

Comments from both supporters and opponents of the amendment agreed that the banking system lacks the ability to detect and distinguish remotely created checks and remotely created payment orders from other checks flowing through the check clearing system. To address this problem, some commenters opposed to the proposal advocated the use of a unique MICR identifier for remotely created checks. First Data suggested that "[b]anks can simply change the file formats used to send remotely created check transactions to the paying bank by adding an indicator field."[151] ECCHO stated that in June 2013 the committee responsible for

---

[150] Dec. Prof. Amelia Helen Boss, *supra* note 113, at ¶ 24, filed in *First Consumers, supra* note 109 ("fraudster may find that use of RCCs is both easier and subjects it to lower risks of detection than the use of ACH debits. . . . A payor bank will often have a pre-approval and underwriting process before it will begin to accept ACH transactions from a merchant, and that relationship is carefully monitored. Moreover, the monitoring of ACH activity by the system processor (NACHA) is much more elaborate. Thus, a fraudulent processor [or merchant] may choose to use the lower technology RCC to escape detection.").

[151] First Data at 8. *See also* Atlanta Federal Reserve Retail Payment Office, *When It Comes to RCCs, Can We Make the Invisible Visible?* (Jan. 6, 2014), *available at* http://portalsandrails.frbatlanta.org/2014/01/when-it-comes-to-rccs-can-we-make-invisible-visible.html.

developing and maintaining technical standards for MICR line information started discussions on the potential for a MICR line identifier for remotely created checks.[152]

Such proposals for ways to separately identify remotely created checks have been debated for at least the past decade, however, and there is nothing in the record to indicate that there will be a solution to the problem in the reasonably foreseeable future. Prior efforts to modify the MICR line have failed. In 2005, the Board of Governors of the Federal Reserve ("Federal Reserve") found that "without broad support for such a rule, and in light of the impracticalities of enforcement, the Board has determined not to pursue a MICR identifier for remotely created checks."[153] And, according to ECCHO, even if financial institutions supported and implemented the MICR identifier for remotely created checks, it would not necessarily provide a means for banks to monitor the transaction or returns activity of individual merchants. This is because "[a] check that is passing through multiple banks in the collection process does not carry with it information that identifies the merchant depositor [but only identifies the merchant's bank or ODFI]."[154] Therefore, while the implementation of an identifier for remotely created checks would assist in monitoring remotely created checks, the future of such proposals is speculative at best, and the barriers to centralized monitoring of RCCs and the individual merchants that issue them will remain for the foreseeable future.

---

[152] For a detailed explanation of the MICR standards committee, visit http://x9.org/. *See also* ECCHO at 10. ECCHO recently published a white paper proposing to "[d]etermine if there is industry support" for piloting a unique MICR identifier for RCCs, "with future intent for a permanent code." ECCHO, RCC Identifier White Paper at 3 (Apr. 23, 2014), *available at* http://www.eccho.org/uploads/Sec%209-1%20RCC%20Identifier%20Paper.pdf. The paper does not outline next steps or a proposed timeline.

[153] Final Rule, Regulation CC, 70 FR 71218, 71223 (Nov. 28, 2005).

[154] ECCHO at 11 ("decentralized nature of forward check presentment and check return presents operational challenges for any one network or collecting bank to see the totality of volume associated with a particular merchant.").

The decentralized nature of the check clearing system further compounds the problem of monitoring remotely created checks and remotely created payment orders.[155] Several commenters agreed there exists no centralized, system-wide monitoring of remotely created check or remotely created payment order volume or returns activity among various financial institutions.[156] As the Federal Financial Institutions Examination Council ("FFIEC") has summarized, "the check-clearing networks do not provide the level of technological and organizational controls of those in the ACH network. This lack of systemized monitoring of the electronically created payment orders increases the susceptibility to fraud by Web-based vendors and telemarketers."[157]

To counteract these deficiencies, some commenters suggested certain voluntary or mandatory reporting measures and regimes.[158] For a variety of reasons, the alternatives proposed by these commenters are equally, if not more, problematic. Creating a searchable national database or registry of all telemarketers would be costly to implement and unnecessarily burdensome for the many legitimate telemarketers and sellers that have never used remotely created checks and remotely created payment orders.[159] The same defects apply to the proposed mandate for telemarketers and payment processors to report to the Commission all return rates

---

[155] Some commenters argued that monitoring exists in the check clearing system, and suggested that the Federal Reserve Bank could calculate check return rates to monitor and deter unauthorized transactions. PPA-Biondi; PPA-Frank; First Data at 9. Comments filed by the FRBA and financial services industry did not confirm the existence of centralized monitoring by any intermediary parties. FRBA-1 at 4; *see generally* ABA; ECCHO; The Associations.
[156] FRBA-1 at 4; ECCHO at 10; NACHA at 3; NCLC at 9.
[157] FFIEC, *Retail Payment Systems Booklet – February 2010* 16 (Feb. 2010), *available at* http://ithandbook ffiec.gov/ITBooklets/FFIEC_ITBooklet_RetailPaymentSystems.pdf; *see also* NACHA at 3 ("Because RCCs are not monitored systemically (indeed, RCCs are difficult, if not impossible, for individual financial institutions to monitor as a class), fraudsters are able to use RCCs to evade the authorization requirements and strong protections that NACHA has implemented through the ACH system."); FFIEC, *Bank Secrecy Act/Anti-Money Laundering Manual, supra* note 28, at 235 ("The increased use of RCCs by processor customers also raises the risk of fraudulent payments being processed through the processor's bank account.").
[158] *See supra* notes 101 - 103 and accompanying text.
[159] *See* PPA-Frank; DCS Holdings.

for their remotely created checks and payment orders.[160] And, because the Commission lacks jurisdiction over banks, it cannot "require every bank to collect and report to its primary federal regulator" when a merchant has "abnormal" or "significant" return rates, nor can it require banks to conduct business only with telemarketers listed in a database or registry.[161] Because none of these proposed solutions provide a near-term, effective means for centralized monitoring, and each would create unnecessary and expansive regulatory burdens, the Commission is not persuaded that they are an adequate substitute for a prohibition on the use of remotely created checks and remotely created payment orders.

The record amply demonstrates that perpetrators of telemarketing fraud exploit the weaknesses of the check clearing system to avoid detection. The Commission has sued telemarketers that relied extensively on remotely created checks and remotely created payment orders to debit the accounts of consumers. In recent cases, the defendants allegedly debited the accounts of consumers with whom they have never spoken; consumers who suffer from dementia; and consumers who felt pressured or tricked into providing their bank account information by telemarketer claims about important health care benefits, Medicare, or other products and services.[162]

The record also lays bare the effect of the potential financial incentives that may encourage unscrupulous payment processors to offer perpetrators of telemarketing fraud these two payment methods that afford the least amount of oversight and transaction monitoring.[163] In

[160] *See* The Associations at 2, 10-11; DCS Holdings
[161] *See* FRBA-1 at 6; DCS Holdings; PPA-Frank.
[162] *See supra* note 109 (listing FTC cases).
[163] NCLC at 11 ("Payment processors and ODFIs rake in transaction fees from the scammers and the scammed alike"); Compl. ¶ 41, *FTC v. Automated Electronic Checking, Inc. ("AEC")*, Civ. No. 3:13-00056-RCJ-WGC (D. Nev. filed Feb. 5, 2013) ("AEC's pricing structure has been such that the income earned by AEC from returned transactions was significantly higher than the income earned from merely processing a transaction that ultimately cleared. The more returned transactions generated by AEC's client merchants, the higher the return fees earned by

many law enforcement cases, the Commission has charged that payment processors have known about or deliberately ignored underlying law violations committed by their merchant clients. Payment processors have sometimes actively helped merchant clients avoid detection and scrutiny, apparently for no reason other than to keep the transaction fees flowing. For example, the Commission alleged that certain payment processors urged fraudulent merchants to switch from ACH debits to remotely created checks and remotely created payment orders to avoid NACHA's one percent threshold for unauthorized returns[164] or used tactics to evade compliance monitoring systems designed to flag fraud.[165] In email communications and promotional materials, defendants in payment processing cases have explicitly described the systemic weaknesses of the check clearing system to detect patterns of fraud.[166]

The rulemaking record confirms the existence and harmful effect of the significant operational weaknesses within the check clearing system that incentivize perpetrators of telemarketing fraud to exploit remotely created checks and remotely created payment orders to siphon money from the bank accounts of their victims. Once deposited into the check clearing

---

AEC and its banks"); Pl.'s Mot. and Memo. In Support of Summ. J. Ex. 2, Dec. Dennis M. Kiefer ¶ 33 (Oct. 2, 2008), filed in *YMA*, *supra* note 146 (expert describing how "YMA charged fees resulting from bad ACH and [remotely created check] transactions that were many multiples of the fees they otherwise would have charged.").

[164] *AEC*, *supra* note 163, at ¶ 29 (defendants allegedly urged merchant clients to avoid NACHA's threshold by switching from ACH debits to RCPOs); *FTC v. Landmark Clearing Inc.*, Civ. No. 4:11-00826 (E.D. Tex. filed Dec. 15, 2011), Compl. ¶ 38 (No. 1) (alleging that defendants expressly advertised their RCPO processing product as a less regulated alternative to ACH transactions); Pl.'s Mot. and Memo. In Support of Summ. J. Ex. 1, Dec. Elliott C. McEntee ¶ 50 (Oct. 1, 2008), filed in *YMA*, *supra* note 146 (expressing his expert opinion that "YMA was moving its highest risk merchants from the ACH to demand drafts to avoid being detected by the Federal Reserve and NACHA. This enabled YMA to continue to assist merchants in defrauding consumers for a much longer period of time.").

[165] *AEC*, *supra* note 163, at ¶ 58 (alleging defendants advised merchants to use different billing descriptors, customer service email accounts and telephone numbers, as well as corporate names or DBAs, to "fly under the bank radar").

[166] *Id.* at ¶ 29 ("For example, in January 2008, AEC's principal Mark Turville notified one client merchant that 'NACHA is going to a 1% threshold for unauthorized transactions starting 12-21-2007 and being enforced 3-21-2008.' Turville urged the merchant to consider switching to RCPOs: 'As you know our new [RCPO] product is now being used by most of our clients and does not have a 1% restriction . . .'"). *See also infra* note 198 and accompanying text (describing marketing claims of some payment processors offering remotely created check and remotely created payment order processing services).

system, banks cannot distinguish remotely created checks and remotely created payment orders from traditional checks, making it impossible to monitor and halt fraudulent transaction activity. The likelihood of any future implementation of a unique MICR identifier or other method for tracking remotely created checks and remotely created payment orders is far from certain.[167] Even a unique identifier would not necessarily permit the monitoring of individual merchants, nor would it provide a centralized, system for monitoring remotely created check volumes and returns activity necessary to manage the risks posed by these payments in telemarketing transactions. These significant consumer protection deficiencies in the check clearing system stand in stark contrast to the centralized transaction monitoring of individual merchants conducted by the payment card networks and the ACH network.[168] For these reasons, the Commission has determined that these weaknesses in the check clearing system have allowed, and are likely to continue to allow, remotely created checks and remotely created payment orders to cause significant consumer injury in telemarketing transactions.

(3) Consumer Protections Available for Unauthorized and Disputed Remotely Created Check and Remotely Created Payment Order Transactions

The significant harm to consumers resulting from the operational weaknesses of the check clearing system (when used in telemarketing transactions) is exacerbated by differences in the laws and regulations governing conventional payment methods and novel payment

[167] ECCHO at 10 ("While ECCHO cannot unilaterally determine that an RCC identifier will be established within the check standard, ECCHO can assure the FTC that the issue of an RCC identifier will be considered at appropriate industry standards meetings."). The Commission notes that the amended Rule will not preclude the financial services industry from adopting a unique MICR identifier or implementing other measures to increase oversight and visibility of remotely created checks and remotely created payment orders. The Commission will consider the effect of such monitoring if and when it is implemented.

[168] *See supra* notes 30-34 and accompanying text.

methods.[169] Basic protections are available to consumers in credit card transactions and ACH transactions, which are subject to federal regulations. These same protections are not necessarily available in remotely created check transactions, which are subject to the UCC.[170] In particular, significant disparities exist in consumer liability for unauthorized transactions when banks disclaim liability for certain transactions or vary by agreement the timeframes in which consumers can dispute unauthorized transactions.[171]

Under Regulation Z, a consumer has no liability for unauthorized credit card transactions conducted over the telephone – so-called "card not present" transactions.[172] Consumers also have the right to dispute a credit card transaction for goods or services if there are problems with the delivery or calculation errors, among other issues, and to hold back payment while the dispute is pending.[173] Likewise, Regulation E and the EFTA provide similar, though less robust, protections against liability for unauthorized electronic fund transfers, including for traditional debit card transactions and ACH debits.[174] For instance, Regulation E imposes limited liability

[169] NACHA at 3 ("Most importantly, however, lack of Regulation E or *NACHA Operating Rule* – type protections for RCC transactions exposes RCCs to the types of heightened risks of fraud and abuse identified in the Release.").
[170] The Commission recognizes the unsettled legal landscape applicable to remotely created payment orders, including the fact that the UCC does not apply to these payments. *See NPRM*, *supra* note 1, at 41204. As a practical matter, however, banks fail to distinguish between remotely created checks and remotely created payment orders, and simply apply the UCC to remotely created payment orders. Industry commenters confirm this fact. ABA at 3; ECCHO at 14; FRBA-1 at 2; The Associations at 4.
[171] In 1995, the Federal Reserve Bank of San Francisco described the protections consumers might have under the UCC as illusory and noted the pronounced financial disincentive to accept claims by a consumer that he or she did not authorize a particular draft because the banks must bear the loss of the amount of any draft that was unauthorized. *TSR Final Rule 1995*, 60 FR at 43850.
[172] 12 CFR 1026.12(b); Regulation Z Official Staff Commentary, Supplement I, 12 CFR 1026.12(b)(2)(iii)-3 ("The cardholder may not be held liable under 1026.12(b) when the card itself (or some other sufficient means of identification of the cardholder) is not presented."). In instances involving unauthorized charges resulting from the theft or loss of the card, a consumer's liability is limited to $50. 15 U.S.C. 1643(a)(1)(B); 12 CFR 1026.12(b).
[173] 12 CFR 1026.13(a) and (d)(1). If a billing error appears on a consumer's monthly statement, a consumer may dispute the error within 60 days from the date the statement is mailed to the consumer. 12 CFR 1026.13(b)(1). In addition to these federal law protections, private payment card network rules have certain voluntary initiatives that may provide consumers with zero liability protection in many instances, with certain exceptions. *See infra* note 178 (describing voluntary zero liability protections).
[174] See 12 CFR 1005.6.

on a consumer for an unauthorized transfer, depending on how quickly she reports the loss.[175] Regulation E also establishes explicit timeframes and rights for consumers addressing disputes about unauthorized or incorrect electronic fund transfers from their bank accounts, including specific notice and investigation timeframes,[176] as well as the right to receive a provisional re-credit of disputed funds.[177] In addition, payment card network rules provide consumers with zero liability protection for debit and GPR card purchases in certain circumstances.[178]

By contrast, remotely created checks and remotely created payment orders are governed by UCC protections.[179] Commenters opposed to the prohibition argued that the UCC provides similar, if not better, protections for consumers than Regulation E and the EFTA or Regulation Z

[175] If a consumer loses an "access device," such as a debit card or ATM card, she faces tiered liability, depending upon when she notifies her bank of the theft or loss. 12 CFR 1005.6(b)(3). If the consumer reports the loss or theft of an access device within two business days from discovery of the loss or theft, the consumer's maximum liability is $50. 12 CFR 1005.6(b)(1). If the consumer notifies the bank more than two days after discovery of the theft or loss, her liability is limited to $500. 12 CFR 1005.6(b)(2). If the consumer fails to notify the bank within sixty days after her statement was mailed to her that first showed the unauthorized charges, she may be held liable for all unauthorized charges occurring after the 60-day period. 12 CFR 1005.6(b)(3). If the unauthorized transfers are made without an access device, the consumer must report them to avoid liability, within 60 calendar days of the bank's transmittal of the periodic statement that shows the unauthorized transfers. Otherwise, the consumer faces liability for any unauthorized transfers that occur after the 60-day period and potentially unlimited liability. *See* 12 CFR 1005.6(b)(3)-2, Supp. 1, CFPB Regulation E Official Staff Commentary.

[176] 15 U.S.C. 1693(b). When a consumer provides her bank notice of an error such as an unauthorized transfer or an incorrect transfer, the bank must complete an investigation of the claim within ten business days. 12 CFR 1005.11; 15 U.S.C. 1693f(a).

[177] If the bank requires a longer time to process or investigate the claim, it must provisionally credit the consumer's account for the amount disputed and can take no more than 45 days to complete its investigation, in most instances. At the conclusion of the investigation, the bank must credit the consumer's account if it determines that an error occurred. If it believes that no error occurred, the bank must send the consumer a notice explaining the findings of its investigation. 12 CFR 1005.11; 15 U.S.C. 1693f(c)-(d).

[178] For so-called signature debit card purchases (*i.e.*, without the use of a PIN) that are processed through their networks, Visa and MasterCard provide consumers with the same zero liability protections extended to credit card purchases, with certain conditions. For example, Visa states that "[r]eplacement funds are provided on a provisional basis and may be withheld, delayed, limited, or rescinded" based on "[g]ross negligence or fraud", [d]elay in reporting unauthorized use", or "[a]ccount standing and history". Visa USA, Visa's Zero Liability Policy: How it works, retrieved from http://usa.visa.com/personal/security/zero-liability.jsp (last visited May 29, 2015). *See also*, MasterCard, Zero Liability Protection, retrieved from https://www.mastercard.us/en-us/about-mastercard/what-we-do/terms-of-use/zero-liability-terms-conditions.html (last visited July 21, 2015) (providing zero liability for consumer purchases if the consumer exercised reasonable care in protecting their card from loss or theft and promptly reported to their financial institution when they knew the card was lost or stolen).

[179] *See supra* note 170 (recognizing that banks treat remotely created payment orders the same way they treat remotely created checks).

and the TILA.[180] These commenters emphasized that section 4-401(a) of the UCC provides that a bank may pay a check only when it is "properly payable."[181] Indeed, absent consumer negligence that substantially contributes to the fraud, the UCC imposes zero liability for consumers where a wrongdoer forges the consumer's signature on a check, uses a counterfeit check, forges an endorsement, or alters the amount of the check.[182] To take advantage of the UCC's limited liability for unauthorized checks, a consumer must examine her bank statement with "reasonable promptness" and provide the bank with notification "promptly" after the discovery of the fraud.[183]

Unlike Regulation E, however, according to commenters who support the amendment, these provisions of the UCC provide no legally mandated error resolution procedure or specific timeframes for enforcing the limits on liability under the UCC.[184] Instead, UCC Articles 3 and 4 generally permit banks to vary the UCC requirements by agreement or contract. For example, in its deposit account agreement, a bank can disclaim its liability for fraudulent checks,[185] so long as the bank does not disclaim "ordinary care" and complies with the mandate of UCC section 1-

[180] ABA at 8; ECCHO at 6; The Associations at 3. Commenters also emphasized that Regulation CC, Federal Reserve Operating Circular Number 3 ("Operating Circular 3"), and private clearinghouse agreements encourage paying banks to promptly re-credit their customers' accounts. *Id.*

[181] ABA at 8-9; ECCHO at 6; The Associations at 4-5.

[182] *Interbank of N.Y. v. Fleet Bank*, 730 N.Y.S. 2d 208 (N.Y. Civ. Ct. 2001) (holding that the notation "verbally authorized by your depositor" is legally equivalent to a customer's signature and can be deemed a forged signature under the UCC).

[183] UCC 4-406 (stating a general obligation of bank customers to examine their bank statements and report unauthorized alterations and signatures on checks with "reasonable promptness").

[184] As one commenter noted, to enforce compliance, the consumer may have to resort to legal action against her bank. NCLC at 4-5. *See also e.g.*, Mark E. Budnitz, *Consumer Payment Products and Systems: The Need for Uniformity and the Risk of Political Defeat*, 24 Ann. Rev. Banking & Fin. L. 247, 253 (2005) ("The UCC contains no error resolution procedure, much less a recredit right. The UCC only gives the consumer the option of suing the financial institution for violating the UCC.").

[185] *See, e.g., Cincinnati Insurance Co. v. Wachovia Bank*, 72 U.C.C. Rep. Serv. 2d (West) 744 (D. Minn. 2010) (holding that a deposit account agreement can shift liability for an unauthorized check from the bank to its customer); *but cf., Kaiser Aluminum & Chem. Corp. v. Mellon Bank*, 43 U.C.C. Rep. Serv. 2d (West) 928, 933 n.4 (W.D. Pa. 1997), *aff'd*, 162 F.2d 1151 (3d Cir. 1998) (holding a fraudulent alteration discharges the liability of a bank customer unless the customer's negligence substantially contributed to the altering of the check, despite deposit account agreement shifting liability from bank to customer).

304 to act in "good faith."[186] Indeed, some bank-customer agreements disclaim liability for paying remotely created checks and remotely created payment orders by deeming such items as authorized, without regard to the express verifiable authorization requirements of the TSR.[187]

Unlike the dedicated timeframes under Regulation E, the UCC also permits banks to define (and significantly shorten) the standard by which "reasonable promptness" will be measured.[188] Some bank-customer agreements define "prompt" reporting to be as few as fourteen days, and similarly shorten the one-year "statute of repose" codified in section 4-406(f) of the UCC.[189] The statute of repose provides that a consumer has one year within which to

---

[186] The UCC states this general rule for contracting out of liability for checks in Article 4 section 4-103(a), including the fact that the provisions of the UCC "may be varied by agreement" and that "the parties may determine by agreement the standards by which the bank's responsibility is to be measured if those standards are not manifestly unreasonable."

[187] *See, e.g.*, Wells Fargo, Consumer Account Agreement, at 23 (Oct. 29, 2014), *available at* https://www08.wellsfargomedia.com/downloads/pdf/online_disclosures/CAA/CAA-EN.pdf ("If you voluntarily disclose your account number to another person orally, electronically, or in writing, or by some other means, and the Bank determines that the context of such disclosure implies your authorization to debit your account, the Bank may treat such disclosure as your authorization to that person to issue *items* drawn against your account") (emphasis in original); Bank of America, Deposit Agreement & Disclosures, at 23 (Feb. 6, 2014), *available at* https://www.bankofamerica.com/deposits/resources/deposit-agreements.go ("If you voluntarily disclose your account number to another person orally, electronically, in writing or by other means, you are deemed to authorize each item, including electronic debits, which result from your disclosure"); Gorham Savings Bank, Deposit Account Agreement, at 2 (Aug. 2014), *available at* https://www.gorhamsavingsbank.com/uploads/PDFs/Deposit%20Account%20Agreement_0814.pdf ("If you give out your account number to a third person by telephone, you also agree that such act authorizes the recipient of the information to initiate debits to the account. You agree that the Bank may not be held liable for complying with such authorizations"); Associated Bank, Deposit Account Agreement, at 21 (June 2014), *available at* https://www.associatedbank.com/pdf/andera/deposit_account_information_booklet.pdf ("If you voluntarily give information about your Account (such as our routing number and your Account number) to a party who is seeking to sell you goods or services, and you don't physically deliver a check to the party, any debit to your Account initiated by the party to whom you gave the information is deemed authorized"); Regions, Deposit Agreement, at 9 (Mar. 2014) *available at* http://www.regions.com/virtualdocuments/Deposit_Agreement_3_6_14.pdf ("If we pay an item that you have not signed, but you have provided information identifying your account to a seller of property or services who created an item purportedly authorized by you, payment of the item is deemed to be authorized.").

[188] Section 4-406(c) requires consumers to exercise "reasonable promptness" in examining the statement and notifying the bank after the discovery of the first fraudulent check in a series. "With respect to any subsequent fraudulent check perpetrated by the same wrongdoer before the bank is notified of the fraud," section 4-406(d) requires the consumer to report the activity to the bank within a "reasonable period of time" not to exceed thirty days. Paul S. Turner, *Contracting Out of the UCC: Variation by Agreement Under Articles 3, 4, and 4A*, 40 LOY. L.A. L. Rev. 443, 454-455 (Fall 2006).

