FEDERAL TRADE COMMISSION

16 CFR Part 310

RIN 3084–AA98

Telemarketing Sales Rule

AGENCY: Federal Trade Commission.

ACTION: Notice of proposed rulemaking; request for public comment.

SUMMARY: The Federal Trade Commission (''Commission'' or ''FTC'') seeks public comment on proposed amendments to the Telemarketing Sales Rule (''TSR'' or ''Rule''). The proposed amendments would: Bar sellers and telemarketers from accepting remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms as payment in inbound or outbound telemarketing transactions; expand the scope of the advance fee ban on ''recovery'' services, now limited to recovery of losses in prior telemarketing transactions, to include recovery of losses in any previous transaction; and clarify other TSR provisions as discussed at the outset of the **SUPPLEMENTARY INFORMATION** section.

DATES: Written comments must be received by July 29, 2013.

ADDRESSES: Interested parties may file, online or on paper, a comment by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write ''Telemarketing Sales Rule, 16 CFR Part 310, Project No. R411001,'' on your comment, and file your comment online at *https://ftcpublic.commentworks.com/FTC/tsrantifraudnprm* by following the instructions on the web-based form. If you prefer to file your comment on paper, mail or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Room H–113 (Annex B), 600 Pennsylvania Avenue NW., Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Karen S. Hobbs or Craig Tregillus, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW., Washington, DC 20580, (202) 326–3587 or (202) 326–2970.

SUPPLEMENTARY INFORMATION:

I. Introduction

A. The Proposed Amendments

The Federal Trade Commission issues this Notice of Proposed Rulemaking (''NPRM'') to invite public comment on proposed amendments to the TSR. These proposed amendments reflect evolutions in the marketplace toward the use of certain retail payment methods in fraud transactions and the growing expansion of recovery services to include losses incurred in non-telemarketing transactions.

The principal proposed amendments would prohibit telemarketers and sellers in both inbound and outbound telemarketing calls from accepting or requesting remotely created checks, remotely created payment orders, money transfers, and cash reload mechanisms as payment and expand the scope of the advance fee ban on recovery services (now limited to recovery of losses sustained in prior telemarketing transactions) to include recovery of losses in *any* previous transaction.

Several additional proposed amendments are designed to clarify the language of certain existing TSR requirements to reflect Commission enforcement policy. These amendments would: (1) Specify that the recording of a consumer's express verifiable authorization must include a description of the goods or services being purchased; (2) 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; (3) 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; (4) emphasize that the prohibition against sellers sharing the cost of Do Not Call Registry fees, which are non-transferrable, is absolute; and (5) 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. A related amendment would 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) will disqualify it from relying on the safe harbor for isolated or inadvertent violations in section 310.4(b)(3).

This NPRM invites written comments on all issues raised by the proposed amendments, including answers to the specific questions set forth in Section VIII of this Notice.

B. Background

On August 16, 1994, the Telemarketing and Consumer Fraud and Abuse Prevention Act (''Telemarketing Act'' or ''Act'') was signed into law.[1] The purpose of the Act was to curb the deceptive and abusive practices in telemarketing and provide key anti-fraud and privacy protections for consumers receiving telephone solicitations to purchase goods or services. The Telemarketing Act directed the Commission to adopt a rule prohibiting deceptive or abusive practices in telemarketing and specified, among other things, certain acts or practices the rule should address—B for example (1) a requirement that telemarketers may not undertake a pattern of unsolicited telephone calls which the reasonable consumer would consider coercive or abusive of his or her right to privacy; (2) restrictions on the time of day telemarketers may make unsolicited calls to consumers; and (3) a requirement that telemarketers promptly and clearly disclose in all calls to consumers that the purpose of the call is to sell goods or services or solicit a charitable contribution.[2] The Act also generally authorized the Commission to address in the rule other practices it found to be deceptive or abusive.[3]

Pursuant to its authority under the Telemarketing Act, the FTC promulgated the TSR on August 16, 1995.[4] The Commission subsequently amended the Rule on three occasions, in 2003,[5] 2008,[6] and 2010.[7] In 2010, the Commission also issued an Advanced Notice of Proposed Rulemaking concerning caller identification (''Caller ID'') services and disclosure of the

[1] 15 U.S.C. 6101–6108.

[2] 15 U.S.C. 6102(a)(3).

[3] 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.''). The Telemarketing Act directs the Commission to include in the TSR provisions that address three specific practices denominated by Congress as ''abusive.'' *Id.* at 6102(a)(3). However, the Act ''does not limit the Commission's authority to address abusive practices beyond these three practices legislatively determined to be abusive.'' *See* Notice of Proposed Rulemaking (''2002 Notice of Proposed Rulemaking''), 67 FR 4492, 4510 (Jan. 30, 2002).