[189] Stephan C. Veltri and Greg Cavanagh, *Survey—Uniform Commercial Code: Payments*, 68 BUS. LAW. 1203, 1213 (2013) ("The [UCC] gives contracting parties wide latitude to vary the effect of the statute's terms. In the hands of some courts, the latitude seems limitless.") (citations omitted). For example, Gorham Savings Bank requires

assert fraud, regardless of the consumer's or the bank's care or lack thereof.[190] Courts have repeatedly upheld such variations of the reporting requirements of the UCC.[191] When banks significantly shorten the reporting period, it can have the same effect as a disclaimer.[192]

The ABA posits that, when combined with Regulation CC and Operating Circular 3, such "differences in the details and the technical legal process between the consumer protections for [unauthorized] check transactions and those for credit and debit cards and ACH transactions" do not result in different outcomes for consumers.[193] According to the ABA, this is because consumers indirectly benefit from the shift in warranties for remotely created checks under Regulation CC and Circular 3, which in theory incentivize paying banks to re-credit consumers' accounts for unauthorized transactions.[194] In practice, however, Regulation CC explicitly

---

customers to notify the bank of any errors, forgeries, or alterations within 14 days. Gorham Savings Bank, Deposit Account Agreement, *supra* note 187, at 3 (14 days). *See, e.g.*, Associated Bank, *supra* note 187, at 32 (14 days); Wilshire State Bank, Deposit Account Agreement, at 10 (July 21, 2011), *available at* https://www.wilshirebank.com/public/pdf/depagreeprivacy.pdf (14 days); *see also Freese v. Regions Bank, N.A.*, 644 S.E.2d 549 (Ga. Ct. App. 2007) (upholding the reduction of time period in 4-406(f) to 30 days); *Peters v. Riggs Nat. Bank, N.A.*, 942 A.2d 1163 (D.C. 2008) (60 days).

[190] Courts have found that, unlike a statute of limitations, the UCC's statute of repose is not subject to equitable tolling. *See, e.g.*, *Peters v. Riggs Nat. Bank, N.A.*, 942 A.2d 1168 ("equitable tolling cannot apply to statutes of repose"); *Estate of Decker v. Farm Credit Servs. of Mid-America, ACA*, 684 N.E.2d 1137, 1139 (Ind.1997) ("While equitable principles may extend the time for commencing an action under statutes of limitation, nonclaim statutes impose a condition precedent to the enforcement of a right of action and are not subject to equitable exceptions"); *Brighton, Inc. v. Colonial First Nat'l Bank*, 422 A.2d 433, 437 (App.Div.1980) ("The one-year period limitation . . . is not merely a statute of limitations, but a rule of substantive law barring absolutely a customer's untimely asserted right to make such a claim against the bank.").

[191] *See, e.g., Stowell v. Cloquet Co-op Credit Union*, 557 N.W.2d 567 (Minn. 1997) (enforcing agreement requiring account holder to examine his monthly statements and notify credit union of errors within 20 days of mailing statement); *Clemente Bros. Contracting Corp. v. Hafner-Milazzo*, 2014 WL 1806924 (N.Y. 2014) (14 days); *Napleton v. Great Lakes Bank, N.A.*, 945 N.E.2d 111 (Ill. App. Ct. 2011) (30 days); *Graves v. Wachovia Bank, Nat'l Ass'n*, 607 F.Supp.2d 1277 (M.D. Ala. 2009) (40 days); *Am. Airlines Employees Fed. Credit Union v. Martin*, 29 S.W.3d 86 (Tex. 2000) (60 days). *But see, In re Clear Advantage Title, Inc.*, 438 B.R. 58 (Bkrtcy. D.N.J. 2010) (finding 60-day timeframe "manifestly unreasonable"); *Mueller v. Miller*, 834 N.E.2d 862 (Ohio Ct. App. 2005) (holding an agreement for a 30-day notice unenforceable).

[192] Turner, *Contracting Out of the UCC*, *supra* note 188, at 453 ("A reporting requirement imposes an obligation on the customer to report the payment of a forged or fraudulent check within a specified period of time. The reporting requirement is not a disclaimer or waiver and does not directly vary the UCC rules on check fraud. When the time allowed for reporting is a very brief period, however, the reporting requirement can have the same effect as a disclaimer") (citations omitted).

[193] ABA at 8.

[194] *Id.* at 9 ("Amendments to Regulation CC in 2006 in 12 CFR 229.34(d) require the bank of first deposit to warrant

permits a bank of first deposit (the warranting bank) to defend a warranty claim in cases of unauthorized signature or alteration by showing that the consumer failed to discover and report the problem to her bank (the paying bank) with reasonable promptness.[195] As noted above, in some cases this may be as few as 14 days.[196]

For the reasons discussed above, the Commission finds that the regulatory framework applicable to remotely created checks, including provisions under the UCC pertaining to unauthorized and fraudulent checks, which may be varied by agreement, are more limited than those provided under Regulation E and the EFTA or Regulation Z and the TILA. This finding applies equally to remotely created payment orders, which commenters agreed are indistinguishable from remotely created checks and, therefore, are handled by banks in the same manner.[197]

Finally, the greater burdens on consumers in recovering unauthorized and fraudulent withdrawals made by remotely created checks and remotely created payment orders are known to fraudulent merchants and create a strong incentive for them to use these payment methods. The record includes examples of payment processors actively marketing remotely created check and remotely created payment order processing services for the purpose of evading the stricter consumer protection requirements of ACH debits and credit card transactions.[198] For instance,

---

that the customer whose account is being debited . . . authorized the RCC payment. The effect is to permit bank customers to dispute such transactions and to have the item returned to the bank of first deposit"); ECCHO at 9; First Data at 7; The Associations at 5.

[195] 12 CFR 229.34(d)(2) ("If a paying bank asserts a claim for breach of warranty under paragraph (d)(1) of this section, the warranting bank may defend by proving that the customer of the paying bank is precluded under U.C.C. 4-406, as applicable, from asserting against the paying bank the unauthorized issuance of the check."). The applicable provisions of Circular 3 do not alter this framework. Federal Reserve Operating Circular 3, Adjustments for Certain Warranty Claims; Errors, 20.10(f) (Dec. 2012) ("The sending bank agrees to deal directly with the requesting bank or another non-Reserve Bank party to resolve any claims or defenses related to the adjustment or the warranty set forth in Section 229.34(d) of Regulation CC with respect to the check.").

[196] *See supra* notes 189-192.

[197] ABA at 3; ECCHO at 14; FRBA-1 at 2; The Associations at 4.

[198] NCLC at 5-6 (citing examples of promotional materials for payment processors). One payment processor's

while promoting its remotely created check product, one payment processor claims on its website that "[a] consumer must visit the bank and sign an affidavit" to dispute a "Check21" transaction, in contrast to an ACH debit, which "[a] consumer can dispute . . . by phone."[199] The goal, in one processor's own words, is to avoid payment systems that "go too far with consumer protection."[200]

Thus, the Commission is persuaded that the protections available to consumers who have been defrauded by telemarketers through the use of remotely created checks are substantially less robust than the protections afforded by conventional payment systems, and that con-artists exploit these weaknesses. The UCC provides no legally mandated error resolution procedure, no recredit right, and no specific timeframes for enforcing its zero liability rule, thereby abandoning a consumer to choose between accepting an unauthorized debit or suing her bank. These deficiencies, in combination with those of the check clearing system to detect and halt fraud, create powerful incentives that attract fraudulent sellers, telemarketers and their payment

---

website states that its remotely created payment order transactions "are governed by check laws and the Uniform Commercial Code, bypassing restrictive ACH rules and regulations." Tina Brandon, National ACH, *Check 21 Payment Processing helps You Increase Sales* (Oct. 1, 2013), *available at* http://www nationalach.com/ach-blog/check-21/check-21-payment-processing-helps-businesses-increase-sales/. The Commission's cases against payment processors confirm the use of remotely created checks and remotely created payment orders as a method of skirting additional scrutiny, regulation, and consumer protections. *See* Compl. ¶ 23, *Landmark Clearing, supra* note 164 (alleging that defendants expressly advertised their RCPO processing product as a less regulated alternative to ACH transactions); Compl. ¶ 29, *AEC, supra* note 163 (defendants allegedly urged merchant clients to avoid NACHA's threshold by switching from ACH debits to RCPOs); Dec. Dennis M. Kiefer ¶ 31, *YMA, supra* note 163 (describing YMA's efforts to migrate telemarketing clients with high ACH return rates to remotely created checks); *see also* George F. Thomas, *It's Time to Dump Demand Drafts*, Digital Transactions 39 (July 2008), *available at* http://www.radixconsulting.com/TimetoDumpDemandDrafts.pdf (noting that certain "organizations believe the check-collection system provides [them] better protections than the ACH . . . in the area of consumer chargeback. This is not sufficient justification for using this instrument.").

[199] Check21.com, *ACH vs. Check21*, retrieved from http://www.check21.com/Check-21-vs-ACH html (last visited on June 24, 2015); *see also*, National Processing, *ACH vs. Check 21 – Which Is Right for You*, (Sept. 17, 2013), *available at* http://nationalprocessing.com/blog/ach-vs-check-21-which-is-right-for-you/ ("If there is a dispute a customer will have only 40 days to visit the local branch of his bank and fill out the proper forms. A stark contrast to this is the way the disputes are handled with ACH. These customers can dispute a transaction over the telephone rather than person and have an additional 20 days to file a dispute.").

[200] NCLC at 6 (citing a blog posting by Ed Starrs, CEO, MyECheck, dated June 20, 2012, retrieved from www.myecheck.com/2012/06/20/merchants-are-at-a-disadvantage-in-most-e-commerce-transactions-due-to-deficiencies-in-payment-systems/).

processors seeking to profit from unauthorized and fraudulent debits from consumers' bank accounts that go unnoticed or unrecovered.

b. The Injury Is Not Reasonably Avoidable by Consumers

Having determined that the use of remotely created checks and remotely created payment orders in telemarketing causes substantial injury, the next inquiry is whether consumers can avoid the injury. The extent to which a consumer can reasonably avoid injury is examined, in part, by analyzing whether the consumer can make an informed choice. In this context, the Unfairness Statement articulates how certain types of sales techniques may prevent consumers from effectively making their own decisions, thus necessitating corrective action.[201] The Commission seeks, through these amendments, "to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[202]

As described in the Federal Register Notice for the debt relief amendments to the TSR, consumers cannot reasonably avoid harm if they do not understand the risk of injury from an act or practice.[203] In the context of remotely created checks and remotely created payment orders in telemarketing transactions, consumers can avoid the injury only if they understand the intricacies of how the operational and regulatory frameworks of these payment methods differ from

[201] 15 U.S.C. 45(n); *see also* Unfairness Policy Statement, *supra* note 62, at 1074.
[202] Unfairness Policy Statement, *supra* note 62, at 1074.; *see also FTC v. Neovi, Inc*., 598 F. Supp. 2d 1104 (S.D. Cal. Sept. 16, 2008), *aff'd*, 604 F.3d 1150, 1158 (9th Cir. 2010) ("In determining whether consumers' injuries were reasonably avoidable, courts look to whether the consumers had a free and informed choice"); *Am. Fin. Servs. Ass'n*, 767 F.2d 957, 976 (D.C. Cir. 1985), *cert. denied*, 475 U.S. 1011, 106 S.Ct. 1185, 89 L.Ed.2d 301 (1986) ("The requirement that the injury cannot be reasonably avoided by the consumers stems from the Commission's general reliance on free and informed consumer choice as the best regulator of the market"); *see also FTC v. J.K. Publs., Inc.*, 99 F.Supp.2d 1176, 1201 (C.D. Cal 2002); *FTC v. Windward Marketing, Ltd.*, 1997 U.S. Dist. LEXIS 17114, *29–30 (N.D.Ga. Sept. 30, 1997).
[203] *TSR Amended Rule 2010*, *supra* note 8, at 48487 (citing Unfairness Policy Statement, *supra* note 62, at 1074); *In re Orkin Exterminating Co.*, 108 F.T.C. 263, 366-67 (1986), *aff'd*, 849 F.2d 1354 (11th Cir. 1988); *In re Int'l Harvester*, 104 F.T.C. 949, 1066 (1984)).

conventional alternatives. Consumers are unlikely to know that remotely created checks are not subject to the same systematic and centralized monitoring as are other payment mechanisms, or to understand the implications of such monitoring on detecting and deterring fraud. Further, consumers are not likely to know that weaker consumer protections apply when remotely created checks are used. Indeed, the various legal requirements and protections that apply to electronic transactions are not transparent to most consumers.[204] The differences between the laws that apply to bank debits processed through the ACH system as opposed to the check clearing system do not lend themselves to easy categorization, description in consumer education pieces, or oral disclosures during telemarketing calls. Helping consumers understand their rights is even more challenging when consumers have to consult individual (and non-negotiable) contracts with their bank to learn how quickly they must act to protect themselves from unauthorized remotely created check transactions. Moreover, the comparative benefits and risks of remotely created checks and remotely created payment orders or the existence of NACHA rules prohibiting outbound telemarketers from initiating ACH debits from their bank accounts are not transparent to consumers.[205]

Some opponents argued that consumers are in control of whether they give out their bank account information over the telephone to fraudsters.[206] As was the case in the debt relief industry, the ability of consumers to understand and avoid the risk of injury here too is compromised by the fact that they do not know that the goods or services offered by the

[204] *See* Budnitz, *Consumer Payment Products and Systems*, *supra* note 184, at 248 ("the development of new payment systems and recent proliferation of new payment products have created a complex and confusing marketplace in which consumers cannot adequately understand their rights and responsibilities.").
[205] *Id.* ("For consumers of payment products, the current legal landscape is incomprehensible. Different payment products are subject to very different laws, or no law at all besides contract law. Consequently, consumers' rights and responsibilities vary greatly"); NCLC at 6 ("Consumers also do not understand the different levels of protection for different types of payments.").
[206] ABA at 6.

telemarketer are a sham. The record leaves no dispute that the widespread unlawful practices employed by fraudulent telemarketers and sellers using remotely created checks cause substantial and unavoidable harm to consumers.

When fraudulent telemarketers deceive consumers into turning over their bank routing and account information, consumers have no knowledge, let alone choice, as to how the telemarketer will decide to initiate the withdrawal from their bank account.[207] The choice of whether to route a consumer's bank account information through the ACH Network or the check clearing system is exclusively in the hands of the telemarketer or seller, as is the threshold decision as to what payment information the telemarketer demands from the consumer.[208] Once the telemarketer has elected to create unsigned checks routed through the check clearing system, the telemarketer causes further economic harm that consumers cannot reasonably avoid. Namely, selecting that payment system creates more obstacles both to detection of any misconduct by industry or law enforcement and to recovery of consumer losses. The paucity of

[207] NCLC at 6 ("the consumer has no way of knowing how the payment will be processed and no effective control over how the payee processes the payments."); ABA at 5 ("Congress believes that choice of payment routing is for the merchant to decide, not the consumer."); Dec. Prof. Amelia Helen Boss, *supra* note 113, at ¶ 16 filed *FTC v. First Consumers*, *supra* note 109 ("From the perspective of a consumer dealing with a merchant and providing banking account information, it is virtually impossible to know whether an RCC or ACH item will be created; once the necessary banking information is given to the payee, the choice between the two is within the control and discretion of the payee.").

[208] Obviously, a fraudulent telemarketer can perpetrate its misdeeds through the ACH Network, depending on its tolerance for scrutiny and detection. However, unscrupulous merchants attempting to originate ACH debits must account for the scrutiny they will receive both in underwriting and risk analysis. In addition, they must account for the systemic monitoring of their transaction activity to detect violations of operating rules and regulations.

Moreover, NACHA's "TEL Rule" (abbreviation for telephone-initiated debits) specifically prohibits the use of the ACH Network by *outbound* telemarketers that initiate calls to consumers with whom they have no existing relationship. NACHA Operating Rules, Art. II, 2.5.15 (Specific Provisions for TEL Entries) (2013). The TEL Rule recognizes the inherent risk of fraud associated with the anonymous and "unique characteristics of TEL Entries, particularly given that a TEL transaction takes place in a non face-to-face environment." NACHA, TEL Brief *Risk Management for TEL ODFIs and RDFIs* Issue No. 3 (Dec. 2009), *available at* http://www.neach.org/uploads/resources/doc/tel_brief_no__3__risk_for_odfirdfi.pdf. Under the TEL Rule, only *inbound* telemarketers and sellers that have existing business relationships with consumers may obtain a consumer's authorization to initiate an ACH debit over the telephone. As evidence of a consumer's authorization of a TEL transaction, the telemarketer or seller must either: (1) record the oral authorization of the consumer, or (2) provide the consumer with written notice confirming the oral authorization prior to the settlement date of the entry. *Id.*

consumer protections available (as discussed in section II.A.3.a(3)) makes it difficult for consumers to obtain a reversal of the transaction from their bank. Further, given the difficulty of locating the telemarketing scammer, consumers typically cannot mitigate this harm by seeking a refund. In sum, the resulting harm in the form of fraudulent withdrawals from consumer bank accounts, as well as the investment of time, trouble, aggravation, and expense of attempting to obtain a reversal of such withdrawals, cannot be avoided.[209]

In opposing the amendment and the Commission's unfairness analysis, the ABA submits that the unavoidability of harm must be connected to the cause of that harm. Here, the ABA posits, the unavoidable harm is the telemarketer's initial deception, and not the telemarketer's choice of payment system routing.[210] The Commission agrees with the ABA's comment to the extent it observes that a seller's or telemarketer's misconduct through misrepresentation or omission undermines the consumer's decisionmaking process and is not reasonably avoidable. However, the initial deception is only one aspect of the seller's behavior that causes substantial injury and is not reasonably avoidable. The telemarketer's use of remotely created checks causes equally unavoidable harm to consumers by taking advantage of another obstacle to the free exercise of consumer decisionmaking – the fact that reasonable consumers are unlikely to know or understand the implications of the telemarketer's choice of payment routing.

The ABA further argues that, unless unavoidability is connected to the telemarketer's deception, the Commission will cast as unavoidable any injury resulting from a merchant's decisions about its operations – a business's choice between two competing debit card networks,

[209] As the Ninth Circuit noted in *FTC v. Neovi*, *supra* note 202, at 1158, "[r]egardless of whether a bank eventually restored consumers' money, the consumer suffered unavoidable injuries that could not be fully mitigated."
[210] ABA at 6.

for example.[211] The Commission finds this argument unpersuasive. A merchant's choice between two competing debit card networks has no effect on consumer protections against fraud because both transactions are covered by Regulation E and subject to the same centralized monitoring regime. This result is in stark contrast to the practices documented in the rulemaking record where a telemarketer deliberately chooses to route a consumer's payment through a specific payment system that affords the consumer less protection from fraud and provides the telemarketer with more ability to evade scrutiny than other payment systems and regulatory frameworks.[212]

Here, telemarketers' misrepresentations and use of remotely created checks and remotely created payment orders routed through the check clearing system undermine consumers' decisionmaking, thereby causing unavoidable substantial injury. This conclusion is amply buttressed by the absence of reliable information in the rulemaking record to identify any legitimate uses of remotely created checks and remotely created payment orders in telemarketing transactions covered by the Rule.

c. The Benefits of Remotely Created Checks and Remotely Created Payment Orders in Telemarketing Do Not Outweigh the Harm to Consumers

The final prong of the Commission's unfairness analysis recognizes that costs and benefits attach to most business practices and requires the Commission to determine whether the harm to consumers from remotely created checks and remotely created payment orders in

[211] *Id*. at 5.
[212] For the same reasons, the Commission is equally unpersuaded by the ABA's other examples of business decisions in which consumers have no choice (*i.e*., the credit reporting agency that a business may consult and the choice of telecommunications company that a business uses to call consumers).

telemarketing is outweighed by countervailing benefits to consumers or competition.[213] Commenters opposed to the amendment have advanced numerous arguments regarding the benefits of remotely created checks and remotely created payment orders, including that there are legitimate uses of these payments in non-telemarketing transactions. The commenters also argue that fraud will continue despite the prohibition. In addition to the public comments, the Commission has considered its own rulemaking history in which the Commission proposed and ultimately declined to adopt a similar provision in 1995 because it deemed sufficient benefits to accrue to consumers from the use of remotely created checks. As a result of the development of numerous payment mechanisms available to consumers with checking accounts, the use of alternative payments by legitimate telemarketers, and the rulemaking record as a whole, the Commission is now persuaded that any historical benefits of remotely created checks in telemarketing are no longer cognizable. Today, the vast majority of consumers with checking accounts have debit cards linked to their accounts.[214] Moreover, the current rulemaking record contains no specific examples of legitimate telemarketers' and sellers' use of remotely created checks and remotely created payment orders.[215] Further, the Commission concludes that consumers and competition benefit from the bright line rule that a prohibition provides.

---

[213] *TSR Amended Rule 2010*, 75 FR at 48485 (employing cost benefit analysis in determining debt settlement amendments to the TSR).

[214] Federal Reserve Bank of Boston, *The 2011 and 2012 Surveys of Consumer Payment Choice*, at Table 2 (Sept. 2014) (hereinafter "2011 and 2012 Surveys of Consumer Payment Choice"), *available at* http://www.bostonfed.org/economic/rdr/2014/rdr1401.pdf (finding 85 percent of consumers have had a traditional debit card). For the small percentage of checking account holders without traditional debit cards, there exist few, if any, barriers to obtaining debit card access. It is not known whether consumers without such traditional debit cards also lack other payment cards, such as credit cards or GPR cards.

[215] *TSR Final Rule 1995*, *supra* note 8, at 43850. The Commission received only one comment from a telemarketing firm, InfoCision, but it did not provide support for its conclusory statement that novel payment methods are important to legitimate businesses and charities. InfoCision at 2. InfoCision's website states that it "work[s] with a roster over 200 clients across industries, including Fortune 500 companies and the nation's leading nonprofit organizations." InfoCision, Our Clients *available at* http://www.infocision.com/CompanyInfo/Clients/Pages/default.aspx (last visited June 10, 2015). InfoCision's website identifies numerous clients, including Easter Seals, March of Dimes, American Diabetes Association, and

According to some commenters, the benefits of remotely created checks and remotely created payment orders in telemarketing transactions for consumers with checking accounts include the convenience of paying for impulse purchases of goods and services sold over the telephone when the consumer does not have (or wish to use) another form of payment.[216] Other commenters argued that consumers also benefit from the ability to receive more detailed transaction information than ACH debits provide and better protection against identity theft than paper checks sent through the mail.[217] The asserted benefits for telemarketers and sellers include faster settlement times than ACH debits,[218] the ability to accept payments quickly and easily over the telephone from any consumer with a checking account,[219] and the potential savings in transaction costs over comparable payment alternatives.[220]

Unicef. A review of the individual donation websites for each listed client indicates they accept card payments directly from consumers, suggesting that the inability to employ novel payment mechanisms should not be a major problem at least when dealing with the vast majority of consumers who have payment cards.

[216] ABA at 7 ("[remotely created checks] allow a customer that does not have a debit, credit, or prepaid card to purchase goods that the customer would otherwise be denied"); First Data at 3 (noting that consumers could be delayed in receiving goods or services); InfoCision at 2 (stating that legitimate businesses and charities "need to offer customers multiple means of accepting payments or charitable donations").

[217] First Data at 3 (citing increased risks of identity theft for checks sent through the mail); PPA-Biondi ("many of the alternative methods don't provide enough transaction information for the consumer"); PPA-Frank (same).

[218] ABA at 6 (emphasizing the speed of settlement compared to ACH transactions in certain circumstances), *but see infra* note 225 (describing improvements to the ACH Network providing for same-day settlement).

[219] ABA at 6 (highlighting the ability of businesses to accept payments from consumers that do not have other types of payment methods); First Data at 4 (describing the lost sales opportunities for sellers that "would be left without a timely and reliable payment mechanism when transacting business with a consumer that solely relies upon checks"); FRBA-1 at 3 (noting reasons why businesses may choose remotely created checks and remotely created payment orders over ACH debits); PPA-Frank (noting that merchants that do not meet credit standards necessary for ACH origination services need remotely created checks).

[220] InfoCision at 2 ("Traditional methods [of payment] are more costly and time consuming"). The NPRM requested, but the Commission did not receive, specific comments detailing what additional costs, if any, would result from using payment alternatives to remotely created checks and remotely created payment orders in telemarketing transactions. *NPRM*, *supra* note 1, at 41223. To the extent that remotely created checks and remotely created payment orders may cost telemarketers and sellers less than comparable payments, such as ACH, any modest cost benefits do not outweigh the significant harm to consumers. As one provider explains on its website, remotely created checks and remotely created payment orders are "an alternative to ACH payment processing and specifically designed for businesses and industries classified as high risk merchants." National ACH website, *supra* note 199. Notably, these providers do not explicitly mention cost savings when comparing remotely created checks and remotely created payment orders with ACH payments. Check21 website, *supra* note 199.

The Commission first considered these benefits of using remotely created checks (referred to as "demand drafts") in telemarketing transactions during the original 1995 TSR rulemaking proceeding when it proposed to require written authorization for remotely created checks. At that time, few electronic payment methods were available for consumers and businesses. For example, less than 15 percent of all consumer transactions were conducted with credit and debit cards, while checks and cash accounted for the remaining 85 percent of consumer transactions.[221] NACHA had not yet introduced electronic check applications that would enable consumers and businesses to utilize the ACH Network for non-recurring payments and credits.[222] Opponents to the 1995 proposal to require written authorization for remotely created checks included numerous telemarketers, sellers, and payment processors. These commenters characterized this payment method as an innovative and important part of the future development of electronic payments and provided specific examples of their legitimate use in telemarketing and non-telemarketing transactions.[223] Against that rulemaking record, which identified the lack of available electronic payment methods for consumers, widespread use by legitimate telemarketers and non-telemarketers, and potential alternative methods of verifying consumer authorization, the Commission instead adopted the express verifiable authorization requirements of the current Rule.

Since then, and despite the express verifiable requirements of the TSR, telemarketers and sellers have continued to perpetrate fraud via remotely created checks and remotely created

---

[221] *TSR Final Rule 1995, supra* note 8, at 43850 & n.79.

[222] Consumers and businesses used the ACH Network primarily for facilitating recurring credits (*i.e.*, payroll and retirement benefits) and recurring debits (*e.g.*, insurance premiums and mortgage payments). *See* Terri R. Bradford, *The Evolution of the ACH* (Dec. 2007), *available at* http://www kansascityfed.org/Publicat/PSR/Briefings/PSR-BriefingDec07.pdf.

[223] *TSR Final Rule 1995, supra* note 8, at 43850-51; *see also TSR RNPRM, supra* note 46, at 30413-14 & n.63.

payment orders, resulting in the persistent, ongoing, and substantial harm to consumers.[224] During the same time period, remarkable developments in technology and the law have paved the way for new electronic payment alternatives and the widespread adoption by consumers of various card-based payments, electronic fund transfer methods, and online payments. As NACHA highlighted, the ACH system has evolved to enable consumers to initiate debits conveniently and securely in many situations where remotely created checks used to be needed by consumers (*i.e.* for last minute bill-pay scenarios) or preferred by merchants (*i.e.* for recurring debits and to receive same day settlement of funds).[225] Commenters in support of the prohibition agreed that today consumers who wish to purchase goods or services from telemarketers and sellers can use payment options such as credit or debit cards or ACH debits (for certain telemarketing transactions) that provide robust and consistent protection against fraud, are subject to systemic monitoring, and offer the same convenience as remotely created checks and remotely created payment orders.[226]

Studies of consumer payment preferences document the decline in check usage and the rise in the adoption of credit, debit, and prepaid cards, as well as online bill payment options and ACH debits.[227] According to the Federal Reserve Bank of Boston, 97.1 percent of American consumers have adopted one or more types of payment card.[228] Similarly, the Federal Reserve's 2010 Survey of Consumer Finances demonstrates that the "usage of electronic forms of payment,

[224] See section II.A.3.a(1).
[225] NACHA at 3; NCLC at 7. On May 19, 2015, NACHA announced that its voting membership approved amendments to the NACHA Operating Rules enabling same-day ACH settlement services, which means ACH debits will clear as quickly as remotely created checks and remotely created payment orders. Press Release, NACHA, *NACHA Leads Industry Toward Ubiquitous, Same-Day ACH Settlement* (May 19, 2015Mar. 18, 2014), *available at* https://www.nacha.org/rules/same-day-ach-moving-payments-faster.
[226] AARP at 3; AFR at 1; NCLC at 7; DOJ-CPB at 3; Transp. FCU.
[227] The Commission notes that consumers increasingly are using prepaid debit cards, mobile payments, and online payment accounts (*e.g.*, PayPal) to purchase goods and services. Unlike remotely created checks, remotely created payment orders, and ACH debits, however, these payment alternatives do not require a bank account.
[228] 2011 and 2012 Surveys of Consumer Payment Choice, *supra* note 214, at Table 6

including ATMs, debit cards, automatic bill paying, and smart cards [closed-loop GPR cards], has risen from about 78 percent of households in 1995 to almost 94 percent of households in 2010."[229] In 2013, the Federal Reserve summarized these adoption and usage patterns by consumers and noted the precipitous decline in checks, finding that "[b]y 2012, about two-thirds of consumer and business payments were made with payment cards [*i.e.*, credit, debit, and prepaid cards]."[230] The same study concluded that card-based payments "increased their share from 43 percent of all noncash payments in 2003 to 67 percent in 2012, while the use of ACH grew more modestly, increasing from a share of 11 percent in 2003 to 18 percent in 2012."[231] In turn, "[c]hecks represented nearly half (46 percent) of all noncash payments in 2003, but only 15 percent in 2012."[232]

In the United States, debit cards have become the most widely used noncash payment instrument, substituting for a significant number of cash, check, and credit card payments at the point of sale and initiated over the telephone or Internet.[233] The decline in check usage and the

---

[229] Loretta J. Mester, *Changes in the Use of Electronic Means of Payment: 1995 – 2010: An Update Using the Recently Released 2010 Survey of Consumer Finances*, 95 Business Review 25 (Third Quarter 2012), *available at* http://www.philadelphiafed.org/research-and-data/publications/business-review/2012/q3/brq312_changes-in-use-of-electronic-means-of-payment-1995-2010.pdf.

[230] The Federal Reserve System, *The 2013 Federal Reserve Payments Study: Recent and Long-Term Payment Trends in the United States: 2003 – 2012*, 12 (Dec. 2013) (citations omitted) (hereinafter "Recent and Long-Term Payment Trends in the United States: 2003-2012"), *available at* https://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf. The survey also found that "[c]ompared with credit, debit, ACH, and check, prepaid card payments (including both general-purpose and private-label) increased at the fastest rate from 2009 to 2012 (15.8 percent annually), reaching a total of 9.2 billion transactions in 2012. The number of prepaid card payments increased 3.3 billion from 2009 to 2012, which is higher growth than reported in previous studies." *Id.* at 8. *See also*, BANKING ON PREPAID 2 (The Pew Charitable Trusts June 30, 2015) (reporting that between 2012 and 2014 use of GPR cards grew by 50 percent, and estimating that approximately 23 million Americans, more than one-quarter of whom do not have a checking account, are now regularly using such cards), *available at* http://www.pewtrusts.org/en/research-and-analysis/reports/2015/06/banking-on-prepaid.

[231] *Recent and Long-Term Payment Trends in the United States: 2003-2012*, *supra* note 230, at 12.

[232] *Id.*

[233] *Id.* (debit and prepaid cards accounted for 45 percent of all noncash payments in 2012); *see also* Bank for International Settlements, Committee on Payment and Settlement Systems, *Innovations in Retail Payments*, 23 (May 2012), *available at* http://www.bis.org/publ/cpss102.pdf. Because remotely created checks (and remotely created payment orders) require a checking account at a financial institution, comparisons with usage rates for electronic

rise in the adoption of payment cards, as well as online bill payment options and ACH debits, contradict the assertions of some commenters that consumers with checking accounts need remotely created checks and remotely created payment orders to make telemarketing purchases. [234] Other comments made conclusory allegations that legitimate telemarketers use remotely created checks and remotely created payment orders, but no comment provided specific evidence of such purported legitimate use in telemarketing transactions covered by the Rule.[235] Consumer preferences and their adoption of payment methods necessarily influence merchants' willingness to accept particular payment instruments, even if, as one commenter generally asserts, it may cost more to do so.[236] Accordingly, as some commenters in support noted, legitimate telemarketers and sellers already accept conventional payment methods.[237] Indeed, when 97.1 percent of U.S. households have adopted one or more types of payment card, is not surprising that legitimate telemarketers and sellers no longer rely on remotely created checks as a method of payment. The rulemaking record contains numerous cases demonstrating that

---

fund transfers (*i.e.*, ACH debits and traditional debit cards linked to consumer checking accounts) are more relevant for purposes of this rulemaking than comparisons with usage rates for credit cards.

[234] Certain opponents of the prohibition claim that the additional transaction information available for remotely created checks and remotely created payment orders is a benefit to consumers, enabling them to better understand the nature of the withdrawals to their accounts. PPA-Biondi; PPA-Frank. Whether such additional transaction information exists (assuming it is truthful), however, does nothing to prevent the harm of unauthorized withdrawals in the first place or to mitigate the damage after unauthorized withdrawals have occurred.

[235] *See supra* note 89 and accompanying text. The Commission received only one comment from a telemarketing firm (InfoCision). While InfoCision states that the prohibition on using novel payment methods in telemarketing will harm legitimate companies, it does not provide specific evidence of transactions or merchants that use these methods. InfoCision at 2. Other commenters provided examples of legitimate transactions conducted over the telephone – to make last-minute credit card payments, pay mortgage or other bills, or receive payments in business-to-business transactions – that are not telemarketing transactions covered by the Rule or the proposed prohibition. ABA at 3; ECCHO at 2; First Data at 7; The Associations at 9. None of these commenters provided any specific information on the number of legitimate telemarketers that rely on remotely created checks and remotely created payment orders.

[236] *See supra* note 220.

[237] AARP at 3; NCLC at 7; DOJ-CPB at 3; Transp. FCU.

deceptive sales techniques and fraud accompany the use of remotely created checks and remotely created payment orders in telemarketing.[238]

Specifically, comments representing the views of financial institutions – including those serving as banks of first deposit ("BOFDs") for bank customers that purportedly deposit remotely created checks and remotely created payment orders in legitimate telemarketing transactions – failed to provide data or even anecdotal evidence about the number of bank customers that do so.[239] The Commission notes that the BSA and associated anti-money laundering ("AML") laws and regulations require financial institutions to engage in initial and ongoing customer due diligence (a process referred to as Know Your Customer ("KYC")).[240] As ECCHO recognized, a "BOFD is required under federal law to apply its [KYC] policy to its merchant and merchant processor customers to understand their business and ensure that their business is and continues to be legitimate."[241] Despite these obligations, including the monitoring of accounts to identify suspicious activities, comments from the financial services industry lacked information on the number and types of customers that would be affected by the prohibition.

Similarly, comments from one payment processor speculated that "thousands" of its merchants rely on these payment methods, but failed to report the number of its own merchant clients engaged in telemarketing that use remotely created checks and remotely created payment

[238] *See supra* note 109 and accompanying text.
[239] ABA at 1 & n.1 (describing the organization as representing banks of all sizes and charters); ECCHO at 1 ("ECCHO is a non-profit clearinghouse owned by 3,000 financial institutions"); The Associations at Appendix A (noting the membership of The Clearing House and The Financial Services Roundtable).
[240] The BSA is codified at 12 U.S.C. 1829b, 12 U.S.C. 1951-1959, 18 U.S.C. 1956-1957 & 1960, 31 U.S.C. 5311-5314 and 5316-5332, with implementing regulations at 31 CFR Ch. X.
[241] ECCHO at 11, citing 31 CFR 1020.210 (Customer Identification Programs for Banks); *see also* The Associations at 7-8 (citing bank regulatory guidance documents emphasizing the responsibility of financial institutions to "take steps to know and monitor their customers in order to prevent unauthorized RCCs from entering the payment stream.").

orders.[242] The only telemarketing firm to submit comments also provided no data on the number of its telemarketing clients that would be affected by the prohibition.[243]

As evidence of the widespread legitimate use of remotely created checks, ECCHO provided an estimate that it asserted showed an overall average of 258 unauthorized remotely created check adjustment claims per day, compared to 2.04 million remotely created checks deposited each day.[244] The Commission finds this estimate unpersuasive and largely irrelevant, as ECCHO's figures materially underestimate the incidence of problematic remotely created checks and remotely created payment orders. First, as ECCHO recognized, its estimate included only unauthorized remotely created check *adjustment* claims, not check *returns*.[245] A check *adjustment* claim is an interbank process, distinct from banks' check-collection and check-return processes, which banks use to make financial adjustments related to checks pursuant to agreements between themselves.[246] A check *return* is an automated means by which a paying bank returns a check unpaid to a depository bank. Because the return process is automated, paying banks use this process to return remotely created checks that were unauthorized by

[242] First Data, itself a credit card payment processor, also stated that it uses remotely created checks and remotely created payment orders in limited scenarios when it telemarkets its payment processing services to small, start-up businesses which do not yet have access to a corporate credit card. First Data at 7. Although First Data did not estimate the number of such transactions, the Commission notes that business-to-business telemarketing transactions (with a few exceptions not relevant here) are exempt from the TSR.

[243] InfoCision at 1 ("InfoCision provides a full spectrum of direct marketing services, including inbound and outbound call center solutions, direct mail and fulfillment, and interactive (web), and data solutions.").

[244] ECCHO at 13-14.

[245] *Id.* at 13 & n.19 ("We would note that the sampling that was conducted for this purpose was limited to RCCs handled by banks in the adjustment process. It is possible that during this sampling period there were also a material number of additional unauthorized RCC claims/items that were handled by paying banks as returns rather than adjustments.").

[246] For example, after the paying bank's midnight deadline to return a check has passed, it might use a check adjustment claim to recover the amount of the check from the depositary bank, provided that the appropriate agreements between the banks are in place. *See, e.g.*, 12 CFR 229.2(xx), comment 1, example (b) (stating that an adjustment request is not a paper or electronic representation of a substitute check, because it is not being handled for collection or return as a check).

consumers. The choice of whether to initiate an adjustment or a return is up to the paying bank.[247]

Second, ECCHO's estimate relied on adjustment claims data for only those items coded as "unauthorized," which fails to account for the variety of return reason codes used by banks when returning fraudulent remotely created checks and payment orders. Indeed, because there are no universal definitions for return reason codes,[248] a paying bank may classify the grounds for return as a breach of warranty, an irregular signature, or simply use the catchall "refer to maker."[249] Moreover, when a consumer's account has been debited repeatedly without authorization, it may become overdrawn and trigger an NSF return, or the consumer may close the account, resulting in a "closed account" return reason code.[250] Accordingly, the OCC advises that banks "should not accept high levels of returns *regardless of the return reason*." [251]

Finally, unauthorized return rates, and even overall return rates, necessarily fail to account for those victims who do not detect the fraudulent withdrawals or who have been

---

[247] *See* Check Image Central, *Resolving Duplicates As Adjustments Versus Returns*, at 2-4 (Dec. 2006), *available at* http://checkimagecentral.org/pdf/ResolvingDuplicatesAsAdjustmentsVersusReturns.pdf (describing the advantages and disadvantages to each method of dishonor, and explaining that the choice is up to the paying bank).

[248] *See* Check Image Central, *Proper Use of Return Codes in Image Exchange*, at 1 (Dec. 20, 2014), *available at* http://checkimagecentral.org/pdf/ProperUseOfReturnCodesInImageExchange.pdf ("The Uniform Commercial Code (UCC) and Regulation CC (Reg. CC), do not include a list of specific reasons that an item may be dishonored and returned. However with image exchange, the . . . [standard] exchange format provides a list of return reasons and associated codes that must be used for image exchange.").

[249] Dec. Prof. Amelia Helen Boss, *supra* note 113, at ¶ 36, filed in *First Consumers*, *supra* note 109 (describing several reasons why "unauthorized return rates [alone] may greatly underestimate the true number of unauthorized transactions.").

[250] *Id.*

[251] OCC, OCC Bulletin 2008-12: Risk Management Guidance n.7 (Apr. 24, 2008) (emphasis added), *available at* http://www.occ.gov/news-issuances/bulletins/2008/bulletin-2008-12.html; *see also* FFIEC, *BSA/AML Examination Manual, Third-Party Payment Processors – Overview* 237 (Nov. 17, 2014), *available at* http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_063.htm ("[A] bank should thoroughly investigate high levels of returns and should not accept high levels of returns on the basis that the processor has provided collateral or other security to the bank."). This also holds true for ACH return rates. *See supra* notes 30-31 (describing NACHA's return rate thresholds, including a new 15 percent overall return rate threshold).

thwarted in obtaining a return by the reporting timeframes of the UCC and their bank deposit agreements.[252] Thus, the Commission does not find ECCHO's estimates persuasive.

A different objection was raised by commenters asserting that the prohibition would prevent, directly or indirectly, a variety of legitimate transactions conducted over the telephone for which remotely created checks and remotely created payment orders are preferable for businesses, citing insurance premium payments, last-minute credit card bill payments and the collection of debts.[253] Thus, opponents argued, the Commission must weigh the costs of a total prohibition on remotely created checks and remotely created payment orders and consider the widespread benefits of such payments to all consumers and businesses. However, the amended Rule covers only telemarketing transactions involving a plan, program, or campaign to induce the purchase of goods or services subject to the TSR. As such, the use of remotely created checks in other transactions conducted over the telephone, including the examples of non-telemarketing transactions cited by commenters, would not be prohibited.

Nevertheless, some commenters anticipate that processors and banks will cease processing all remotely created checks and payment orders because they will fear liability under the TSR's prohibition against assisting and facilitating a Rule violation.[254] The risk of unwittingly processing remotely created checks or remotely created payment orders on behalf of a telemarketer appears exaggerated.[255] The TSR prohibition against assisting and facilitating

---

[252] *Id.* ("The most important reasons why the return rates understate the number of unauthorized returns, however, stem from the fact that the rate is completely dependent upon the victim discovering the unauthorized activity and following a prescribed method of seeking reimbursement. . . . [M]any fraudulent debits go undetected by the consumer victim and, even if discovered, the victim may not assert its claim against the bank in time, or the bank may refuse to re-credit the account and return the check.").

[253] *See supra* note 98 and accompanying text. The Commission notes that these examples are not telemarketing transactions covered by the TSR.

[254] *See, e.g.*, DCS Holdings; ETA at 1; FRBA-1 at 2.

[255] Notably, First Data, the only payment processor to file a comment, never suggested that it would cease processing remotely created checks and remotely created payment orders altogether. First Data at 4.

violations of the TSR is not a strict liability standard. Instead, liability depends upon a showing that the alleged facilitator knew or consciously avoided knowing that the telemarketer was violating the TSR prohibitions against remotely created checks and remotely created payment orders.[256] Non-bank providers of remotely created check processing services subject to the Commission's jurisdiction will continue to implement and enforce appropriate KYC policies and procedures, as already required by their financial institutions,[257] to determine which of their merchant-customers are engaged in covered telemarketing activities.[258] Indeed, currently payment processors routinely conduct risk assessments and ongoing monitoring that should include a basic understanding of each merchant-customer's marketing methods and a review of unusual changes in transaction activity. To investigate suspicious spikes in reversals of transactions by merchant-consumers (or other signs of fraudulent activity), payment processors already have in place policies and procedures designed to ensure they know which of their merchant-customers engage in telemarketing and, therefore, must comply with certain authorization requirements.[259] For example, section 310.3(a)(3) of the TSR requires

[256] 16 CFR 310.3(b).

[257] As discussed above, banks also have in place Know Your Customer requirements, policies, and procedures to understand their customers' (and their payment processor's customers') businesses. *See supra* notes 240-241 and accompanying text; *see also* Ana R. Cavazos-Wright, Federal Reserve Bank of Atlanta, An Examination of Remotely Created Checks at 14-15 (May 2010) ("Banks' risk management programs must address their customers' use of remotely created checks to ensure the integrity of the check clearing network is preserved. Strong risk management practices such as customer due diligence at account origination and during the customer relationship are the first line of defense against fraudulent transactions.").

[258] Financial institutions themselves will continue to enforce KYC requirements as well. For example, First Data asserted that "[m]any of the egregious business types cited in the proposal such as phony telephone offers, bogus charity solicitations, purported medical discount plans, illegal online gambling, etc. are high-risk areas that should have been properly screened by the depository bank. In these cases, the depository bank could have prevented this activity through properly applying Know Your Customer policies and complying with the FDIC and/or OCC Third-Party Processor Guidelines."). First Data at 8. *See also* Transp. FCU. ("the proposed rule changes should not unduly restrict legitimate commerce, particularly involving already regulated financial institutions. . .").

[259] States requiring express written authorization or signed confirmation before submitting payment against a consumer's account include: Arkansas (ARK. CODE ANN. 4-99-203(b)(1)); Hawaii (HAW. REV. STAT. 481P-1); Kansas (KAN. STAT. ANN. 50-672(c)); Kentucky (KY. REV. STAT. 367.46955(5)); Montana (MONT. CODE ANN. 30-14-1411(1)(e)); and Vermont (9 VT. STAT. ANN. 2464(b)(2)).

telemarketers and sellers to obtain (and retain)[260] evidence of a consumer's express verifiable consent to be charged when using payment methods that are not credit or debit cards. The same is true for payment processors that initiate ACH debits for merchant-customers, as NACHA Operating Rules require payment processors (also referred to as "Third-Party Senders") and their merchant-customers to meet the authorization requirements for TEL Entries.[261] The Commission, therefore, is persuaded that remotely created check payment processors (and banks) can and will continue to identify the marketing methods used by their merchant-customers and keep processing remotely created checks for those merchant-customers not engaged in telemarketing. For the same reasons, the Commission also is persuaded that payment processors will not face increased compliance costs.[262]

Finally, comments in opposition to the Rule argue that the prohibition will not benefit consumers because perpetrators of fraud will continue to submit remotely created checks and remotely created payment orders without consumers' authorization or simply switch to other payment methods.[263] The Commission disagrees that the prohibition will have little or no impact in reducing consumer harm.[264] First, these comments overstate the ease with which perpetrators

---

[260] *See* 16 CFR 310.5(a)(5) (requiring telemarketers and sellers to keep, for a period of 24 months from the date the record is produced, certain records, including all verifiable authorizations received under the Rule).

[261] *See supra* note 208 (describing the authorization requirements for TEL Entries (either obtaining a tape recording of the consumer's oral authorization or providing, in advance of the settlement date of the entry, written notice to the consumer that confirms the oral authorization)).

[262] First Data asserted that it would take considerable time and expense to implement automated processes to block remotely created checks for telemarketing transactions. First Data at 4. Similarly, CUNA stated that "financial institutions and other entities will have to make appropriate risk management changes." CUNA at 2. Neither CUNA nor First Data identified any expenses they would incur, over and above those currently incurred for compliance with KYC and BSA, and other existing requirements. The fact that existing compliance obligations should necessitate determining whether customers are engaged in covered telemarketing undermines industry's claims about possible increased compliance costs.

[263] ABA at 5 (arguing the FTC has failed to demonstrate that a ban will "measurably address the problem" because unscrupulous telemarketers will simply shift to other payment instruments); First Data at 3 ("prohibiting the use and acceptance of remotely created checks in telemarketing transactions does not provide any meaningful benefit to consumers . . ."); *see also* ECCHO at 4; FRBA-1 at 2; The Associations at 8-9.

[264] The Commission is not alone in this conclusion. As the NCLC comment noted, several years after the

can gain and maintain access to traditional payments channels like the ACH Network. For example, originating depository financial institutions ("ODFIs") are familiar with and already must take steps to ensure compliance with NACHA's TEL Rule prohibiting ACH debits in outbound telemarketing transactions.[265] Second, based on the injury estimates in the law enforcement cases in the rulemaking record, hundreds of millions of dollars in consumer injury could be minimized or prevented by restricting the use of remotely created checks and remotely created payment orders in telemarketing.[266] Neither the existing TSR nor the amended Rule can eliminate all telemarketing fraud. No statute or rule can. However, the provisions of the TSR provide vital guidance to industry and create a level playing field for legitimate marketers. Such rules also guide consumers and form the basis for effective consumer education campaigns and law enforcement actions that protect consumers from deception and abuse.

In sum, the evidence in the rulemaking record demonstrates that the harm to consumers, in the form of unauthorized and fraudulent charges from remotely created checks and remotely created payment orders in telemarketing transactions vastly outweighs the benefits to consumers or competition. With the advent of payment alternatives offering the same convenience and more consumer protection against unauthorized charges, the past benefits of remotely created checks and remotely created payment orders no longer remain cognizable. Studies on consumer payment preferences confirm consumers' migration to electronic payment alternatives including

---

Commission adopted the express verifiable authorization requirements of the TSR, the Canadian Payments Association ("CPA") banned the use of remotely created checks (referred to as "tele-cheques"). In doing so, the CPA "considered whether procedures could be put in place to sufficiently mitigate the risks associated with this payment instrument" and found "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." Canadian Payments Association. *Prohibition of Tele-cheques in the Clearing and Settlement System - Policy Statement* (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.

[265] *See supra* note 208.

[266] *See NPRM*, 78 FR at 41207 & n.84 (describing injury estimates from cases).

online bill pay, ACH debits, traditional and prepaid debit cards, and credit cards. In turn, the rulemaking record contains only conclusory assertions that legitimate telemarketers and sellers use or rely on remotely created checks and remotely created payment orders. Moreover, the Commission concludes that a prohibition against the use of remotely created checks and remotely created payment orders in telemarketing will serve to push telemarketers engaged in illegal conduct to use payment methods that are subject to greater monitoring and afford greater protections to consumers. A prohibition also will provide the telemarketing industry with bright lines for compliance with the Rule. These changes will benefit both consumers and competition.

d. Additional Policy Arguments Do Not Alter the Commission's Conclusion

Some commenters argued that a prohibition on remotely created checks and remotely created payment orders will result in the fragmentation of the payment system and amounts to a direct and impermissible regulation of banks, an action exceeding the FTC's jurisdiction. The direct regulation of telemarketing under the TSR, however, is a proper exercise of the Commission's authority to protect consumers from deceptive and abusive telemarketing practices. Indeed, the Telemarketing Act specifically directed the Commission to promulgate and enforce the TSR to address deceptive and abusive telemarketing practices.[267] The final Rule is consistent with the Commission's authority under the Act.

Rather than further fragmenting the payment system, the Commission believes that the prohibition will result in clearer compliance obligations for telemarketers and sellers. Under the existing TSR and state law, telemarketers and sellers already are subject to a variety of overlapping restrictions and requirements regarding the acceptance of certain payment methods.

[267] 15 U.S.C. 6101-6108.

For example, telemarketers and sellers must abide by state laws that mandate prior written authorization for remotely created checks or other debits from consumer bank accounts.[268] Like the express verifiable authorization requirement for remotely created checks in section 310.3(a)(3) of the existing TSR, the prohibition against remotely created checks is a direct regulation of telemarketers and sellers covered by the TSR, not a regulation of the payment system or financial institutions. Such compliance obligations for telemarketers and sellers already affect the criteria used by payment processors to conduct initial due diligence and ongoing monitoring of their clients engaged in telemarketing.

Finally, some commenters argued that the Commission's analysis demonstrated a pure policy preference for ACH transactions over checks. They expressed the opinion that, because ACH debits and remotely created checks are both payee-initiated withdrawals from consumer bank accounts, they share the same risk profile in telemarketing. In support of this position, commenters cited FTC cases against telemarketing frauds and payment processors that used ACH debits. As described in section II.A.3 above, the regulatory framework, due diligence, and centralized monitoring of the ACH Network generally provide consumers with more robust consumer protections against fraud. Even with the added safeguards of the ACH Network, NACHA has never permitted the use of ACH debits in outbound telemarketing, due to the substantial risk of fraud in telephone-initiated transactions.[269] It is appropriate, therefore, to prohibit the use of remotely created checks and remotely created payment orders, which provide fewer safeguards than ACH debits in telemarketing transactions.

[268] *See supra* note 259.
[269] NACHA, TEL Brief *Risk Management for TEL ODFIs and RDFIs* Issue No. 3, *supra* note 208 (the TEL Rule recognizes the inherent risk of fraud associated with the anonymous and "unique characteristics of TEL Entries, particularly given that a TEL transaction takes place in a non face-to-face environment.").

4. Final Rule Language

The NPRM proposed adding to the TSR new definitions for "remotely created check" and "remotely created payment order." As proposed, the definition of remotely created check mirrored the definition used in Regulation CC. The definition of remotely created payment order closely tracked the definition of remotely created check, but was broad enough to encompass electronic payment orders that most closely resemble remotely created checks.

The Commission solicited public comment as to whether the proposed definitions adequately, precisely, and correctly described each payment alternative. In response, the Commission received relevant comments from the Federal Reserve Bank of Atlanta and the CFPB. Both commenters expressed concern that the definitions were too narrow to be effective. Specifically, they emphasized the limitations of including a requirement that the check or payment order be "unsigned," because a telemarketer or seller could easily apply a "graphical image of a signature" to the signature block of a check or payment order to circumvent the prohibition.[270] The Commission agrees that the definitions should be modified to reduce the likelihood of circumvention.

Based on the record evidence, the Commission concludes that there are two defining characteristics of remotely created checks and remotely created payment orders. First, these payments are created or initiated by the payee-merchant, not the payor-consumer. Second, these payments are deposited into or cleared through the check clearing system, not the ACH Network. The new definition incorporates these two elements. In addition, based on the convergence of paper and electronic payments in the check clearing system, the Commission thinks it appropriate to combine the definition of remotely created check with the definition of remotely

[270] FRBA-2 at 2.

created payment order. Therefore, the amended Rule eliminates the separate definition of remotely created check, and includes a single definition of remotely created payment order, which includes any payment instruction or order drawn on a person's account that is (a) created by or on behalf of the payee and (b) deposited into or cleared through the check clearing system. To be clear, the term includes, without limitation, a "remotely created check," as defined in Regulation CC, Availability of Funds and Collection of Checks, 12 CFR part 229.2(fff), but does not include a payment order cleared through an Automated Clearinghouse or subject to the Truth in Lending Act, 15 U.S.C. 1601 *et seq.*, and Regulation Z, 12 CFR part 1026, *et. seq*.

In practice, the amended Rule prohibits telemarketers and sellers from accepting any payment order, instruction, or check, whether electronic, imaged, or paper, that is remotely created by the payee *and* deposited into the check clearing system. As the rulemaking record demonstrates, when combined with the weaknesses of the check clearing system, these types of payee-initiated withdrawals pose a significant risk in telemarketing transactions.

The payments landscape is constantly evolving to meet the needs of consumers and businesses, as evidenced by recent payment innovations, including mobile payments, digital wallets, and virtual currencies. The Rule amendments do not and cannot address the benefits and risks of all existing or future electronic payment alternatives.[271] The Commission is confident, however, that the amended Rule's definition of remotely created payment order is sufficiently tailored and flexible to protect consumers from telemarketing fraud while enabling the use of current and future payment alternatives. For example, a payment order or instruction sent

[271] The Commission continues to monitor developments in the marketplace, including developments and improvements in payments utilized by telemarketers and sellers, to ensure that consumers are adequately protected against telemarketing fraud while balancing the needs of businesses. For example, the Commission published a 2013 report entitled "Paper, Plastic. . . or Mobile? An FTC Workshop on Mobile Payments" which summarized consumer protection concerns surrounding the increase in use of mobile payments, including dispute resolution, data security, and privacy.

through the ACH Network would not qualify as a remotely created payment order under the definition. The definition also excludes so-called "digital checks" that a consumer creates and sends via a smartphone application, for example, as long as the payment was not created by the payee-merchant. The Commission recognizes that, unlike remotely created payment orders and remotely created checks, such digital checks or "electronic payment orders" could provide consumers with robust authentication features to ensure that the transaction has been initiated and authorized by the account holder.

To implement the prohibition against the use of remotely created payment orders in outbound telemarketing transactions, the Commission amends section 310.4(a) to add a new subsection (9). Section 310.4(a)(9) of the amended Rule states that it is an abusive practice for a seller or telemarketer to create or cause to be created, directly or indirectly, a remotely created payment order as payment for goods or services offered or sold through telemarketing or as a charitable contribution solicited or sought through telemarketing.

Section 310.6(b) exempts certain types of inbound telemarketing calls from TSR coverage. For example, inbound calls from consumers in response to general media advertisements are exempt from coverage, with the exception of a few types of products and services.[272] Similarly, inbound calls from consumers in response to a direct mail solicitation that provides material disclosures and makes no misrepresentations are exempt from coverage.[273]

[272] The Rule excludes from the general media exemption the following products and services: investment opportunities, business opportunities other than business arrangements covered by the Franchise or Business Opportunity Rules, credit card loss protection plans, debt relief services, credit repair services, recovery services, and advance fee loans. 16 CFR 310.6(b)(5). The exceptions to the general media exemption reflect the Commission's law enforcement experience with deceptive telemarketers' use of mass media to advertise "certain goods or services that have routinely been touted by fraudulent sellers using general media advertising to generate inbound calls." *2003 TSR Amendments*, *supra* note 8, at 4658.

[273] Inbound calls in response to direct mail advertising, like general media advertising, are exempt from coverage under the Rule. 16 CFR 310.6(b)(6). The Rule also excludes from the direct mail exemption investment opportunities, business opportunities other than business arrangements covered by the Franchise or Business

The NPRM proposed changes to the general media and direct mail exemptions that would prohibit the use of remotely created checks and remotely created payment orders in inbound telemarketing transactions by sellers that wish to take advantage of the exemption.

Only one commenter, First Data, offered specific comments on this aspect of the proposal. First Data suggested that the Commission should adopt an amendment akin to NACHA's TEL Rule that would permit the use of remotely created checks and remotely created payment orders in inbound telemarketing transactions.[274] First Data argued that, like ACH debits, the use of remotely created payment orders should be permitted in inbound transactions.[275] However, the same operational and regulatory weaknesses associated with the use of remotely created payment orders exist equally in inbound and outbound telemarketing calls. Specifically, unlike ACH debits subject to NACHA's TEL Rule, remotely created checks and remotely created payment orders are not subject to centralized monitoring or identification and expose consumers to the lesser remedies of the UCC.

For these reasons, the Commission has determined that the prohibitions in section 310.4(a)(9) should apply to both outbound and inbound telemarketing. However, to minimize the burden on sellers and telemarketers that have qualified for the general media and direct mail exemptions from the TSR for inbound telemarketing, the Commission has modified the proposed amendments to sections 310.6(b)(5) and (6). The purpose of the modification is to clarify that sellers and telemarketers that comply with the prohibition on the use of remotely created payment orders (including remotely created checks) in inbound telemarketing remain exempt from the TSR's requirements if they otherwise qualify for the general media or direct mail

---

Opportunity Rules, credit card loss protection plans, debt relief services, credit repair services, recovery services, and advance fee loans. *Id.*

[274] First Data at 6.

[275] *Id.*

exemptions. Thus, they only are covered by the TSR if they violate the prohibition. Moreover, while non-compliance with one of these prohibitions subjects the violator to a TSR enforcement action for the violation, it does not deprive the violator of its exemption from the other requirements of the TSR.

B. Final Rule and Comments Received on Cash-to-Cash Money Transfers and Cash Reload Mechanisms

Money transfer providers enable individuals to send (or "remit") money quickly and conveniently to distant friends and family using a network of agents in different locations in the U.S. and abroad. As used in the current rulemaking proceeding, the term "cash-to-cash money transfer" describes a specific type of money transfer in which a consumer brings currency to a money transfer provider that transfers the value to another person who picks up currency at the money transfer provider's location or agent in a different location. The definition does not include money transfers that meet the definition of "electronic fund transfer" in section 903 of EFTA.

As the NPRM described, the perpetrators of telemarketing scams frequently instruct consumers to use cash-to-cash money transfers because this method of payment is a fast way to extract money anonymously and irrevocably from the victims of fraud. As discussed in section I.B.1.a above, cash-to-cash money transfers are: (1) not subject to the same limits on liability and error resolution procedures as ACH debits and traditional debit cards; (2) not subject to voluntary zero liability protection as provided for certain GPR card transactions; and (3) not subject to the same robust dispute resolution procedures as for credit card payments.[276] Indeed, after a cash-to-cash money transfer is picked up, there is no recourse for the consumer to obtain a refund. This

[276] *See also supra* notes 175-177 (discussing ACH debits and traditional debit cards); 36 & 178 (discussing GPR cards); and 172-173 (discussing credit cards).

is true even for those cash-to-cash transfers made to locations outside of the U.S., which are governed by the Remittance Rule under Regulation E. Moreover, cash-to-cash money transfers are not subject to the same systemic monitoring and rules framework applied to ACH debits or card payments.[277]

Increasingly, perpetrators of fraud are migrating from using cash-to-cash money transfers to cash reload mechanisms. Cash reload mechanisms are codes or devices that act as a virtual deposit slip for consumers to load funds onto a GPR card without a bank intermediary. A consumer simply pays cash, plus a small fee, to a retailer that sells a cash reload mechanism, such as MoneyPak, Vanilla Reload Network, or Reloadit.[278] In exchange, the consumer receives a unique access or authorization code to use over the telephone or Internet to load the funds onto an existing GPR card within the same prepaid network, to add cash to a "digital wallet" with a payment intermediary (*e.g.*, PayPal), or to pay a utility or other bill owed to an approved partner of the cash reload mechanism provider. Perpetrators of telemarketing fraud persuade consumers to buy a cash reload mechanism and provide the PIN code directly to the perpetrator over the telephone. The perpetrator can then offload a victim's money onto its own prepaid card and thereby anonymously and irrevocably extract money from its victims. As with cash-to-cash money transfers, once a cash reload mechanism is transmitted to an anonymous con artist who has loaded the funds onto his GPR card, the money is gone and cannot be recovered.

Like remotely created checks, remotely created payment orders, and cash-to-cash money transfers, cash reload mechanisms lack the same dispute resolution rights provided for card-based payments and ACH debits under the TILA and Regulation Z or the EFTA and Regulation

[277] *See supra* section I.B.1.a (discussing systemic monitoring of ACH Network and payment card system).
[278] There are three major providers of cash reload mechanisms in the United States: Green Dot Corporation (MoneyPak); InComm (Vanilla Reload Network); and Blackhawk Network California, Inc. (Reloadit).

E, respectively.[279] As such, these novel payment methods expose consumers to a substantial risk of unrecoverable losses from telemarketing fraud. Because the Commission's law enforcement experience showed that such payment methods are used extensively by perpetrators of telemarketing fraud, who typically ignore the TSR's "express verifiable authorization" requirement, the NPRM proposed to prohibit their use in all telemarketing transactions.

Since the publication of the NPRM, all three major cash reload providers have developed alternatives to PIN-code cash reload mechanisms for adding funds to GPR cards. In July 2014, Green Dot acknowledged the risk that cash reload mechanisms pose to consumers and announced the complete discontinuance of its MoneyPak cash reload product by mid-2015.[280] Users of Green Dot's prepaid products can now reload their cards by swiping them at a cash register. The swipe-reload is a "card-present" transaction, which prevents scammers from using a cash reload mechanism to load their own GPR cards remotely. In October 2014, InComm also announced the phase-in of a swipe reload process and the discontinuance of its cash reload mechanism, Vanilla Reload packs, at all retail stores in 2015.[281] In November 2014, Blackhawk Network testified that it has created new alternatives to its "quick reload" Reloadit cash reload mechanism, including a swipe reload process.[282]

---

[279] As noted above, the Rule's definition of "cash-to-cash money transfers" excludes transfers that are electronic funds transfers as defined in section 903 of EFTA, which provides for dispute resolution procedures. Cash reload mechanisms are not currently governed by Regulation E. The CFPB's proposed Prepaid Account Rule seeks to extend to "prepaid accounts" the protections of Regulation E and the EFTA, with certain important modifications. Prepaid Account Rule, *supra* note 36, at 77102. Although the proposed Prepaid Account Rule arguably might be read to cover cash reload mechanisms, the error resolution and liability limits of Regulation E would not be available unless the cash reload mechanism is "registered" (*i.e.*, the consumer provides "identifying information such as name, address, date of birth, and Social Security Number or other government-issued identification number so that the financial institution can identify the cardholder and verify the cardholder's identity."). *Id.* at 77166. Thus, unregistered cash reload mechanisms would not be covered by the error resolution and liability limits of Regulation E under the proposed Prepaid Account Rule. The Commission may revisit the definition of cash reload mechanism if warranted by a final Prepaid Account Rule.

[280] Written Statement of Green Dot, *supra* note 50, at 2.

[281] InComm Press Release, *supra* note 51.

[282] Testimony of Blackhawk Network, *supra* note 51, at 3 (highlighting the company's "elimination of quick load

1. Comments Supporting the Prohibition on Cash-to-Cash Money Transfers and Cash Reload Mechanisms

Ten commenters, including consumer advocacy groups, staff from state and federal agencies, and a United States senator, supported a prohibition on the use of cash-to-cash money transfers and cash reload mechanisms in telemarketing transactions.[283] These comments advanced several common arguments, summarized below.

a. Cash-to-Cash Money Transfers

Many commenters agreed that the basic characteristics of cash-to-cash money transfers make them susceptible to abuse in telemarketing transactions. Commenters noted that such transfers provide a quick and convenient means for perpetrators of telemarketing and other frauds to receive money from their victims at locations around the world.[284] The speed of the transfers, commenters argued, enables perpetrators to disappear with the funds within minutes of transmission.[285] In addition, commenters noted that such transfers can be picked up in cash from remote locations with little or no identification, which allows scammers "to remain practically anonymous when retrieving their victim's money."[286] Supporters of a prohibition emphasized that the lack of chargeback protections exacerbates the injury sustained by victims of telemarketing fraud.[287] As a result, some commenters noted, perpetrators exploit cash-to-cash

---

with the scratch-off PIN and enhanced fraud mitigation efforts . . .").

[283] AARP; AFR; AGO; DOJ-CPB; DOJ-Criminal; Michalik; NCLC; NetSpend; Hon. Bill Nelson; Transp. FCU.

[284] AGO at 4 & nn.9-10 (noting that Western Union has more than 489,000 agent locations and MoneyGram has approximately 244,000 agents).

[285] AGO at 3; DOJ-Criminal at 2; NCLC at 11.

[286] NCLC at 11; *see also* AGO at 2 (noting that cash-to-cash money transfers can be "picked up by a person with a forged ID in many different locations"); DOJ-Criminal at 2 (stating that fraudsters "can rapidly receive and transfer victim proceeds with less regulatory or industry oversight than traditional payment methods such as checks and payment cards").

[287] AGO at 4 ("Compounding the difficulty for consumers is the fact that unlike with fraudulent credit card payments or unauthorized bank debits, senders of money transfers have no established right to a refund once their transfer has been picked up, regardless of how fraudulent the conduct of the receiver was in inducing the transaction.").

money transfers in connection with nearly every type of mass-marketing fraud, including so-called 419 scams from West Africa,[288] lottery, loan, investment, and work-at-home schemes, and "the grandparent scam."[289]

Comments supporting the amendment acknowledged that the amount of actual consumer loss is unknown, but agreed that losses to consumers are significant.[290] Because legitimate telemarketers and sellers do not rely on cash-to-cash money transfers, the commenters argued that a prohibition would have "little to no impact on legitimate businesses."[291] Commenters emphasized that the effectiveness of the prohibition will depend on the efforts of cash-to-cash money transfer providers to detect and deter the use of their money transfer systems by telemarketers.[292] Some commenters argued that money transfer companies provide substantial assistance or support to those who engage in violations of the TSR.[293] NCLC opined that money transfer providers lack sufficient financial incentives to detect misuse systematically because every money transfer earns a fee.[294] According to DOJ-CPB, "[e]ven when fraud may be clear

[288] The term "419 scam" encompasses a variety of common confidence scams. The number "419" refers to the article of the Nigerian Criminal Code dealing with fraud.
[289] AGO at 4-5.
[290] *See* AARP at 3 (AARP agrees with the FTC that these payment methods "pose a significant threat to potential victims of telemarketing fraud."); AGO at 5 (noting that the overall extent of the problem "cannot be known with precision, but it is clearly very substantial"); DOJ-CPB at 1 (stating that losses resulting from "global mass-marketing fraud is in the tens of billions of dollars per year"); NCLC at 12 (reporting that in 2012 cash-to-cash money transfers were the top method of payment in telemarketing fraud reported to the National Consumer League's Fraud Center, "accounting for nearly 63 percent of all telemarketing payments (up from 49 percent in 2009).").
[291] NCLC at 12 (suggesting that, when used in the telemarketing context, such transfers are "merely vehicles for evading consumer protections and liability for fraud"); *see also,* AARP at 3 ("[C]onsumers are not well protected when novel payment methods are used, and legitimate businesses have access to a variety of other payment methods that do provide consumers with more robust protections, the benefit to consumers of the proposed rule outweighs the burden to businesses in complying with this rule."); DOJ-CPB at 1 (noting that the proposal would "[leave] open safer mechanisms for legitimate marketers to accept consumer payments.").
[292] AGO at 10 ("It is now appropriate, indeed critical, for the FTC to clarify those companies' responsibility for making reasonable inquiry into whether consumers who propose to wire money are doing so in response to a prohibited communication."); NCLC at 14 ("Money transmitters are in a position to police their system").
[293] AGO at 10; NCLC at 14-15; DOJ-CBP at 3; DOJ-Criminal at 3.
[294] NCLC at 14 ("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."); DOJ-

to money transfer businesses themselves, they do not always stop the fraudulent proceeds from passing through their hands."[295] To counter this problem, several commenters urged the Commission to "make clear the legal responsibility, and liability, of the entities that *control the method of payment.*"[296] At a minimum, commenters argued, money transfer companies should ask their customers about the purpose of the transfer, stop any transfers prohibited by the amended TSR, and take additional steps to identify and terminate money transfer agents that are complicit in violating the TSR and other laws.[297]

Some commenters suggested that the prohibition on cash-to-cash money transfers should go further to protect consumers. For example, NCLC argued that the Commission should alter the existing knowledge standard for assisting and facilitating violations of the Rule to impose strict liability on money transfer providers.[298] According to NCLC, "[m]oney transmitters are in a position to police their system, and they will do so if they have strict liability for violations."[299] In addition, several commenters encouraged the Commission to extend the prohibition beyond telemarketing transactions to protect consumers from fraud-induced transfers initiated via email

---

Criminal at 3 & n.10 (describing the proliferation of corrupt money transfer agents and citing criminal prosecutions); *see also infra* note 350 and accompanying text.

[295] DOJ-CPB at 3 (citing the *U.S. v. MoneyGram Int'l, Inc.*, Cr. No. 12-291 (M.D. Pa. Nov. 9, 2012).

[296] AGO at 10 (emphasis in original).

[297] *Id.*; *see also* AFR at 1 ("The FTC should strengthen the rules against assisting or facilitating the use of the banned payment methods"); DOJ-Criminal at 3 ("Over the past decade, criminals' techniques have shifted from bribery or physical intimidation or assault of money transfer agents to fraudulent applications by mass-marketing fraud ring members to become agents of legitimate money transfer companies") (citations omitted).

[298] NCLC at 13.

[299] *Id.*

or the internet.[300] According to these commenters, the use of cash-to-cash transfers in such transactions causes as much harm to consumers as transactions over the telephone."[301]

b. Cash Reload Mechanisms

Several commenters expressed general support for the prohibition against the use of cash reload mechanisms in telemarketing transactions for the same reasons they supported the prohibition on cash-to-cash money transfers.[302] Some provided more detailed responses, noting that cash reload mechanisms provide perpetrators of telemarketing fraud with the same speed, irrevocability, and convenience as cash-to-cash money transfers.[303] These commenters noted that the use of cash reload mechanisms in telemarketing fraud is increasing. DOJ-Criminal agreed that perpetrators are now using cash reload mechanisms in work-at-home, advance-fee loan, and sweepstakes scams.[304] According to NCLC, cash reload mechanisms were the second most common method of payment in telemarketing fraud reported to the National Consumers League Fraud Center in 2012, accounting for eight percent of all telemarketing payments,[305] compared to one percent in 2009.[306] In one criminal case, DOJ-Criminal noted that "a single defendant obtained tens of thousands of dollars from the [Green Dot] MoneyPak cards of 50 different victims in at least 14 states."[307]

---

[300] AFR at 1 ("The payment system ban should apply to sales initiated by email or other methods that do not use a telephone."); AGO at 9 ("The prohibition on telemarketing using money transfers should extend to commercial communications using money transfers."); NCLC at 13 ("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.").
[301] AGO at 1; NCLC at 2.
[302] *See generally* AARP; AGO; AFR; DOJ-Criminal; DOJ-CPB; Michalik; NCLC; Hon. Bill Nelson.
[303] AGO at 11; DOJ-CPB at 3; DOJ-Criminal at 4; NCLC at 11-12.
[304] DOJ-Criminal at 4; *see also* AGO at 11.
[305] NCLC at 12.
[306] *Id*.
[307] DOJ-Criminal at 4.

Like cash-to-cash money transfers, commenters argued, cash reload mechanisms are not used by legitimate businesses as a payment method for telemarketing transactions. Commenters stated that legitimate businesses instead use electronic payments or debit or credit cards and have no need to use a cash reload system.[308] These commenters noted that cash reload mechanisms enable perpetrators of fraud to evade consumer protections and liability for fraud.[309] Supporters of the prohibition acknowledged that the sale of cash reload mechanisms off the rack at retail stores differentiates this payment method from cash-to-cash money transfers that are facilitated by money transfer agents. This "self-service" nature of cash reload mechanisms makes it difficult for the reload provider to intercept and warn potential victims.[310] Nevertheless, commenters argued, a reload provider 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."[311]

2. Comments Opposing the Prohibition Against Cash-to-Cash Money Transfers and Cash Reload Mechanisms

a. Cash-to-Cash Money Transfers

The Commission received detailed comments opposing the prohibition of cash-to-cash money transfers in telemarketing transactions from The Money Services Roundtable ("TMSRT"), a group of several national non-bank money transmitters.[312] Other commenters

[308] AARP at 3; NCLC at 13.
[309] AGO at 4; DOJ-CPB at 3; DOJ-Criminal at 4; NCLC at 12.
[310] NCLC at 15 ("Cash reload systems operate somewhat differently from cash-to-cash money transfers").
[311] *Id.* ("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 the systemic problems.").
[312] TMSRT at 1. The group includes: RIA Financial Services, Sigue Corporation, Western Union Financial Services, Inc., MoneyGram Payment Systems, Inc., and Integrated Payment Systems, Inc.

indicated their general opposition to a prohibition on the use of any novel payment methods in telemarketing, including cash-to-cash money transfers.[313] At least one opponent of the amendment argued that deceptive or abusive telemarketers and sellers are the root of the problem, not the payment method itself.[314] Neither TMSRT nor any other commenter, however, identified a single legitimate telemarketer or seller that requested or accepted payment via money transfer. For example, telemarketing firm InfoCision claimed generally that novel payment methods are "extremely important" to legitimate businesses and charities, but focused its comment on remotely created checks and remotely created payment orders.[315]

According to TMSRT, the "vast majority of the millions of transactions completed by TMSRT members each week are not fraudulently induced."[316] TMSRT highlighted the numerous reasons why consumers use money transfers, including to pay their rent or receive money used to pay children's tuition at school or medical expenses, and to help victims in areas devastated by disasters.[317] Opponents expressed concern that the prohibition in telemarketing could disrupt such legitimate uses of cash-to-cash money transfers by those who depend on them, causing consumers to incur added costs and inconvenience. This is because consumers may "abandon" legitimate transactions in the face of additional scrutiny by providers of cash-to-cash money transfers designed to detect whether a transaction is the result of telemarketing.

TMSRT asserted that it would be challenging for money transfer providers to distinguish telemarketing-related money transfers from all other types of transfers. As a result, two comments warned, the prohibition could severely restrict consumer access to international and

[313] CUNA at 1; ETA at 1; InfoCision at 2.
[314] ETA at 1-2.
[315] InfoCision at 2; *see also supra* note 215.
[316] TMSRT at 1.
[317] *Id*. None of these money transfers involve telemarketing under the TSR.

domestic funds transfers for all consumers, many of whom are unbanked, underserved by mainstream financial services, or do not have credit or debit cards because they are of "limited financial means and seek to avoid the fees associated with traditional banking products."[318] TMSRT expressed concern that the restriction may force money transfer customers to use other payment methods, such as "sending cash in the mail, or worse, through unlicensed 'underground' money transfer providers."[319]

In addition, TMSRT questioned whether the prohibition would be effective against the types of fraud-induced money transfers discussed in the NPRM, and argued that it would not deter bad actors. Both the Electronic Transactions Association ("ETA") and TMSRT expressed concern about third party liability for money transfer providers who accept telemarketing-related money transfers.[320] Specifically, TMSRT noted that the amended Rule would require money transfer providers to "take steps to prevent potential telemarketers from receiving money transfers, even though the transmitters are unlikely to know or have reason to know if the individual recipient is a telemarketer (or a fraudster posing as a legitimate recipient)."[321] TMSRT expressed confusion as to whether money transfer providers "will be required to ask consumers several questions at the point of sale in order to ascertain whether they are sending money related to a telemarketing call."[322] TMSRT argued that such questions can be easily circumvented when perpetrators coach their victims on how to answer and noted that some consumers may find such questioning invasive or may not know that they are dealing with a telemarketer. If the Commission adopts the prohibition, TMSRT argued, it should provide a safe

[318] TMSRT at 4; *see also* ETA at 2.
[319] TMSRT at 5.
[320] ETA at 1 ("The ETA is concerned that a payment processor's innocent acceptance or processing of a 'novel' payment method in a non-fraudulent telemarketing sales transaction would be deemed an abusive act or practice.").
[321] TMSRT at 5.
[322] *Id.*

harbor for money transfer providers that act in good faith and utilize fraud protection programs that include: (a) designation of employees accountable for the fraud monitoring program; (b) transaction blocking for designated consumers; and (c) evaluation of transactional data to monitor and predict fraudulent activity.[323]

TMSRT further argued that the prohibition is unnecessary because money transfer providers already have "taken steps to substantially reduce the amount of fraudulent activity that is occurring."[324] Instead of a prohibition on the use of cash-to-cash money transfers in telemarketing, TMSRT suggested, the Commission should elicit information from other intermediaries that "unknowingly interact with abusive telemarketers," such as Internet service providers or telecommunications companies.[325] TMSRT further opined that the Commission should encourage information sharing among law enforcement and money transfer providers and conduct research into more effective disclosures for consumers to prevent fraud-induced transfers. According to TMSRT, the Commission should abandon the prohibition in favor of providing guidance on fraud prevention programs that money transfer providers should adopt.[326]

b. Cash Reload Mechanisms

The Commission received general comments from InfoCision and ETA regarding the importance of all novel payment methods in telemarketing, and specific comments on the prohibition of cash reload mechanisms in telemarketing from two providers, Green Dot and InComm.[327] InComm expressed the view that cash reload mechanisms are no more vulnerable to fraud than other payment methods, and noted that the rate of fraud for cash reloads is low in

[323] *Id.* at 6-7.
[324] *Id.* at 5.
[325] *Id.* at 5-6.
[326] *Id.* at 6.
[327] InfoCision at 2; ETA at 1.

comparison to the overall transaction volume and dollar amount.[328] In contrast, Green Dot agreed with the Commission's concerns about the misuse of cash reload mechanisms in telemarketing transactions.[329] Both commenters described cash reload mechanisms as a convenient, low-cost payment method for consumers to pay authorized billing partners, load funds to accounts with online payment intermediaries, and conduct person-to-person transactions.[330] Notably, neither commenter identified legitimate telemarketers or sellers covered by the TSR that use cash reload mechanisms.

After the close of the comment period, Green Dot submitted written testimony in a hearing held before the United States Senate Special Committee on Aging on July 16, 2014, in which the company announced the discontinuance of "the MoneyPak PIN method of reloading a card" in favor of a "card swipe" reload process.[331] The card swipe reload method requires the GPR cardholder to physically present the card in the store and swipe it at the retail point of sale terminal in order to reload funds. Green Dot's testimony confirmed that "without the MoneyPak PIN, the scammer will have no method of instructing a senior to buy a [MoneyPak] and no method of redeeming any associated PIN number."[332] In October 2014, InComm, which operates the Vanilla Reload Network cash reload mechanism, also announced its migration to the swipe reload process.[333] InComm stated the new process would "eliminate[] opportunities for fraud and scam artists to take advantage of unsuspecting customers through the use of reload

[328] InComm at 3.
[329] Green Dot at 1; *see* Written Statement of Green Dot, *supra* note 50.
[330] InComm at 3; Green Dot at 1.
[331] Written Statement of Green Dot, *supra* note 50, at 2.
[332] *Id.* At a subsequent hearing held by the U.S. Senate Special Committee on Aging, a third cash reload provider, Blackhawk Network, testified it will replace its "Quick Reload" process with swipe reload. Testimony of Blackhawk Network, *supra* note 51, at 3.
[333] InComm Press Release, *supra* note 51.

packs."[334] Similarly, Blackhawk Network – a cash reload provider that did not comment on the proposed Rule – indicated that it has eliminated the use of its cash reload mechanism ("Reloadit pack") to apply funds directly to any existing GPR card.[335]

Before announcing its voluntary discontinuance of MoneyPak, Green Dot's comment expressed support for a prohibition, but suggested the Commission narrow the definition of cash reload mechanism to exclude from coverage those types of payment mechanisms that facilitate bill payment and other money transmission activity "so long as the payment mechanism cannot be used to add funds to a GPR Card."[336] Similarly, before InComm started phasing out Vanilla Reload packs, InComm's comment opined that the broad definition of "telemarketing" would mean that unbanked consumers might not be able to use cash reload mechanisms to pay billers or e-commerce merchants, or make payments to a friend, family member, or other third party who happens to engage in telemarketing activities.[337] InComm argued that a prohibition will not deter fraudulent telemarketers from utilizing cash reload mechanisms to defraud consumers, so the costs of a prohibition would necessarily outweigh any benefits.[338]

InComm and Green Dot each expressed additional concern about the potential liability of a cash reload provider under the TSR's prohibition against assisting and facilitating violations of the Rule.[339] These commenters noted that no single party in the lifecycle of a prepaid card

---

[334] *Id.* As of March 31, 2015, Vanilla Reload PIN code cash reload is no longer available for purchase. *See* www.vanillareload.com (last visited June 6, 2015).
[335] Testimony of Blackhawk Network, *supra* note 51, at 3. Instead, consumers can use a swipe reload method to reload their own GPR card at a register, or sign up for a Reloadit Safe – an account that acts like a digital wallet into which consumers can deposit the funds on Reloadit packs. In turn, the consumer can use the funds from the Reloadit Safe to load GPR cards she has registered with her Reloadit Safe. *See* Reloadit How It Works, *available at* https://www.reloadit.com/HowItWorks (last visited June 6, 2015).
[336] Green Dot at 2.
[337] InComm at 2-3 (noting the proposal "could potentially prohibit consumers' legitimate uses of cash reload mechanisms that are unrelated or incidental to any telemarketing activity").
[338] InComm at 2.
[339] Green Dot at 2; InComm at 4.

transaction that uses a cash reload mechanism has "full visibility into the transaction from beginning to end," which makes it difficult for the reload provider to know whether the transaction is related to telemarketing.[340] In addition, one said, perpetrators of fraud frequently use stolen identities to open and access GPR cards onto which such funds are loaded, making it difficult for cash reload providers to preemptively shut off the redemption of the cash reload mechanism by telemarketers.[341] To address these concerns, both commenters requested that the Commission explicitly exempt cash reload providers from the Rule's prohibition against providing substantial assistance or support to any seller or telemarketer while knowing or consciously avoiding knowledge that the seller or telemarketer is engaged in violations of certain provisions of the TSR.[342]

3. The Commission Concludes that the Use of Cash-to-Cash Money Transfers and Cash Reload Mechanisms in Telemarketing Meets the Test for Unfairness

This amendment proceeding is limited in scope to the direct regulation of those telemarketers and sellers covered by the TSR and subject to the jurisdiction of the FTC. Accordingly, the amendment is limited to the use of cash-to-cash money transfers and cash reload mechanisms by telemarketers and sellers covered by the TSR. The Commission, therefore, cannot extend the prohibition to Internet based transactions, as suggested by some advocates.[343] In addition, the Commission declines to revise the Rule's provision against

[340] Green Dot at 2; *see also* InComm at 4.
[341] InComm at 4.
[342] InComm at 4; *see also* Green Dot at 2.
[343] AGO at 1 (recommending that "the prohibition extend to transactions proposed by email, which transactions cause as much harm to consumers, if not more, than transactions over the phone"). The AGO comment cites to Consumer Sentinel Network data provided by the FTC to conclude that fraud-induced money transfers in connection with email communication is a problem of "equivalent or greater magnitude" than telemarketing. AGO at 7. The AGO letter notes that, from January 1, 2011 through June 3, 2013, the Commission received 26,379 complaints

assisting and facilitating to create strict liability for the providers of cash-to-cash money transfers and cash reload mechanisms, as suggested by supporters of a prohibition. Likewise, the Commission finds it unnecessary and inappropriate either to explicitly exempt or otherwise provide a safe harbor for money transfer or cash reload providers, as suggested by industry representatives. As described in more detail in Section II.A.3, the Commission continues to believe that the "conscious avoidance" standard is appropriate when seeking to hold third parties accountable for the actions of others under the TSR.

After careful consideration of the entire rulemaking record, the Commission concludes that the use of cash-to-cash money transfers and cash reload mechanisms in telemarketing transactions meets the unfairness test for an abusive telemarketing practice.

a. The Use of Cash-to-Cash Money Transfers and Cash Reload Mechanisms in Telemarketing Causes Substantial Harm to Consumers

The substantial consumer harm resulting from cash-to-cash money transfers and cash reload mechanisms in telemarketing is ongoing and persistent. The rulemaking record confirms that perpetrators of telemarketing fraud – not legitimate telemarketers and sellers – depend on the speed, convenience, anonymity, and irrevocability of these payment methods to siphon millions

---

(accounting for $188,963,368 of injury) in which consumers identified the payment method as "wire transfer" and the method of communication as "telephone." *Id.* During the same time frame, the Commission received 67,217 complaints (accounting for $596,315,020 in injury) for money transfer complaints where the method of contact was "email." *Id.*

The Commission notes that the data cited by the AGO comment include only those complaints in which the consumer reported both the method of payment and the method of initial contact. As a result, these figures exclude a significant number of complaints in which consumers did not report either the method of payment or the method of contact. For example, from January 1, 2011 through June 3, 2013, only 26 percent (or 305,990) of all consumer complaints (1,165,090) reported the method of payment, while 48 percent of consumer complaints (560,811) included the method of contact. FTC, *Consumer Sentinel Network Data Book for January - December 2013*, at 8-9 (Feb. 2014), *available at* https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf. Moreover, the overall Consumer Sentinel data in 2013 demonstrated that consumer fraud victims reported the telephone as the method of contact in 40 percent of complaints, while email was the method of contact in 33 percent of complaints. *Id.* at 9.

from consumer victims each year. Furthermore, the record is conspicuously devoid of evidence of the use of such payment mechanisms by legitimate telemarketers or sellers covered by the TSR.[344]

The law enforcement experience of the Commission and the Department of Justice evidences the high risk to consumers and widespread injury caused by fraud-induced money transfers and cash reload mechanisms in telemarketing. As these enforcement cases and alerts show, perpetrators of fraud have employed a variety of means to dupe or pressure consumers into sending cash-to-cash money transfers, including fake foreign lottery or sweepstakes prizes,[345] phony mystery shopper scams,[346] and work-at-home opportunities.[347] Increasingly, law

[344] InComm expressed concern that the proposed amendment would restrict the ability of consumers to use cash reload mechanisms for non-telemarketing transactions, including e-commerce transactions and payments to billers (such as utility, cable, or telephone providers). InComm at 2-3. As discussed in detail in section II.B.3.c(2) below, the Commission is unpersuaded that these transactions will be adversely affected by the prohibition on cash reload mechanisms in telemarketing.

[345] *See, e.g.*, *FTC v. Bezeredi*, Civ. No 05-1739 (W.D. Wash. Apr. 3, 2007) (Summ. J.); *FTC v. 627867 B.C. Ltd. dba Cash Corner*, Civ. No 03-3166 (W.D. Wash. Aug. 4, 2006) (Stip. Perm. Inj.); *FTC v. World Media Brokers, Inc.*, No. 02C6985 (N.D. Ill. June 22, 2004), *aff'd*, 415 F.3d 758 (7th Cir. 2005) (Partial Summ. J.); *see also* Press Release, DOJ, *Jamaican Man First to be Extradited to Face Fraud Charges in International Lottery Scheme* (Feb. 12, 2015) (indictment describing how defendant and co-conspirators obtained victims' money via MoneyGram, Western Union, and Jamaica National money transfers), *available at* http://www.justice.gov/opa/pr/jamaican-man-first-be-extradited-face-fraud-charges-international-lottery-scheme; Press Release, FBI, *Jamaican DJ Arrested in Florida in Connection with North Dakota Telemarketing Lottery Scam: Twenty-Six Individuals Currently Indicted* (May 27, 2014), *available at* http://www.fbi.gov/minneapolis/press-releases/2014/jamaican-dj-arrested-in-florida-in-connection-with-north-dakota-telemarketing-lottery-scam; Press Release, FBI, *Telemarketer Sentenced in Manhattan Federal Court to 75 Months in Prison for Sweepstakes Fraud That Targeted Elderly Victims* (Sept. 24, 2013), *available at* http://www fbi.gov/newyork/press-releases/2013/telemarketer-sentenced-in-manhattan-federal-court-to-75-months-in-prison-for-sweepstakes-fraud-that-targeted-elderly-victims.

[346] *See, e.g.*, *U.S. v. Brister*, Cr. No. 13-0276 (E.D. Pa. June 6, 2013) (indictment describing various mystery shopper and job schemes used by defendant to induce victims to transfer money via Western Union), *available at* http://www.justice.gov/usao/pae/News/2013/June/brister_indictment.pdf; FTC Consumer Alert, *Mystery Shopper Scams* (Nov. 2012), *available at* http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt151.shtm; Press Release, DOJ, *Georgia Woman Pleads Guilty In Mystery Shopper Scam* (July 23, 2014), *available at* http://www.justice.gov/usao/paw/news/2014/2014_july/2014_07_23_03 html; Press Release, DOJ, *Santa Barbara County Man Sentenced to Six Years in Federal Prison for Running $6 Million Job Scam* (Apr. 5, 2011), *available at* http://www.justice.gov/usao/cac/Pressroom/pr2011/048 html (defendant sentenced for $6 million bogus mystery shopper scam).

[347] *FTC v. USS Elder Enters., Inc.*, Civ. No. 04-1039 (C.D. Cal. Jul. 26, 2005) (default judgment against telemarketers using bogus work-at-home opportunity to lure consumers to send at least $885,196 in money transfers).

enforcement is finding these same tactics are being used to convince consumers to send money via cash reload mechanisms.[348]

In some widespread telemarketing frauds, the agents of cash-to-cash money transfer providers have been complicit in the schemes used to defraud consumers. The U.S. Department of Justice has obtained numerous criminal convictions of corrupt and collusive MoneyGram and Western Union agents that carried out, participated in, or laundered the proceeds from telemarketing fraud.[349] For example, the U.S. Attorney's Office for the Middle District of Pennsylvania, alone, has brought conspiracy, fraud and money laundering charges against 28 former MoneyGram agents.[350]

Law enforcement cases demonstrate that some money transfer providers "have a strong financial incentive to continue facilitating such transactions despite unmistakable signs of fraud."[351] For nearly a decade, federal and state agencies have brought civil and criminal law enforcement actions against cash-to-cash money transfer providers to stop them from profiting from the use of their systems by fraudulent telemarketing schemes and other frauds. In 2005, Western Union entered into an agreement with 47 states and the District of Columbia to resolve allegations about the use of the company's wire transfer services by fraudulent telemarketers.[352]

---

[348] AARP Bulletin, *Scam Alert: Beware of Green Dot MoneyPak Scams - The crooks' other preferred payment method has become the weapon of choice* (Apr. 23, 2012), *available at* http://www.aarp.org/money/scams-fraud/info-04-2012/avoid-moneypak-scams.html; Press Release, Better Business Bureau, *Fraud Task Force Warns Consumers Of Scams Using Western Union, MoneyGram, Green Dot MoneyPaks* (Aug. 2, 2012), *available at* http://www.bbb.org/us/article/fraud-task-force-warns-consumers-of-scams-using-western-union-moneygram-green-dot-moneypaks-36126.

[349] DOJ-Criminal at 3 & n.10 (citing examples of cases involving corrupt money transfer agents); NCLC at 14 & nn.56-59 (same).

[350] Press Release, DOJ, *MoneyGram International Inc. Admits Anti-Money Laundering and Wire Fraud Violations, Forfeits $100 Million in Deferred Prosecution* (Nov. 9, 2012), *available at* http://www.justice.gov/opa/pr/2012/November/12-crm-1336 html.

[351] *Id.*; DOJ-CPB at 3.

[352] *See* Press Release, Office of the Vermont Attorney General, *Western Union Enters Into Settlement With Attorneys General* (Nov. 14, 2005), *available at* http://www.atg.state.vt.us/news/western-union-enters-into-settlement-with-attorneys-general.php. A copy of the five-year, multi-state agreement is available on the website of

Under the settlement, Western Union agreed to fund an $8.1 million national consumer awareness program, place prominent consumer warnings on the send forms used by customers, terminate agents who are involved in fraud, develop a computerized system aimed at identifying transfers that are at risk of fraud and blocking fraud-induced transfers before they are completed, and increase the company's anti-fraud staffing.

In 2008, MoneyGram entered into a similar agreement with 44 states and the District of Columbia to address the high number of money transfers sent by consumers to fraudulent telemarketers.[353] The agreement required the company to fund a $1.1 million national consumer awareness program, use prominent consumer warnings on the forms used by consumers to wire money, revise and enhance the company's agent anti-fraud training programs, and provide special training to agents with elevated fraud levels at their locations.

In October 2009, the Commission reached a separate $18 million settlement with MoneyGram to settle charges that it allowed telemarketers to bilk U.S. consumers out of tens of millions of dollars using its money transfer system.[354] According to the complaint, MoneyGram knew that its system was being used to defraud people but did very little about it. For example, the FTC alleged that MoneyGram knew, or consciously avoided knowing, that 131 of its more than 1,200 agents accounted for more than 95 percent of the fraud complaints MoneyGram received in 2008 regarding money transfers to Canada. The Commission further alleged that MoneyGram ignored warnings from law enforcement officials and its own employees that

---

the Office of the Iowa Attorney General at http://www.state.ia.us/government/ag/latest_news/releases/nov_2005/Western_Union.html.

[353] *See* Press Release, Office of the Vermont Attorney General, *Attorney General Announces $1.2 Million Settlement With MoneyGram* (July 2, 2008), *available at* http://www.atg.state.vt.us/news/attorney-general-announces-1.2-million-settlement-with-moneygram.php. A copy of the five-year, multi-state agreement can be found on the website of the Texas Attorney General at http://www.oag.state.tx.us/newspubs/releases/2008/070208moneygram_avc.pdf.

[354] *FTC v. MoneyGram Int'l, Inc.*, Civ. No. 1:09-06576 (N.D. Ill. Oct. 19, 2009) (Stip. Perm. Inj.).

widespread fraud was being conducted over its network, and even discouraged its employees from enforcing the company's own fraud prevention policies or taking action against suspicious or corrupt agents.[355] As a result of the settlement, MoneyGram is permanently enjoined from failing to: (1) provide consumer fraud warnings, which must be reviewed and updated to ensure the company's effectiveness in preventing fraud, (2) enable a consumer to reverse a money transfer if the funds have not been picked up and the consumer alleges the transfer was induced by fraud; (3) establish, implement, and maintain a comprehensive anti-fraud program reasonably designed to detect and prevent fraud-induced money transfers as well as money transfer agents who may be complicit in fraud.[356] The Commission sent more than 34,000 checks totaling almost $18 million to consumers identified as victims of a series of cross-border fraud schemes.[357]

In 2012, the U.S. Attorney for the Middle District of Pennsylvania filed a criminal case against MoneyGram, alleging that the company willfully disregarded obvious signs that its money transfer network was being used by fraudulent telemarketers and other con-artists, including its own money transfer agents.[358] According to the Statement of Facts, "MoneyGram's processing of fraudulent transactions [through complicit MoneyGram agents] was critical to the success of the fraud scheme because the Perpetrators relied on MoneyGram's money transfer system to receive the victim's money."[359] To resolve the case, MoneyGram entered into a five-year deferred prosecution agreement in which it admitted to "criminally

---

[355] *See* Press Release, FTC, *MoneyGram to Pay $18 Million to Settle FTC Charges That it Allowed its Money Transfer System To Be Used for Fraud* (Oct. 20, 2009), *available at* http://www ftc.gov/news-events/press-releases/2009/10/moneygram-pay-18-million-settle-ftc-charges-it-allowed-its-money.
[356] Stip. Order for Perm. Inj. and Final Judgment, *filed in FTC v. MoneyGram*, *supra* note 354.
[357] *See* Press Release, FTC, *FTC Mails Redress Checks to Fraud Victims Who Lost Money Through MoneyGram's Money Transfer System* (Apr. 28, 2010), *available at* http://www ftc.gov/news-events/press-releases/2010/04/ftc-mails-redress-checks-fraud-victims-who-lost-money-through.
[358] *U.S. v. MoneyGram Int'l, Inc.*, Cr. No. 1:12-291 (M.D. Pa. Nov. 9, 2012).
[359] Statement of Facts, ¶ 18, filed in *US v. MoneyGram*, Cr. No. 1:12-291 (M.D. Pa. Nov. 9, 2012).

aiding and abetting wire fraud and failing to maintain an effective anti-money laundering program."[360] The agreement required MoneyGram to provide $100 million to the victims of fraud-induced transfers, undertake enhanced compliance monitoring procedures, and employ a corporate compliance monitor.[361]

Increasingly, law enforcement and consumer advocates have encountered the use of cash reload mechanisms in telemarketing schemes that defraud consumers in a variety of ways.[362] The testimony and voluntary actions of three cash reload providers also support the conclusion that perpetrators of fraud are increasingly turning to cash reload mechanisms.[363] As with cash-to-cash money transfers, these schemes include advance fees on bogus loans,[364] "processing" fees for government grants,[365] taxes on purported lottery or sweepstakes winnings,[366] and claims of money owed to the IRS.[367]

---

[360] *See* Press Release, DOJ, *supra* note 350 (alleging, among other things, that MoneyGram failed to implement policies or procedures governing the termination of agents involved in fraud and/or money laundering; (2) failed to implement policies regarding the filing of the required Suspicious Activity Reports (SARs) when victims reported fraud to MoneyGram on transactions over $2,000; (3) failed to file SARs on agents MoneyGram knew were involved in the fraud; and (4) failed to conduct effective AML audits of or due diligence on its agents, prospective agents, and outlets).

[361] *Id.* According to the Statement of Facts, MoneyGram has implemented a number of remedial actions, including the creation of an Anti-Fraud Alert System to identify and place on hold potentially fraudulent transactions. Statement of Facts, *supra* note 359, at ¶ 32f.

[362] S*ee supra* note 348; DOJ-Criminal at 4; NCLC at 11-12; AFR at 1; *see also* Jorgen Wouters, Daily Finance, Beware of Green Dot MoneyPak Scams (June 23, 2011), *available at* http://www.dailyfinance.com/2011/06/23/beware-of-green-dot-moneypak-scams/ (article including statements of president and CEO of the BBB regarding the increase of frauds using cash reload mechanisms).

[363] *See, e.g.*, Written Statement of Green Dot, *supra* note 50, at 2; Testimony of Blackhawk Network, *supra* note 51, at 3; InComm Press Release, *supra* note 51.

[364] Consumer Alert, Bill Schuette Attorney General, *Green Dot MoneyPak Cards*, *available at* http://www.michigan.gov/ag/0,4534,7-164-17337_20942-318482--,00 html.

[365] Consumer Alert, Federal Reserve, $ Consumer Help (Dec. 11, 2013), *available at* https://www.federalreserveconsumerhelp.gov/.

[366] Sue McConnell, *BBB Consumer News and Opinion Blog: Cleveland Woman Loses Hundreds of Dollars to Government Grant Scam* (Feb. 28, 2014), *available at* http://www.bbb.org/blog/2014/02/cleveland-woman-loses-hundreds-of-dollars-to-government-grant-scam/.

[367] Press Release, FBI, *Internal Revenue Service Telephone Scam* (Sept. 29, 2014), *available at* https://www.fbi.gov/sandiego/press-releases/2014/internal-revenue-service-telephone-scam; Press Release, FBI, *U.S. Attorney's Office Warns Public of Lottery Scam Telephone Calls* (May 28, 2013), *available at* https://www.fbi.gov/minneapolis/press-releases/2013/us-attorneys-office-warns-public-of-lottery-scam-telephone-calls.

Existing consumer complaint data, including the complaints collected by the Commission's Consumer Sentinel Network ("CSN"), also indicates the significant injury resulting from fraud-induced money transfers and cash reload mechanisms. The CSN data includes unverified complaints and does not represent a statistical consumer survey. However, it provides important information on the number of consumer complaints reported and the amount of injury reported. The CSN data is consistent with the significant injury documented in law enforcement cases involving fraud-induced money transfers and cash reload mechanisms.[368] Both MoneyGram and Western Union are data contributors to the CSN. These companies voluntarily contribute to the CSN a significant numbers of consumer complaints they receive from customers, which necessarily affects the distribution of the reported methods of payment.[369] For example, in 2014 consumer complaints contributed to the CSN by MoneyGram and Western Union represented 3 percent of the total number of complaints received.[370]

Between January 1, 2012, and December 31, 2014, the CSN database logged 322,850 consumer fraud complaints[371] in which the victims reported the method of payment as "Wire Transfer" – a category that includes cash-to-cash money transfers. These fraud complaints accounted for more than $1.4 billion in total reported consumer injury.[372] In 2014 alone, the CSN received 106,472 consumer fraud complaints in which the method of payment was Wire Transfer, accounting for $500,705,082 in reported consumer injury.[373] Statistics from the

[368] *See supra* notes 345-350 and accompanying text (describing law enforcement cases involving money transfers).
[369] FTC, *Consumer Sentinel Network Data Book for January - December 2014*, at 8 & n.2 (Feb. 2015) (hereinafter "2014 Consumer Sentinel Network Data Book"), *available at* https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf.
[370] *Id.* at 74.
[371] *Id.* at 8-9. These figures include telemarketing and non-telemarketing complaints.
[372] The 2014 Consumer Sentinel Network Data Book documented a total of $1,468,647,723 in injury from January 1, 2011 through December 31, 2014. *Id.* at 8 & n.2.
[373] *Id.* at 8-9. These figures include telemarketing and non-telemarketing complaints.

National Consumers League's ("NCL") Fraud Center confirm the widespread use of cash-to-cash money transfers in telemarketing fraud. According to NCL's 2012 complaint data, cash-to-cash money transfers accounted for "nearly 63 percent of all telemarketing [fraud] payments."[374]

The CSN consumer complaint data also is beginning to show the significant injury inflicted when perpetrators of fraud use cash reload mechanisms to siphon money from consumer victims. In 2014, CSN logged 119,100 consumer fraud complaints accounting for $80,860,327 in reported injury in which the victims reported the method of payment as "Prepaid Card" – a category that captures cash reload mechanisms.[375] Green Dot voluntarily contributed a significant number (4 percent) of consumer complaints received by the CSN in 2014, which affects the distribution of the reported methods of payment.[376] According to Green Dot estimates, consumer complaints of fraud-induced cash reloads "represented approximately $30 million in cash loads in 2013 out of total load volume of approximately $20 [b]illion, or approximately one-quarter of one percent of loads."[377] NCL stated that its 2012 complaint data also indicate that a growing percentage of telemarketing fraud complaints involve payments made via cash reload mechanisms.[378]

Notwithstanding the investigations, lawsuits, consumer alerts, monetary settlements, and injunctions requiring implementation and strengthening of anti-fraud measures, the use of cash-to-cash money transfers and cash reload mechanisms by telemarketers continues to cause substantial injury to consumers. As the rulemaking record makes clear, the substantial harm and

[374] NCLC at 12.
[375] 2014 Consumer Sentinel Network Data Book, *supra* note 369, at 8.
[376] *Id.* at 8 n.2 & 74.
[377] Written Statement of Green Dot Corporation, *supra* note 50, at 2.
[378] NCLC at 12.

losses sustained by consumers usually cannot be undone.[379] Once a cash-to-cash money transfer is picked up, or funds are offloaded from a cash reload mechanism to a GPR card, the money is irretrievable. There are no federal or state statutory or contractual chargeback rights for consumers who make such payments.[380] Existing federal and state laws pertaining to cash-to-cash money transfers and cash reload mechanisms are not aimed at consumer protection and do not address the abuse of these payment methods by fraudulent telemarketers and con artists.[381] The absence of consumer protections providing consumers with the means to recover their money once they or their family members discover the fraud compounds the substantial injury sustained by consumers.

---

[379] *See NPRM*, *supra* note 1, at 41213 (describing injury estimates from consumer complaint data and cases).

[380] If the CFPB's proposed Prepaid Account Rule is adopted, the protections of the EFTA and Regulation E would extend to registered cash reload mechanisms. *See supra* note 279. The Commission is aware of no state law providing chargeback rights for consumers using cash-to-cash money transfers or cash reload mechanisms. State laws governing money services businesses ("MSBs"), including the Texas statute highlighted in the comment submitted by InComm, typically mandate disclosures to consumers. InComm at 5 & n.2 (referencing a Texas statute, 7 TX ADC 33.51, which requires MSBs to provide consumers with customer service contact information, and information on how to file a complaint with the Texas Department of Banking if a complaint remains unresolved).

[381] The BSA and related laws target terrorism financing, tax evasion, and money laundering activity. U.S. Department of Treasury, FinCEN, *Statutes & Regulations: Bank Secrecy Act*, *available at* http://www.fincen.gov/statutes_regs/bsa/. The Prepaid Access Rule amends the money services businesses rules of the BSA regulations to mandate similar reporting and transactional information collection requirements on providers and sellers of certain types of prepaid access, including some cash reload mechanisms that meet certain criteria. *Final Rule; Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access*, 76 FR 45403-02 (Jul. 29, 2011). In addition, state statutes provide licensing requirements for money transfer providers. *See, e.g.*, ARIZ. REV. STAT. 6-1202 (licensing requirements for money transfer providers); KAN. STAT. ANN. 9-509 (same).

Certain cash-to-cash money transfers (those made to locations outside of the U.S.) are governed by the Remittance Rule, which provides disclosures to customers of money transfer providers. 12 CFR part 1005.30(e) (definition of "remittance transfer" includes transfers "sent by a remittance transfer provider" to a "designated recipient" outside of the United States). In contrast, cash reload mechanisms, which consumers purchase directly from a retailer at the point of sale, may not qualify as remittance transfers covered by the Remittance Rule, depending on whether cash reloads are transferring funds outside of the United States and whether the transfer is "sent by a remittance transfer provider." Whether the Remittance Rule applies to a particular cash-to-cash money transfer or cash reload mechanism, however, is immaterial to the Commission's analysis of the Final Rule. As discussed in section I.B.1.b above, existing laws regulate the relationship between the consumer and the money transfer provider, not the relationship between the consumer and the telemarketer or seller. *See also, supra* note 279 (discussing the CFPB's Proposed Prepaid Account Rule).

b. The Injury Is Not Reasonably Avoidable by Consumers

As described in the context of remotely created checks and remotely created payment orders, the Commission considers the extent to which a consumer can reasonably avoid injury, in part, by whether the consumer can make an informed choice. The Commission seeks "to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking." [382] Unscrupulous telemarketers are adept at interfering with a consumer's decisionmaking by spawning lies about the products and services offered, as well as by steering consumers into making payments that are irretrievable.

As is true in other telemarketing contexts, the ability of consumers to identify and avoid the risk of injury is substantially diminished when telemarketers engage in deceit to sell sham goods or services. Consumers often rely upon the representations made in telemarketing calls and comply with the payment instructions dictated by the telemarketer or seller. When deceitful telemarketers persuade consumers to deliver payment via cash-to-cash money transfers or cash reload mechanisms, the telemarketer causes additional harm that consumers cannot reasonably avoid. Consumers cannot avoid risks they do not perceive, and consumers generally do not appreciate that these payment mechanisms pose enhanced obstacles to detection of fraudulent conduct, to identification of the perpetrator, and to recovery of financial losses.

The lack of systematic monitoring of these payment mechanisms makes detection and deterrence of fraud challenging. In particular, as noted previously, these payments are difficult to track, and by the time consumers realize the operation was a scam, they cannot mitigate their losses by seeking a refund or a reversal of the transaction.[383] In fact, consumers typically

[382] *See supra* note 202 (citing cases deciding whether consumers' injuries were reasonably avoidable).
[383] *See Neovi*, *supra* note 202, at 1158 ("Regardless of whether a bank eventually restored consumers' money, the consumer suffered unavoidable injuries that could not be fully mitigated.").

discover all too late that legal protections to help recover money lost in a fraudulent transaction are absent once a cash-to-cash money transfer is picked up or a cash reload mechanism is offloaded.

Some opponents of a prohibition seem to suggest that consumers who have been deceived can and should reasonably avoid the harm – the initiation of a cash-to-cash money transfer or the turnover of a cash reload mechanism – by heeding the warnings not to transfer money or provide cash reloads to strangers.[384] These warnings are posted by money transfer providers in storefronts and on send forms, among other places, or are provided on the back of cash reload mechanisms.

Consumers, however, are under no duty to ferret out the truthfulness of marketing claims.[385] In telemarketing fraud perpetrated through cash-to-cash money transfers and cash reload mechanisms, a consumer often is thoroughly convinced and compelled – through false promises or fear of imminent threat of financial or legal consequences – to consummate payment by taking a number of burdensome steps. The consumer leaves his home in a determined effort to make immediate payment in the amount and manner dictated by the telemarketer or seller. Once a consumer is so deceived, generalized warnings against fraud (at the money transfer location or on the back of a cash reload mechanism) do not render avoidable the harm inflicted after the cash-to-cash transfer is picked up or the cash reload mechanism is offloaded by the telemarketer.

---

[384] TMSRT at 2 n.5 (noting that "consumers engage in cash-to-cash transfers with telemarketers despite explicit warnings not to do so.").

[385] As Judge Easterbrook stated in *Mayer v. Spanel Intern. Ltd.*, 51 F.3d 670, 675 (7th Cir. Mar. 31, 1995), "[t]olerating fraud by excusing deceit when the victim is too easily gulled increases . . . the volume of fraud"). *See also, FTC v. Crescent Pub. Group, Inc.*, 129 F.Supp.2d 311, 321 (S.D.N.Y. Jan. 24, 2001) (describing consumer reliance on express claims to be "presumptively reasonable," and noting that "[i]n evaluating [the] tendency . . . to deceive, it is appropriate to look not at the most sophisticated, but the least sophisticated consumer.") (citations omitted).

Green Dot recognized this dynamic in recent testimony to the U.S. Senate Special Committee on Aging, "it would appear that this tactic [consumer warnings on MoneyPak packaging] has not achieved the intended goal because the seniors ignore the warnings, convinced that the con artist is genuine."[386] Thus, it is clear that for some consumers, once they are persuaded to initiate a cash-to-cash money transfer or provide the cash reload mechanism to the perpetrator, it is impossible to cure the initial deception with subsequent general warnings about the potential danger of sending money to strangers.[387]

Opponents further argue that a prohibition against cash-to-cash money transfers and cash reload mechanisms is unwarranted because it is the unscrupulous actions of telemarketers and sellers – not the payment methods – that cause the unavoidable harm to consumers.[388] The Commission agrees that the immediate source of the problem is the fraudulent conduct of the telemarketer or seller, but the payment mechanism makes the economic injury more significant as the money is largely irretrievable once it's been sent. Consumers are unlikely to appreciate that the regulatory framework includes a paucity of consumer protections or that the systems moving their money cannot track the specific recipient of their payment.

Furthermore, this argument by opponents ignores the fact that the record is replete with evidence of corrupt money transfer agents who have colluded with the perpetrators of

---

[386] Written Statement of Green Dot, *supra* note 50, at 2; *see generally*, Testimony of Blackhawk Network, *supra* note 51.

[387] AARP at 2 ("AARP studies have confirmed that education alone will not protect older people from telemarketing fraud. . . . "there is always a hard core of victims whose behavior cannot be changed by messages"); *see also* Letter from the FTC to Hon. John D. Dingell, Chairman Committee on Energy and Commerce, United States House of Representatives, Commission Policy Statement on Deception, appended to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984) ("When representations or sales practices are targeted to a specific audience, such as children, the elderly, or the terminally ill, the Commission determines the effect of the practice on a reasonable member of that group.").

[388] ETA at 1 ("The ETA submits that it is not the payment methods themselves that are fraudulent, but rather the actors that are attempting to sell goods and services in a fraudulent manner that constitute the real problem."); TMSRT at 2 ("[T]he NPRM suggests that these payment methods themselves, rather than an abusive telemarketing practice are the problem.").

telemarketing frauds, while money transfer companies did little to stop it.[389] It also ignores the inextricable link in telemarketing transactions between these payment methods and fraudulent schemes, as there is no record evidence that legitimate telemarketers or sellers use cash-to-cash money transfers or cash reload mechanisms. For these reasons, the Commission has determined that a prohibition on the use of cash-to-cash money transfers and cash reload payment mechanisms by telemarketers and sellers is necessary to prevent substantial and unavoidable consumer harm.

c. The Benefits of Cash-to-Cash Money Transfers and Cash Reload Mechanisms in Telemarketing Do Not Outweigh the Harm to Consumers

The use of cash-to-cash money transfers and cash reload mechanisms by telemarketers and sellers produces clear adverse consequences for consumers that are not accompanied by an increase in services or benefits to consumers or to competition.

(1) Cash-to-Cash Money Transfers

The rulemaking record confirms that the substantial and unavoidable harm to consumers resulting from the use of cash-to-cash money transfers in telemarketing transactions is not outweighed by any countervailing benefits to consumers or competition. No commenter cited a single legitimate telemarketer or seller that uses cash-to-cash money transfers in telemarketing. Instead, representatives of the money transfer industry described the benefits that cash-to-cash money transfers provide to consumers in non-telemarketing transactions, such as personal remittances to family and friends. As the law enforcement cases and consumer complaint data demonstrate, fraudulent telemarketers and sellers prefer anonymous, unrecoverable money

[389] DOJ-Criminal at 3 & nn.9-13 (citing numerous cases brought by the Department of Justice); *see supra* note 350.

transfers to conventional payment alternatives that are subject to federal consumer protections and that ensure systemic monitoring and dispute rights.

The Commission recognizes that consumers who wish to transfer money to friends, send money to family to pay tuition and medical bills, or remit money abroad to family may benefit from the convenience, speed, and cost that cash-to-cash money transfers can provide. These benefits, however, do not extend to the telemarketing context. Unlike ACH debits and card-based payment methods – including GPR cards that are used widely by unbanked and underbanked consumers[390] – that permit a telemarketer to instantly complete the sale over the telephone, cash-to-cash money transfers require the consumer to take several burdensome steps to initiate payment after the telephone call ends. The consumer typically must go to a money transfer provider's location, fill out a send form, pay a fee, and provide the currency to be transferred. In addition, the recipient, which cannot even ensure the consumer will comply with its directions, incurs time and costs resulting from the delay in payment by having to go to a money transfer location to receive the funds in cash. As a result, legitimate telemarketers simply do not rely on burdensome, unpredictable and costly cash-to-cash money transfers to receive payment for goods or services purchased over the telephone. Not surprisingly then, the record is devoid of evidence that any legitimate telemarketers or sellers currently use (or have ever used) cash-to-cash money transfers in telemarketing transactions.

The Commission is of the firm view that a prohibition on the use of these payment methods by telemarketers and sellers will provide bright line guidance benefitting both consumers and the telemarketing industry. While the warnings that money transfer providers provide are useful, there are substantial benefits to bright line guidance. First, the message is

[390] *See supra* notes 227-233 and accompanying text (describing studies of consumer payment preferences and the rapid growth of prepaid cards).

clear and it is concise: it is illegal for telemarketers ask consumers to wire cash. Second, it is delivered by the government, a neutral and authoritative source. Third, it is a message about the requirements of the law rather than advice on when to be cautious in these types of transactions.

Pragmatically, consumers educated about the prohibition who later encounter a telemarketer asking for a cash-to-cash money transfer will be able to more quickly identify the illegal behavior and simply hang up. Money transfer providers will have the benefit of being able to deliver a clear and concise message to all consumers, and importantly, a message that does not implicate cash transfers to relatives or friends. Legitimate telemarketers and sellers should also benefit from increased consumer confidence.

Citing to the benefits that cash-to-cash money transfers provide to consumers in non-telemarketing transactions, such as personal remittances to family and friends,[391] TMSRT asserts that the prohibition threatens to deprive consumers of these benefits because money transfer providers cannot distinguish such personal remittances from cash-to-cash money transfers "to individuals who may be telemarketers."[392] Therefore, TMSRT argues, the prohibition on cash-to-cash money transfers in telemarketing will have the unintended consequence of severely restricting all cash-to-cash money transfers.[393]

The Commission does not find TMSRT's argument persuasive. First, the prohibition affects a discrete sub-set of all money transfers: cash-to-cash transfers. The prohibition does not restrict or prohibit the use, in telemarketing or non-telemarketing transactions, of other types of money transfers that originate from or are received into bank accounts, payment cards (including GPR cards), or accounts with payment intermediaries, for example. Second, money transfer

[391] TMSRT at 1.
[392] *Id.* at 3.
[393] *Id.* At the same time, TMSRT maintains that money transfer providers "have taken steps to substantially reduce the amount of fraudulent activity that is occurring." *Id.* at 5.

providers already are trained in how to detect consumer fraud[394] and other types of illegal activity. Indeed, they are required to file with FinCEN suspicious activity reports ("SARs") identifying certain transactions in which the provider knows, suspects, or has reason to suspect its system is being used to facilitate criminal activity.[395] Finally, two of the largest money transfer providers, MoneyGram and Western Union, have taken voluntary and court-mandated measures to improve their BSA and AML compliance, including their ability to identify and stop fraud-induced transactions and those agents who are complicit in fraud.[396]

For cash-to-cash money transfer providers that have and enforce policies and procedures designed to screen out fraud-induced transfers, any additional burden should be minimal. TMSRT indicates that its members already have implemented fraud prevention programs, and it does not quantify the costs of any programmatic changes the Rule would require.[397] Indeed, a prohibition on the use of cash-to-cash money transfers in telemarketing transactions should enhance the effectiveness of the efforts taken by responsible money transfer providers to deter

---

[394] For example, in testimony to the U.S. Senate Special Committee on Aging, an official from Western Union explained how the company trains money transfer agents to help identify potential fraud victims, including "how to listen to consumers for verbal cues indicating fraudulent activity, look for body language that indicates nervousness or a sense of urgency, and ask questions to determine the consumer's relationship with the receiver and reasons for sending the money." Testimony of Mr. Phil Hopkins, Vice President Global Security, The Western Union Company, submitted to the United States Senate, Special Committee on Aging, at 4-5 (Mar. 13, 2013). http://www.aging.senate.gov/imo/media/doc/07_Hopkins_3_13_13.pdf. According to the testimony, "[i]f an Agent suspects the transaction is fraudulent, the Agent is trained to refuse the transaction or report it to Western Union for further investigation." *Id.*

[395] Indeed, money transfer providers are required to implement an effective AML program, which is "reasonably designed to prevent the [money transfer provider] from being used to facilitate money laundering and the financing of terrorist activities," and "shall be commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided by, the [money transfer provider]." FinCEN, Interpretive Release 2004-01: Anti-Money Laundering Program Requirements For Money Services Businesses with respect to Foreign Agents or Foreign Counterparties, 7 (2004) (citing 31 CFR 103.125). In addition, FinCEN has made clear that the AML programs of money transfer providers should, among other things, "establish procedures for conducting reasonable, risk-based due diligence on potential and existing foreign agents and counterparties to help ensure that such foreign agents and counterparties are not themselves complicit in illegal activity." *Id.* at 9. This includes "establish[ing] procedures for risk-based monitoring and review of transactions" sufficient to "identify and, where appropriate, report as suspicious such occurrences as[] instances of unusual wire activity". *Id.* at 10.

[396] *See supra* notes 352-361 and accompanying text discussing law enforcement cases against Western Union and MoneyGram.

[397] TMSRT at 3.

and detect the abuse of their money transfer systems by reinforcing their anti-fraud warnings to consumers and money transfer agents.[398]

TMSRT further argues that the amended rule would result in "substantial disruption" absent additional guidance on how members should determine if the recipient is a telemarketer.[399] Commission staff regularly provides guidance to industry about how to comply with specific rules, as well as other legal obligations,[400] while also recognizing in other contexts that it is critical for industry segments and individual members to have the flexibility to comply with the requirements of a rule in ways that are consistent with their business practices. As noted above, some members of TMSRT already have practices in place, for example, to train and incentivize agents to recognize and halt unlawful transactions. For instance, Western Union trains agents "on how to detect and deter fraud at the point-of-sale," makes a fraud hotline available to all agents, has a monetary reward program to encourage agents to detect and deter consumer fraud, and monitors agent activity to identify those complicit in fraudulent activity.[401]

The Commission also declines TMSRT's request to amend the proposed Rule to provide an exemption or safe harbor for providers of cash-to-cash money transfers.[402] Past law enforcement actions by the Commission and others provide detailed information about how money transfer providers can operate within the bounds of the law. For example, in the Commission's case against MoneyGram, the complaint contains detailed allegations describing

---

[398] Moreover, the prohibition will have no adverse impact on the industry's potential implementation of a database of terminated agents. *Id.* at 7 ("Facilitation of such a database will be instrumental in fighting telemarketing fraud and should be considered as an approach to addressing the issues raised in the rulemaking.").
[399] *Id.* at 5.
[400] *See, e.g.*, Compliance Guide, FTC, *Complying With the Telemarketing Sales Rule*, *available at* http://www.ftc.gov/tips-advice/business-center/complying-telemarketing-sales-rule; Business Guide, FTC, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising* (March 2013), *available at* http://www.ftc.gov/system/files/documents/plain-language/bus41-dot-com-disclosures-information-about-online-advertising.pdf.
[401] *See supra* note 394.
[402] TMSRT at 7.

how MoneyGram knew that its system was being used to defraud people but did very little about it.[403] The stipulated permanent injunction in the case also outlines specific measures that MoneyGram must take to detect and prevent fraud-induced money transfers (not just cash-to-cash money transfers), including those involving telemarketing.[404] Similarly, DOJ-Criminal's complaint and deferred prosecution agreement illustrates the company's failure to terminate specific MoneyGram agents it knew to be involved in fraud schemes and its willful failure to maintain an effective AML program.[405]

Under the amended Rule, a cash-to-cash money transfer provider that has actual knowledge that the transfer is related to telemarketing, or consciously avoids knowing (such as by deliberately ignoring) signs that the transfer is related to telemarketing, may be found liable for assisting and facilitating a violation of the TSR. The Commission sees no reason to afford special treatment to this industry segment, particularly given past actions, by either lowering or raising the liability standard.[406] To the contrary, the Commission expects the bright lines set by the amended Rule to create a level playing field for all money transfer providers and assist consumers in avoiding fraud.

Finally, addressing commenters' general concerns about this Rule amendment, the Commission recognizes that regulation and law enforcement have limitations and cannot prevent or eliminate all fraud. However, the Commission concludes, based on the substantial record of fraudulent telemarketers' use of cash-to-cash money transfers, that a prohibition on the use of this type of money transfer in telemarketing is an important, beneficial, and a vital step in

[403] *See supra* notes 354-355 and accompanying text.
[404] The allegations and settlements reached by state attorneys general against Western Union are similarly instructive. *See supra* notes 352-353 and accompanying text.
[405] *See supra* notes 350 and accompanying text.
[406] The Commission also declines the requests of some commenters to impose strict liability on those cash-to-cash money transfer providers that, despite their best efforts to detect unlawful transactions, unwittingly transfer money in connection with telemarketing transactions. AFR at 1; NCLC at 13.

protecting consumers from the substantial and unavoidable harm caused by these practices. Given that there is no evidence that legitimate telemarketers use this payment mechanism, the Commission concludes that the burden on legitimate marketers is non-existent and that any burden to money transmitters seeking to comply with the new rule would be minimal given the existing prohibition against assisting and facilitating violations of the Rule and past law enforcement actions.

(2) Cash Reload Mechanisms

The rulemaking record confirms that the substantial and unavoidable harm to consumers resulting from the use of cash reload mechanisms in telemarketing transactions is unjustified by any countervailing benefits to consumers or competition. As with cash-to-cash money transfers, fraudulent telemarketers and sellers exploit cash reload mechanisms to avoid the use of conventional payment alternatives that are subject to federal consumer protection laws. Recent complaint data indicates that increasing numbers of consumers each year are paying tens of millions of dollars in fraud-induced cash reload mechanisms, including in the telemarketing context.[407]

Also, as with cash-to-cash money transfers, the use of cash reload mechanisms in telemarketing requires the consumer to take several burdensome steps to initiate payment after the telephone call ends. The consumer typically must go to a retail location to select a cash reload card, pay a fee, provide the funds to be loaded, and engage in another telephone call to provide the telemarketer with the PIN code. For these reasons, it is not surprising that the record is devoid of evidence that any legitimate telemarketers or sellers rely on cash reload mechanisms in telemarketing transactions.

[407] Written Statement of Green Dot, *supra* note 50, at 2; 2014 Consumer Sentinel Network Data Book, *supra* note 371, at 8.

The rulemaking record demonstrates that cash reload mechanisms offer perpetrators of telemarketing fraud a relatively anonymous and irretrievable method for obtaining funds from consumers. The Commission concludes that this mounting economic harm is not outweighed by any countervailing benefits to consumers or competition. The largest cash reload provider, Green Dot, evidently agrees.[408] Green Dot recently completed the discontinuance of its MoneyPak cash reload mechanism for GPR cards on its network.[409] The company's testimony explains that "without the MoneyPak PIN, the scammer will have no method of instructing a senior to buy a product and no method of redeeming any associated PIN number."[410] Notably, other cash reload providers, InComm and Blackhawk Network, also completed the voluntary discontinuance of cash reload mechanisms for GPR cards on their networks.[411] Despite the voluntary measures taken by these three major cash reload providers, the prohibition is necessary to ensure that all current and future cash reload providers abide by the same rules.

The Commission believes that a prohibition on the use of cash reload mechanisms will complement and reinforce the laudable response of these three cash reload providers to the growing use of these payment methods in telemarketing fraud. A prohibition on the use of these payment methods by telemarketers and sellers will provide bright line guidance benefitting both consumers and the telemarketing industry. Instead of general warnings from cash reload providers, consumer will receive the benefit of clear instructions and guidance from the federal government, advising that it is illegal for a seller or telemarketer to accept a cash reload

[408] Green Dot weighed the impact of its decision on "honest customers who routinely rely on the MoneyPak PIN method for adding money to a family member's card" in determining to "eliminate the MoneyPak as an instrument of [fraud]"). Written Statement of Green Dot, *supra* note 50, at 2.
[409] According to the website www moneypak.com (last visited April 8, 2015), "MoneyPak® is no longer available for purchase."
[410] *Id.*
[411] InComm Press Release, *supra* note 51; Testimony of Blackhawk Network, *supra* note 51, at 3 & 5.

mechanism as payment. Legitimate telemarketers and sellers, in turn, should benefit from increased consumer confidence.

Commenters opposed to the prohibition submit that the amendment is overbroad and "could potentially prohibit consumers' legitimate uses of cash reload mechanisms that are unrelated or incidental to any telemarketing activity," such as payments to billers, e-commerce merchants, and utility companies.[412] These comments overlook the fact that the prohibition is limited to telemarketing transactions covered by the Rule and does not extend to non-telemarketing transactions like the bill payment transactions they cite. The payment of an existing bill without further solicitation is not a telemarketing transaction subject to the TSR, and the language of the amended Rule does not broadly prohibit or restrict the use of cash reload mechanisms in such non-telemarketing transactions, as some opponents suggested.[413]

Moreover, the implementation by the three major cash reload providers of the swipe reload process for GPR cards will likely render obsolete the use of cash reload mechanisms as direct payment for such non-telemarketing transactions. Today, consumers without access to traditional banking can load funds using the swipe process directly to a GPR card instead of using a PIN-based reload mechanism. In turn, consumers can use these GPR cards to pay for goods or services, make a bill payment, or buy from an e-commerce merchant. To the extent that cash reload mechanisms may have been used for such transactions in the past,[414] the

[412] InComm at 2; *see* Green Dot at 2.
[413] InComm at 2-3; ETA at 1. The prohibition restricts a telemarketer or seller from accepting a cash reload mechanism as payment only "for goods or services offered or sold through telemarketing or as a charitable contribution solicited or sought through telemarketing"). *NPRM*, *supra* note 1, at 41218.
[414] Before the discontinuance of MoneyPak, Green Dot established "authorized biller relationships" permitting consumers to use a cash reload mechanism to legitimately pay existing bills without having to first load the funds onto an existing GPR card or into an account with an online payment intermediary. It appears that no other cash reload providers currently have established such authorized biller relationships. For example, consumers cannot redeem a Vanilla Reload Pack directly with a biller or e-commerce merchant. Instead, consumer must use Vanilla Bill Payment, which is a single-use prepaid card that can be used to make purchases or pay bills wherever

Commission is not persuaded that permitting their use is still necessary. Thus, any adverse effect of the TSR's prohibition against cash reload mechanisms on their use in non-telemarketing transactions would be minimal.

In light of the swipe reload availability, it may be useful to further clarify the scope of the cash reload ban in telemarketing. The prohibition does not prevent the use of other payment mechanisms, such as GPR cards, single-use prepaid cards, or funds in an account with an online payment intermediary, to pay for purchases. This is true even if a consumer uses a (PIN-based) cash reload mechanism to load funds onto an existing GPR card or another personal account. The Commission's concern is not the use of GPR cards or personal accounts – these have additional and more robust protections than cash reload mechanisms.[415]

Comments opposed to the prohibition expressed concern about liability exposure for assisting and facilitating violations of the Rule and argue for a safe harbor or limitation on what constitutes "substantial assistance" under the TSR.[416] The Commission recognizes that the "self-service" nature of cash reload mechanisms, to the extent they still exist in the marketplace, could create particular challenges for providers to know whether a consumer will use a cash reload mechanism to pay an authorized biller, reload a GPR card for a college-bound student, or send funds to a fraudulent telemarketer. The Commission is not persuaded, however, that it is

---

MasterCard or Visa are accepted. *See*, InComm, *Vanilla Bill Pay: Important Things to Know, available at* https://www.vanillabillpay.com/important.html?csrfToken=3IU1JoeDwueue2gIFvpIf2mmVficlXTi (last visited February 12, 2015). Similarly, Blackhawk's Reloadit Pack can be used only to reload an existing GPR or a Reloadit Safe (an online account balance). *See*, Blackhawk Network, Inc., *Reloadit: How it Works, available at* https://www.reloadit.com/HowItWorks (last visited February 11, 2015). For these reasons, the Commission is unpersuaded that the prohibition against cash reload mechanisms in telemarketing will have any adverse effect on consumers' ability to pay billers and utility companies.

[415] *See supra* notes 32 & 36 (describing how merchants accepting network-branded debit cards, including prepaid cards, are subject to the operating rules and anti-fraud monitoring of the payment card networks) and 178 (describing the voluntary zero liability protections afforded consumers in signature debit card transactions). In addition, the CFPB's proposed Prepaid Account Rule may extend to GPR cards the protections of the EFTA and Regulation E. *See* Prepaid Account Rule, *supra* note 36.

[416] Green Dot at 2; InComm at 4; ETA at 1.

necessary or appropriate to amend the proposed Rule to provide an exemption or safe harbor for providers of cash reload mechanisms, or otherwise to limit the assisting and facilitating provision as it may be applied to them. The record makes clear that providers of cash reload mechanisms already have implemented anti-fraud measures and proactively already have restricted the availability of a reload mechanism altogether. Commenters, however, have not shown how the rule change might impose costs different from those already incurred (or being eliminated) for fraud detection or why the general "substantial assistance" standard otherwise imposes a burden unique to providers of cash reload mechanisms. Thus, the Commission sees no basis upon which to change the existing TSR standards for "substantial assistance."

4. Final Rule Language

The NPRM proposed new definitions of "cash-to-cash money transfer" and "cash reload mechanism." The Commission solicited public comment as to whether the proposed definitions adequately, precisely, and correctly described each payment alternative. In response, the Commission received no comments on the definition of cash-to-cash money transfer; and relevant comments from two cash reload providers, InComm and Green Dot regarding the definition of cash reload mechanism. Both of these comments were received before three providers began implementing a swipe reload process for adding funds to GPR cards on their networks. At that time, both commenters expressed concern that the term, in combination with the definition of "telemarketing," would restrict the use of this payment method by consumers in legitimate non-telemarketing transactions, such as bill payments.[417] Only Green Dot proposed a specific change to the definition, suggesting that the Commission amend the definition

[417] Green Dot at 2; InComm at 2-3.

specifically to cover only those cash reload mechanisms used to load GPR cards.[418] Based on the evidence in the record, the Commission declines to narrow the definition of "cash reload mechanism" as proposed by Green Dot, which was based on a business model that has now shifted dramatically with the discontinuance of GreenDot's cash reload mechanism.

Nevertheless, the Commission concludes that some changes to the definition are warranted. As noted previously, the Commission's concern pertains to the ease with which perpetrators of telemarketing fraud use cash reload mechanisms as an inexpensive and largely irreversible method of siphoning money from defrauded consumers who divulge their cash reload PIN number or similar security code. Con artists can easily abscond with the money by applying funds from the cash reload mechanism to GPR cards or to online accounts they obtain using false names. This is the problem the Commission intends to curtail.

By contrast, the Commission does not intend the Rule to cover telemarketing transactions in which a consumer uses a GPR card (or an online account balance with a payment intermediary) to pay for goods and services. This is true even if the consumer previously added funds to the GPR card or other online account via a swipe reload process or (to the extent it still exists) a PIN-based cash reload mechanism). In those instances, the telemarketer or seller is accepting the GPR card as payment, not a cash reload mechanism like a PIN number.[419] The Commission has revised the final definition of cash reload mechanism to ensure that the language is flexible enough to cover future adaptations by scammers, and sufficiently narrow to prohibit the abusive practices documented in the rulemaking record.

[418] Green Dot at 2.
[419] Similarly, the prohibition does not apply to payments made from a digital wallet or safe, regardless of whether they were deposited by means of a swipe reload or PIN-based cash reload mechanism.

To implement the prohibition against the use of cash-to-cash money transfers and cash reload mechanisms, the Commission amends section 310.4(a) to add a new subsection (10). Section 310.4(a)(10) of the amended Rule states that it is an abusive practice for a seller or telemarketer to accept from a customer or donor, directly or indirectly, a cash-to-cash money transfer or cash reload mechanism as payment for goods or services offered or sold through telemarketing or as a charitable contribution solicited or sought through telemarketing. The language of the prohibition addresses the receipt, directly or indirectly, of a cash reload mechanism by a telemarketer or seller. For reasons already discussed above, the prohibition does not cover circumstances where a consumer pays bills or merchants (including telemarketers) using a GPR card or account with an online payment intermediary that was funded by a cash reload mechanism.

As with the prohibition against the use of remotely created payment orders, the Commission concludes that the risks associated with cash-to-cash money transfers and cash reload mechanisms exist equally in outbound and inbound telemarketing calls. Accordingly, the prohibitions in section 310.4(a)(10) apply to both outbound and inbound telemarketing. However, to minimize the burden on sellers and telemarketers that have qualified for the general media and direct mail exemptions from the TSR for inbound telemarketing, the Commission is modifying the proposed amendments to sections 310.6(b)(5) and (6). The purpose of the modification is to clarify that sellers and telemarketers that comply with the prohibition on the use of cash-to-cash money transfers and cash reload mechanisms in inbound telemarketing remain exempt from the TSR's requirements if they otherwise qualify for the general media or direct mail exemptions. Thus, they are covered by the TSR only if they violate the prohibition. Moreover, while non-compliance with one of these prohibitions subjects the violator to a TSR

enforcement action for the violation, it does not deprive the violator of its exemption from the other requirements of the TSR.

C. Final Rule and Comments Received on Expansion of Advance Fee Ban on Recovery Services

The original TSR prohibited the abusive telemarketing practice of collecting advanced fees for services promising to recover losses incurred by consumers in a previous telemarketing transaction.[420] The NPRM proposed to expand the coverage of the existing advance fee ban on recovery services to include losses incurred in any prior transaction, not just telemarketing transactions.[421] The Commission received several comments supporting the expansion of the Rule to cover non-telemarketing transactions.[422] No commenters opposed the amendment.

The NPRM proposed the expansion in response to the widespread migration of frauds to other communication channels made possible by new technologies, including Internet websites and email. As a result, the Commission finds that telemarketers selling recovery services are just as likely to obtain lists of online scam victims as they are to obtain lists of victims of telemarketing fraud. These telemarketers can easily avoid the Rule's current advance fee prohibition simply by telemarketing their advance fee recovery services only to victims of online scams. Indeed, in *United States v. Business Recovery Services, LLC*, the defendants were

[420] 16 CFR 310.4(a)(3).
[421] *NPRM*, *supra* note 1, at 41215.
[422] AARP at 1 ("AARP strongly supports the FTC proposal[] to . . . expand the scope of the advance fee ban on recovery services"); AFR at 2 ("We support the proposal to ban advance fees charged for purported help in recovering losses in connection with prior internet scams"); AGO at 12 (expressing support for "broadening the ban on telemarketing recovery services to include losses incurred in any medium"); DOJ-CPB at 3-4 ("The goal of this specific provision is to protect consumers from the deceptive acts of recovery services, not the underlying business from which the consumer lost money. Thus, whether the underlying business acted through telemarketing is irrelevant."); DOJ-Criminal at 4 ("Because mass-marketing fraud techniques have changed over time, there is no substantial reason that the TSR's scope should be limited only to recovery schemes that claim to recover funds lost in a previous telemarketing transaction."); Michael (stating that recovery companies "prey on victims of work-at-home and other similar companies who have been defrauded for thousands of dollars and are looking for a place to turn."); NCLC at 15 ("There is no reason to make a distinction based on the circumstances of the [original] loss."); *see generally* Transp. FCU.

charged with selling worthless do-it-yourself kits for as much as $499 to consumers who had lost money on business opportunity and work-at-home scams sold via telemarketing and online marketing.[423] Where consumers' losses resulted from online scams, prosecutors could not charge defendants with violations of the TSR.

The Commission agrees with the DOJ-CPB that there exists "no logical reason" to differentiate recovery room victims based on whether the original scam was a telemarketing scam.[424] To ensure that advanced fees are prohibited for all recovery services, regardless of whether the loss resulted from a telemarketing transaction, the Commission adopts the change to section 310.4(a)(3) proposed in the NPRM.

III. Final Rule and Comments Received on Clarifying Amendments

The Commission received comparatively few comments on the proposals in the NPRM to modify five existing TSR provisions to make Commission enforcement policy more transparent. These amendments: (1) clarify that any recording made to memorialize a customer's or donor's express verifiable authorization ("EVA") pursuant to section 310.3(a)(3)(ii) must include an accurate description, clearly and conspicuously stated, of the goods or services or charitable contribution for which payment authorization is sought; (2) clarify that the exemption for calls to businesses in section 310.6(b)(7) extends only to calls inducing a sale or contribution from the business, and not to calls inducing sales or contributions from individuals employed by the business; and (3) address provisions pertaining to the Do Not Call requirements of the TSR.

---

[423] *U.S. v. Bus. Recovery Servs., LLC*, Civ. No. 11-00390-JAT (D. Ariz. Sept. 13, 2013) (Stip. Perm. Inj.); DOJ-CPB at 4-5; Press Release, FTC, *FTC Settlement and Default Judgment Impose Permanent Ban on Marketers of Scam 'Recovery' Kits* (Nov. 20, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/11/ftc-settlement-default-judgment-impose-permanent-ban-marketers.

[424] DOJ-CPB at 4.

Specifically, the amendments to the Do Not Call provisions pertain to three sections. The first amendment expressly states that a seller or telemarketer bears the burden of demonstrating that the seller has an existing business relationship ("EBR") with a customer whose number is listed on the Do Not Call Registry, or has obtained an express written agreement ("EWA") from such a customer, as required by section 310.4(b)(1)(iii)(B)(i)-(ii). Second, the amendments illustrate the types of impermissible burdens on consumers that violate section 310.4(b)(1)(ii), which prohibits denying or interfering with a consumer's right to be placed on a seller's or telemarketer's entity-specific do-not-call list. In addition, they specify that a seller's or telemarketer's failure to obtain the information needed to place a consumer on a seller's entity-specific do-not-call list pursuant to that section disqualifies it from relying on the safe harbor for isolated or inadvertent violations in section 310.4(b)(3). Third, they modify the prohibition in section 310.8(c) against sellers sharing the cost of registry fees to emphasize that the prohibition is absolute.

A. Section 310.3(a)(3)(ii) – Oral Verification Recording as Evidence of EVA

The NPRM proposed an amendment to make it unmistakably clear that an oral verification recording of a consumer's agreement to be charged for a telemarketing transaction must include "an accurate description, clearly and conspicuously stated, of the goods or services or charitable contribution for which payment authorization is sought."[425] Five comments supported this clarification,[426] and none opposed it.

[425] *NPRM*, *supra* note 1, at 41217.
[426] Transp. FCU at 1; DOJ-Criminal at 5; AGO at 12; AARP at 1-2; NCLC at 15-16. The latter two comments, while supporting the amendment, also argued for a recording of the entire telemarketing call, a proposal that would require a separate rulemaking proceeding.

Section 310.3(a)(3)(ii) permits the use of an audio recording to memorialize a consumer's express verifiable oral authorization of a charge for a telemarketing transaction.[427] It requires that the recording "evidences clearly both the customer's or donor's authorization of payment for the goods or services or charitable contribution that are the subject of the telemarketing transaction," and the customer's or donor's receipt of specified material information about the transaction.[428] The Commission has uniformly interpreted this provision as requiring a clear and conspicuous description in the recording of the goods, services, or charitable donation for which payment is sought.[429] Because the Commission's law enforcement experience shows that some sellers and telemarketers appear to have omitted this information intentionally from their audio recordings to conceal from consumers the real purpose of the verification recording and the fact that they will be charged,[430] the Commission has decided to adopt the proposed amendment.

B. Section 310.6(b)(7) – Limitation on Business-To-Business Exemption

The NPRM proposed an amendment to make it explicit that the business-to-business exemption is available only to sellers and telemarketers that are soliciting the purchase of goods or services or a charitable contribution by the business itself, rather than personal purchases or

---

[427] Section 310.3(a)(3) prohibits sellers and telemarketers from billing for telemarketing purchases or donations without a customer's or donor's "express verifiable authorization," if payment is not made by credit or debit card.
[428] 16 CFR 310.3(a)(3)(ii). The new mandate of an accurate description of the goods or services or charitable contribution will be added to the list of required disclosures identified in section 310.3(a)(3)(ii)(A). The six original disclosures the seller or telemarketer has been required to make and include in the recording by sections 310.3(a)(3)(ii)(A)-(G) will be renumbered as sections 310.3(a)(3)(ii)(B)-(H). These disclosures are the number of debits, charges or payments (if more than one); the date(s) the debit(s), charge(s), or payment(s) will be submitted for payment; the amount(s) of the debit(s), charges(s), or payment(s); the customer's or donor's name; the customer's or donor's billing information identified with sufficient specificity that the customer or donor understands what account will be used to collect payment for the goods or services or charitable contribution that are the subject of the telemarketing transaction; a telephone number for customer or donor inquiry that is answered during normal business hours; and the date of the customer's or donor's oral authorization.
[429] As the Commission noted in the NPRM, "it is difficult to imagine how a verification recording could 'evidence clearly' a payment authorization 'for the goods or services or charitable contribution that are the subject of the telemarketing transaction' without mentioning the goods, services, or charitable contribution." 78 FR at 41217 & n. 182 (citing cases alleging material changes or complete omissions in verification recordings of the pre-sale descriptions of the goods or services).
[430] *Id.*

contributions by employees of the business. Five comments generally supported the amendment,[431] and one argued against it.[432]

The comment opposing the amendment is based on a fundamental misunderstanding. It incorrectly presumes that the existing provision exempts telemarketing calls directed to a business telephone number to solicit sales or charitable contributions from individual employees. That has never been the case. By its terms, the exemption applies only to "[t]elephone calls between a telemarketer *and any business*."[433] Moreover, the fact that the exemption expressly excludes "calls to induce the retail sale of non-durable cleaning or office supplies," which are hardly for the personal use of individual employees, provides additional evidence that the Commission limited the exemption at the outset to solicitations directed to a business, and not its employees.[434]

Thus, the Commission's decision to adopt this amendment is simply a clarification of the scope of the existing exemption, not a change in its substance. This clarification should further deter telemarketers from attempting to circumvent the Registry by soliciting employees at their places of business to make personal charitable contributions or to purchase goods or services for their individual use.[435] As amended, the exemption applies only to "[t]elephone calls between a

[431] AFR at 2; NCLC at 16; AGO at 12; DOJ-CPB at 1; DOJ-Criminal at 1; *cf.* Blue Diamond Remodeling at 1 (complaining that its business has been "flooded by telemarketer calls for years").
[432] InfoCision at 4-5.
[433] 16 CFR 310.6(b)(7) (emphasis added).
[434] *Id.*; *see also TSR Final Rule 1995*, *supra* note 8, at 43861 (discussing the exemption and noting that cleaning and office supply scams are not included in the exemption because "such telemarketing falls within the Commission's definition of deceptive telemarketing acts or practices"). Contrary to an additional objection on First Amendment grounds, InfoCision at 4-6, it remains the Commission's opinion that telemarketing calls made to business telephone numbers to solicit individual employees at work can be deceptive, and therefore are properly subject to the limited commercial speech restrictions of the TSR.
[435] *NPRM*, *supra* note 8, at 41219 (mentioning solicitations to employees at work for dietary products, auto warranties, and credit assistance).

telemarketer and any business to induce the purchase of goods or services or a charitable contribution by the business."

C. Amendments to Clarify Do Not Call Provisions

The 2003 amendments to the TSR that created the National Do Not Call Registry included provisions: (1) permitting live telemarketing calls to numbers on the registry if the seller has an EBR with the person called or has obtained his or her EWA to receive the call; (2) prohibiting sellers or telemarketers from denying or interfering in any way with a consumer's right to be placed on its entity-specific do-not-call list; and (3) barring sellers and telemarketers from sharing the fees for accessing the Registry. The remaining amendments seek to clarify these three provisions to reflect the Commission's intent and enforcement policy. The TSR requires sellers and telemarketers to delete from their calling lists any home or cell phone number that consumers have placed on the Registry.

1. Section 310.4(b)(1)(iii)(B) – EBR and EWA Burden of Proof

The NPRM proposed modifications to the EBR and EWA carve outs from the prohibition against outbound telemarketing calls to numbers on the National Do Not Call Registry. The amendments emphasize that calls to numbers on the Registry are permitted only if the seller or telemarketer "can demonstrate that the seller has" an EBR or EWA.[436] Four comments supported the amendments.[437] One comment opposed the amendment as unnecessary in view of prior Commission statements that sellers and telemarketers bear that burden, arguing that it would "confuse sellers, telemarketers, consumers, and regulators."[438]

[436] *Id.* at 41218-19.
[437] AFR at 2; NCLC at 16; AGO at 12; DOJ-CPB at 4 (citing legal principles and case law assigning the burden to the seller or telemarketer).
[438] InfoCision at 4.

As stated in the NPRM, the Commission's goal in proposing these amendments was "to make it unmistakably clear that the burden of proof for establishing" an EWA or EBR as an affirmative defense to otherwise prohibited calls to numbers on the Registry "falls on the seller or telemarketer relying on it."[439] The Commission believes that the two carve outs from the prohibition should transparently alert anyone reading them that the seller or telemarketer must be able to demonstrate that the seller meets the EWA or EBR requirements, rather than require research into applicable law and prior Commission statements to determine this burden of proof. Consequently, the Commission has decided to adopt the two amendments that accurately reflect existing law.

In adopting the amendments, the Commission again wishes to emphasize that each of the carve outs is limited to the specific seller that obtained the EWA directly from, or has an EBR directly with, the person called.[440] Consequently, cold calls to consumers whose names and numbers appear on a calling list purchased from a third-party list broker are prohibited by the TSR's do-not-call provisions because the calls are not placed by the specific seller that obtained the EWA or EBR.

2. Sections 310.4(b)(1)(ii) & 310.4(b)(3) – Denying or Interfering with a Consumer's Right To Opt-Out

The NPRM proposed an amendment to clarify the types of burdens that impermissibly deny or interfere with a consumer's right to be placed on an entity-specific do-not-call list. In addition, it included an amendment to disqualify a seller or telemarketer from the safe harbor for

[439] *NPRM, supra* note 1, at 41218.
[440] *Id.* at 41219.

isolated or inadvertent violations if it fails to obtain the information needed to honor a do-not-call request.[441] Six comments supported the amendments,[442] and none opposed them.

The Commission accordingly has decided to adopt the amendment to Section 310.4(b)(1)(ii), which currently prohibits sellers and telemarketers from "[d]enying or interfering in any way, directly or indirectly" with a consumer's right to be placed on an entity-specific do-not-call list. In order to make the prohibition more explicit and to put sellers and telemarketers clearly on notice of the practices it prohibits, the amendment adds illustrative examples of the types of burdens the Commission regards as impermissible. As amended, the prohibition lists the following examples of impermissible burdens: harassing consumers who make such a request, hanging up on them, failing to honor the request, requiring the consumer to listen to a sales pitch before accepting the request, assessing a charge or fee for honoring the request, requiring the consumer to call a different number to submit the request, and requiring the consumer to identify the seller or charitable organization making the call or on whose behalf the call is made.[443]

The Commission also amends section 310.4(b)(3), which provides a safe harbor for inadvertent violations of the prohibition in section 310.4(b)(1)(ii) against denying or interfering with an entity specific do-not-call request if certain requirements are met. The amendment was specifically supported by one comment and none opposed it.[444] As amended, section 310.4(b)(3) withholds the benefits of the safe harbor from a seller or telemarketer that fails to obtain the information necessary to honor an entity-specific do-not-call request. This amendment emphasizes that section 310.4(b)(1)(ii) places the burden on sellers and

[441] *Id.* at 41218.
[442] Transp. FCU; AFR at 2; NCLC at 16; AGO at 12; DOJ-CPB at 1; DOJ-Criminal at 1.
[443] *See NPRM, supra* note 1, at 41218.
[444] DOJ-Criminal at 1.

telemarketers to obtain the information they need to comply with a do-not-call request because they are in a better position to obtain the information they need than consumers, who are often uncertain about the identity of the seller on whose behalf a call is made.[445]

3. Section 310.8(c) – Prohibition on Registry Fee Sharing

The NPRM proposed a clarification that would make it explicit that the TSR prohibition against sellers sharing the cost of Registry fees is absolute. Five comments noted their support for the amendment,[446] and none opposed it.

The original prohibition was adopted by the Commission in conformity with regulations previously adopted by the FCC that flatly ban any sharing or division of costs for accessing the National Do Not Call Registry.[447] As the NPRM noted, it was the Commission's intention to adopt a blanket prohibition on any division or sharing of costs for accessing the Do Not Call Registry, but the provision could be read as permitting a person to sign up to access the Registry and, before ever actually accessing it, sell or transfer the registration for consideration to others seeking Registry access. The Commission has determined to adopt the proposed amendment to conform it more closely to the FCC prohibition and to prevent any possible misreading of the absolute prohibition.[448] As amended, the prohibition in the final sentence of section 310.8(c) emphasizes that "[n]o person may participate in any arrangement to share the cost of accessing the National Do Not Call Registry, including any arrangement with any telemarketer or service provider to divide the costs to access the registry among various clients of that telemarketer or service provider."

---

[445] *See NPRM, supra* note 1, at 41200.
[446] AFR at 2; NCLC at 16; AGO at 12; DOJ-CPB at 1; DOJ-Criminal at 1.
[447] *Telemarketing Sales Rule Fees*, 68 FR 45134, 45136 nn.29-30 (July 31, 2003) (citing 47 CFR 64.1200(c)(2)(i)(E), as amended July 3, 2003)). The prohibition is necessary because "allowing telemarketers and others to share the information obtained from the national registry "would threaten the financial support for maintaining the database." *Id.* at 45136.
[448] *See NPRM, supra* note 1, at 41220.

IV. Regulatory Analysis and Regulatory Flexibility Act Requirements

The Regulatory Flexibility Act of 1980 ("RFA")[449] requires a description and analysis of proposed and final rules that will have a significant economic impact on a substantial number of small entities.[450] The RFA requires an agency to provide an Initial Regulatory Flexibility Analysis ("IRFA")[451] with the proposed rule and a Final Regulatory Flexibility Analysis ("FRFA")[452] with the final rule, if any. Section 605 of the RFA[453] provides that such an analysis is not required if the agency head certifies that the regulatory action will not have a significant economic impact on a substantial number of small entities.

Although the Commission believed that the amendments it proposed would not have a significant economic impact upon small entities, it included an IRFA in the NPRM and solicited public comment on it. None of the public comments received addressed the IRFA. The Commission continues to believe that the amendments it is adopting will not have a significant economic impact upon small entities, but nonetheless in the interest of caution is providing this FRFA.

A. Need for and Objectives of the Rule Amendments

As described in Sections II through III above, the amendments are intended to address telemarketing sales abuses arising from the use of remotely created checks, remotely created payment orders, cash-to-cash money transfers, cash reload mechanisms, recovery services, and entity-specific do-not-call requests. Other amendments clarify several TSR requirements in order to reflect longstanding Commission enforcement policy. The objective of the amendments

[449] 5 U.S.C. 601-612.
[450] The RFA definition of "small entity" refers to the definition provided in the Small Business Act, which defines a "small-business concern" as a business that is "independently owned and operated and which is not dominant in its field of operation." 15 U.S.C. 632(a)(1).
[451] 5 U.S.C. 603.
[452] 5 U.S.C. 604.
[453] 5 U.S.C. 605.

is to curb deceptive and abusive practices occurring in telemarketing. The legal basis for the amendments is the Telemarketing Act.

B. Significant Issues Raised by Public Comments in Response to the IRFA, including any Comments Filed by the Chief Counsel for Advocacy of the Small Business Administration, and the Agency's Response, Including any Changes Made in the Final Rule Amendments

As noted earlier, no comments, including any from the Small Business Administration, were received directly in response to the IRFA. Some concerns were raised about the potential effect of the prohibition against remotely created payment orders and remotely created checks on small business by FRBA and by InfoCision, as discussed in section II.A.2 above.[454]

C. Description and Estimate of the Number of Small Entities to Which the Amendments Will Apply or Explanation Why No Estimate Is Available

The amendments to the Rule affect sellers and telemarketers engaged in "telemarketing," as defined by the Rule to mean "a plan, program, or campaign which is conducted to induce the purchase of goods or services or a charitable contribution, by use of one or more telephones and which involves more than one interstate telephone call."[455] For the majority of entities subject to the amendments – sellers and telemarketers – a small business is defined by the Small Business

[454] *See also supra* note 220; InfoCision at 2; FRBA-1 at 3.
[455] 16 CFR 310.2(dd). The Commission notes that, as mandated by the Telemarketing Act, the interstate telephone call requirement in the definition excludes small business sellers and the telemarketers who serve them in their local market area, but may not exclude some sellers and telemarketers in multi-state metropolitan markets, such as Washington, DC.

Administration as one whose average annual receipts do not exceed $7 million.[456]

Determining a precise estimate of how many of these are small entities, or describing those entities further, is not readily feasible because the staff is not aware of published data that report annual revenue or employment figures for the industry. The Commission invited comment and information on this issue, but received no comments.

D. Description of the Projected Reporting, Recordkeeping and Other Compliance Requirements of the Amendments, Including an Estimate of the Classes of Small Entities That Will Be Subject to the Requirement and the Type of Professional Skills Necessary for Preparation of the Report or Record

The Commission does not believe that the amendments impose any new disclosure, reporting, recordkeeping or other compliance burdens. Rather, the amendments add to or revise existing TSR prohibitions and clarify existing requirements. The amendments: (1) add new prohibitions barring the use of remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms in both outbound and inbound telemarketing; and (2) revise the existing prohibition on advance fee recovery services, now limited to recovery of losses in prior telemarketing transactions, to include recovery of losses in *any* previous transaction.

The amendments also include a number of minor technical revisions that do not impose any new disclosure, reporting, recordkeeping or other compliance burdens, but merely clarify

[456] These numbers represent the size standards for most sellers in retail and service industries ($7 million total receipts). The standard for "Telemarketing Bureaus and Other Contact Centers" (NAICS Code 561422) is also $7 million. A list of the SBA's current size standards for all industries can be found in SBA, *Table of Small Business Size Standards Matched to North American Industry Classification System Codes, available at* http://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf.

existing TSR requirements to reflect Commission enforcement policy. These amendments state expressly (1) that the seller or telemarketer bears the burden of demonstrating under 16 CFR 310.4(b)(1)(iii)(B) that the seller has an existing business relationship ("EBR") with a customer whose number is listed on the Do Not Call Registry, or has obtained the express written agreement ("EWA") of such a customer to receive a telemarketing call, as previously stated by the Commission; (2) that the requirement in 16 CFR 310.3(a)(3)(ii) that any recording made to memorialize a customer's or donor's express verifiable authorization ("EVA") must include an accurate description, clearly and conspicuously stated, of the goods or services or charitable contribution for which payment authorization is sought; (3) that the business-to-business exemption in 16 CFR 310.6(b)(7) extends only to calls inducing a sale or contribution from the business itself, and not to calls inducing sales or contributions from individuals employed by the business; (4) that under 16 CFR 310.8(c) no person can participate in an arrangement to share the cost of accessing the National Do Not Call Registry; and (5) provide examples of the types of impermissible burdens on consumers that the Commission regards as violations of 16 CFR 310.4(b)(1)(ii) because they deny or interfere with their right to be placed on a seller's or telemarketer's entity-specific do-not-call list. A related amendment specifies that a seller's or telemarketer's failure to obtain the information necessary to honor a consumer's request to be placed on a seller's entity-specific do-not-call list pursuant to 16 CFR 310.4(b)(1)(ii) disqualifies it from relying on the safe harbor in 16 CFR 310.4(b)(3) for isolated or inadvertent violations.

The classes of small entities affected by the amendments include telemarketers or sellers engaged in acts or practices covered by the Rule. The Commission maintains its belief, in the absence of any comments it requested on this issue, that no professional skills will be required

for compliance with the amendments because the amendments do not impose any new reporting, recordkeeping, disclosure or other compliance requirements, and do not extend the scope of the TSR to cover additional entities.

E. Steps Taken to Minimize the Significant Impact, If Any, of the Rule Amendments, Including Why any Significant Alternatives Were Not Adopted

Although some of the public comments did suggest alternatives to the prohibition on the use of remotely created checks and remotely created payment orders in telemarketing, the Commission is not persuaded that the alternatives suggested would be equally effective in protecting consumers or that they are within the Commission's authority, as described above in section II.A.3.a(2). Nonetheless, in formulating the amendments, the Commission made every effort to avoid imposing unduly burdensome requirements on sellers and telemarketers. To that end, sellers and telemarketers that comply with the prohibitions on the use of remotely created checks and payment orders, cash-to-cash money transfers, and cash reload mechanisms in inbound telemarketing remain exempt from the TSR's requirements if they otherwise qualify for the general media or direct mail exemptions. Moreover, while non-compliance with one of these prohibitions subjects the violator to a TSR enforcement action for the violation, it does not deprive the violator of its exemption from the other requirements of the TSR. The Rule amendments regarding the advance fee ban on recovery services and the inapplicability of the safe harbor for telemarketers that fail to obtain the information necessary to honor a request to be placed on a seller's entity-specific do-not-call list do not add additional disclosure or recordkeeping burdens or unduly expand the scope of the TSR and are necessary to protect consumers.

V. Paperwork Reduction Act

The amendments adopted by the Commission do not create any new recordkeeping or disclosure requirements, or expand the existing coverage of those requirements to marketers not previously covered by the TSR. Accordingly, they do not invoke the Paperwork Reduction Act.[457]

The new prohibitions on the use of remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms apply not only to marketers making outbound calls that are currently subject to the TSR, but also to those who receive inbound calls from consumers as a result of direct mail or general media advertising. While the new prohibition on the use of novel payment methods applies to both outbound and inbound telemarketing calls, sellers and telemarketers that comply with these inbound telemarketing prohibitions remain exempt from the TSR if they otherwise qualify for the direct mail or general media exemptions.[458] These two exceptions include exemption from the TSR's disclosure and recordkeeping obligations. Moreover, while non-compliance with one of these prohibitions subjects the violator to a TSR enforcement action for the violation, it does not deprive the violator of its exemption from the other requirements of the TSR.

The expansion of the TSR's ban on advance fees for recovery services to apply to funds lost in *any* prior transaction also has no discernible PRA ramifications because it, too, requires no disclosures or recordkeeping. The same is true for the amendment making sellers and telemarketers ineligible for the safe harbor for isolated or inadvertent TSR violations if they fail to obtain the information necessary to honor a request to be placed on a seller's entity-specific

[457] 44 U.S.C. 3501-3521. The PRA also addresses reporting requirements, but neither the TSR nor the amendments present them.
[458] 16 CFR 310.6(b)(5)-(6).

do-not-call list. Nothing in that amendment requires any disclosure or recordkeeping.[459] Likewise, the Commission believes that the five technical amendments intended to make explicit the existing requirements of the TSR does not impose any new disclosure or recordkeeping obligations.

List of Subjects in 16 CFR Part 310

Telemarketing, trade practices.

For the reasons set forth in the preamble, the Federal Trade Commission amends title 16, Code of Federal Regulations as follows:

PART 310 TELEMARKETING SALES RULE 16 CFR PART 310

1. The authority citation for part 310 continues to read as follows:

Authority: 15 U.S.C. 6101-6108.

2. Amend § 310.2 by redesignating paragraphs (f) through (z) as paragraphs (h) through (bb), redesignating paragraphs (aa) through (ee) as paragraphs (dd) through (hh), and adding new paragraphs (f) through (g) and (cc), to read as follows:

§ 310.2 Definitions

* * * * *

(f) *Cash-to-cash money transfer* means the electronic (as defined in section 106(2) of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7006(2)) transfer of the value of cash received from one person to another person in a different location that is sent by a money transfer provider and received in the form of cash. The term includes a remittance transfer, as defined

[459] Even though some sellers and telemarketers, in order to prove that they are eligible for the safe harbor, might seek to document the fact that they have honored such requests, neither the amendment nor the TSR requires them to do so.

in section 919(g)(2) of the Electronic Fund Transfer Act ("EFTA"), 15 U.S.C. 1693a, that is a cash-to-cash transaction; however it does not include any transaction that is:

(1) An electronic fund transfer as defined in section 903 of the EFTA;

(2) Covered by Regulation E, 12 CFR part 1005.20, pertaining to gift cards; or

(3) Subject to the Truth in Lending Act, 15 U.S.C. 1601 et seq.

For purposes of this definition, *money transfer provider* means any person or financial institution that provides cash-to-cash money transfers for a person in the normal course of its business, whether or not the person holds an account with such person or financial institution.

(g) *Cash reload mechanism* is a device, authorization code, personal identification number, or other security measure that makes it possible for a person to convert cash into an electronic (as defined in section 106(2) of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7006(2)) form that can be used to add funds to a general-use prepaid card, as defined in Regulation E, 12 CFR part 1005.2, or an account with a payment intermediary. For purposes of this definition, a cash reload mechanism is not itself a general-use prepaid debit card or a swipe reload process or similar method in which funds are added directly onto a person's own general-use prepaid card or account with a payment intermediary.

* * * * *

(cc) *Remotely created payment order* means any payment instruction or order drawn on a person's account that is (a) created by the payee or the payee's agent

and (b) deposited into or cleared through the check clearing system. The term includes, without limitation, a "remotely created check," as defined in Regulation CC, Availability of Funds and Collection of Checks, 12 CFR part 229.2(fff), but does not include a payment order cleared through an Automated Clearinghouse (ACH) Network or subject to the Truth in Lending Act, 15 U.S.C. 1601 *et seq.*, and Regulation Z, 12 CFR part 1026, *et seq*.

* * * * *

3. Amend § 310.3 by redesignating paragraphs (a)(3)(ii)(A) through (G) as paragraphs (a)(3)(ii)(B) through (H), and adding new paragraph (a)(3)(ii)(A) to read as follows:

§ 310.3 Deceptive telemarketing acts or practices.

(a) * * *

(3) * * *

(ii) * * *

(A) An accurate description, clearly and conspicuously stated, of the goods or services or charitable contribution for which payment authorization is sought;

* * * * *

4. Amend § 310.4 by:

a. Revising paragraph (a)(3);

b. Adding new paragraphs (a)(9) and (a)(10);

c. Revising paragraphs (b)(1)(ii), (b)(1)(iii)(B), and (b)(3)(vi);

d. Amending paragraph (b)(7)(ii)(B) by removing "or" from the end of the paragraph; and

e. Amending paragraph (b)(8) by removing the final period and adding a semicolon in its

place to read as follows:

§ 310.4 Abusive telemarketing acts or practices.

(a) * * *

(3) Requesting or receiving payment of any fee or consideration from a person for goods or services represented to recover or otherwise assist in the return of money or any other item of value paid for by, or promised to, that person in a previous transaction, until seven (7) business days after such money or other item is delivered to that person. This provision shall not apply to goods or services provided to a person by a licensed attorney;

* * * * *

(9) Creating or causing to be created, directly or indirectly, a remotely created payment order as payment for goods or services offered or sold through telemarketing or as a charitable contribution solicited or sought through telemarketing; or

(10) Accepting from a customer or donor, directly or indirectly, a cash-to-cash money transfer or cash reload mechanism as payment for goods or services offered or sold through telemarketing or as a charitable contribution solicited or sought through telemarketing.

* * * * *

(b) * * *

(1) * * *

(ii) Denying or interfering in any way, directly or indirectly, with a person's right to be placed on any registry of names and/or telephone numbers of persons who

do not wish to receive outbound telephone calls established to comply with § 310.4(b)(1)(iii)(A), including, but not limited to, harassing any person who makes such a request; hanging up on that person; failing to honor the request; requiring the person to listen to a sales pitch before accepting the request; assessing a charge or fee for honoring the request; requiring a person to call a different number to submit the request; and requiring the person to identify the seller making the call or on whose behalf the call is made;

(iii) * * *

(B) That person's telephone number is on the "do-not-call" registry, maintained by the Commission, of persons who do not wish to receive outbound telephone calls to induce the purchase of goods or services unless the seller or telemarketer:

(i) Can demonstrate that the seller has obtained the express agreement, in writing, of such person to place calls to that person. Such written agreement shall clearly evidence such person's authorization that calls made by or on behalf of a specific party may be placed to that person, and shall include the telephone number to which the calls may be placed and the signature[6] of that person; or

(ii) Can demonstrate that the seller has an established business relationship with such person, and that person has not stated that he or she does not wish to receive outbound telephone calls under paragraph (b)(1)(iii)(A) of this section; or

* * * * *

(3) * * *

[6] For purposes of this Rule, the term "signature" shall include an electronic or digital form of signature, to the extent that such form of signature is recognized as a valid signature under applicable federal law or state contract law.

(vi) Any subsequent call otherwise violating § 310.4(b)(1)(ii) or (iii) is the result of error and not of failure to obtain any information necessary to comply with a request pursuant to § 310.4(b)(1)(iii)(A) not to receive further calls by or on behalf of a seller or charitable organization.

* * * * *

5. Amend § 310.6 by revising paragraphs (b)(5) - (7) to read as follows:

§ 310.6 Exemptions

* * * * *

(b) * * *

(5) Telephone calls initiated by a customer or donor in response to an advertisement through any medium, other than direct mail solicitation, *provided*, however, that this exemption does not apply to:

(i) Calls initiated by a customer or donor in response to an advertisement relating to investment opportunities, debt relief services, business opportunities other than business arrangements covered by the Franchise Rule or Business Opportunity Rule, or advertisements involving offers for goods or services described in §§ 310.3(a)(1)(vi) or 310.4(a)(2)-(4);

(ii) The requirements of §§ 310.4(a)(9) or (10); or

(iii) Any instances of upselling included in such telephone calls;

(6) Telephone calls initiated by a customer or donor in response to a direct mail solicitation, including solicitations via the U.S. Postal Service, facsimile transmission, electronic mail, and other similar methods of delivery in which a solicitation is directed to specific address(es) or person(s), that clearly,

conspicuously, and truthfully discloses all material information listed in § 310.3(a)(1) of this Rule, for any goods or services offered in the direct mail solicitation, and that contains no material misrepresentation regarding any item contained in § 310.3(d) of this Rule for any requested charitable contribution; *provided,* however, that this exemption does not apply to:

(i) Calls initiated by a customer in response to a direct mail solicitation relating to prize promotions, investment opportunities, debt relief services, business opportunities other than business arrangements covered by the Franchise Rule or Business Opportunity Rule, or goods or services described in §§ 310.3(a)(1)(vi) or 310.4(a)(2)-(4);

(ii) The requirements of §§ 310.4(a)(9) or (10); or

(iii) Any instances of upselling included in such telephone calls; and

(7) Telephone calls between a telemarketer and any business to induce the purchase of goods or services or a charitable contribution by the business, except calls to induce the retail sale of nondurable office or cleaning supplies; *provided,* however, that § 310.4(b)(1)(iii)(B) and § 310.5 of this Rule shall not apply to sellers or telemarketers of nondurable office or cleaning supplies.

6. Amend § 310.8 by revising paragraph (c) to read as follows:

§ 310.8 Fee for access to the National Do Not Call Registry

* * * * *

(c) The annual fee, which must be paid by any person prior to obtaining access to the National Do Not Call Registry, is $60 for each area code of data accessed, up to a maximum of $16,482; provided, however, that there shall be no charge to any

person for accessing the first five area codes of data, and provided further, that there shall be no charge to any person engaging in or causing others to engage in outbound telephone calls to consumers and who is accessing area codes of data in the National Do Not Call Registry if the person is permitted to access, but is not required to access, the National Do Not Call Registry under this Rule, 47 CFR 64.1200, or any other Federal regulation or law. No person may participate in any arrangement to share the cost of accessing the National Do Not Call Registry, including any arrangement with any telemarketer or service provider to divide the costs to access the registry among various clients of that telemarketer or service provider.

* * * * *

By direction of the Commission, Commissioner Ohlhausen dissenting.

Donald S. Clark,
Secretary.