[4] Statement of Basis and Purpose and Final Rule (''Original TSR''), 60 FR 43842 (Aug. 23, 1995). The effective date of the original Rule was December 31, 1995.

[5] *See* Statement of Basis and Purpose and Final Amended Rule (''2003 TSR Amendments''), 68 FR 4580 (Jan. 29, 2003).

[6] *See* Statement of Basis and Purpose and Final Rule Amendments (''2008 TSR Amendments''), 73 FR 51164 (Aug. 29, 2008).

[7] *See* Statement of Basis and Purpose and Final Rule Amendments (''2010 TSR Amendments''), 75 FR 48458 (Aug. 10, 2010). The Commission subsequently published correcting amendments to the text of section 310.4 the TSR. Telemarketing Sales Rule; Correcting Amendments, 76 FR 58716 (Sept. 22, 2011).

identity of the seller or telemarketer responsible for telemarketing calls.[8]

The Telemarketing Act authorizes the Commission to promulgate rules ''prohibiting deceptive telemarketing acts or practices and other abusive telemarketing acts or practices.'' [9] Section 310.3 of the TSR targets deceptive telemarketing acts or practices. It contains provisions requiring certain disclosures during telemarketing calls,[10] prohibiting specific material misrepresentations,[11] and imposing liability on third parties that provide substantial assistance to telemarketers that violate the Rule.[12] Section 310.4 of the TSR focuses on abusive telemarketing acts or practices. It includes provisions intended to curb the deleterious effects these acts or practices may have on consumers. This section of the Rule delineates five categories of abusive conduct: (1) Conduct related to a pattern of calls, including conduct prohibited under the Rule's Do Not Call provisions; [13] (2) violations of the Rule's calling time restrictions; [14] (3) failure to make required oral disclosures in the sale of goods or services; [15] (4) failure to make required oral disclosures in charitable solicitations; [16] and (5) other abusive telemarketing acts or practices.[17]

In interpreting its rulemaking authority over ''other abusive telemarketing acts or practices,'' [18] the Commission has determined that its authority includes acts or practices ''within the purview of its traditional unfairness analysis as developed in Commission jurisprudence.'' [19] Thus, the Commission employs its unfairness analysis when identifying a telemarketing practice as abusive.[20] An act or practice is unfair under Section 5 of the FTC Act if it causes or is likely to cause substantial injury to consumers, if the harm is not outweighed by any countervailing benefits to consumers or competition, and if the harm is not reasonably avoidable.[21]

II. Retail Payment Methods Susceptible to Fraud in Telemarketing

The following section of this Notice explores the features and vulnerabilities of four types of novel payment methods used in telemarketing, with a particular focus on the use of a consumer's bank account and routing number to withdraw funds from the account without authorization.[22] Noncash retail payment mechanisms used in telemarketing can be divided into two major categories: ''Conventional payment methods'' and ''novel payment methods.'' As used in this Notice, the term ''conventional payment method'' includes credit cards, debit cards, and other types of electronic fund transfers, which are processed or cleared electronically through networks that can be monitored systematically for fraud.[23] In addition, federal laws subject such conventional payments to procedures for resolving errors and statutory limitations on a consumer's liability for certain disputed transactions.[24]

As used in this Notice, the term ''novel payment method'' refers to four types of noncash payments—remotely created checks,[25] remotely created payment orders,[26] ''cash-to-cash money transfers,'' [27] and ''cash reload mechanisms.'' [28] These novel payment methods differ significantly from credit card transactions subject to the Truth-in-Lending Act (''TILA'') and Regulation Z, as well as from debit card transactions, Automated Clearinghouse (''ACH'') debits from consumer bank

[8] Advanced Notice of Proposed Rulemaking, 75 FR 78179 (Dec. 15, 2010).

[9] *Supra* note 3.

[10] The TSR requires that telemarketers soliciting sales of goods or services promptly disclose several key pieces of information during a telephone call: (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 310.3(a)(1). In addition, telemarketers must, in any telephone sales call, disclose the total costs and material restrictions on the purchase of any goods or services that are the subject of the sales offer. 16 CFR 310.3(a)(1). In telemarketing calls soliciting charitable contributions, the Rule requires prompt disclosure of the identity of the charitable organization on behalf of which the request is being made and that the purpose of the call is to solicit a charitable contribution. 16 CFR 310.3(d).

[11] 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 a false or misleading statement to induce any person to pay for goods or services or to induce a charitable contribution. 16 CFR 310.3(a)(4).

[12] The TSR prohibits any person from providing substantial assistance or support to a seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any act or practice that violates sections 310.3(a), (c) or (d), or section 310.4 of the Rule. 16 CFR 310.3(b).

[13] 16 CFR 310.4(b).

[14] 16 CFR 310.4(c).

[15] 16 CFR 310.4(d).

[16] 16 CFR 310.4(e).

[17] 16 CFR 310.4(a) (prohibiting the use of threats, intimidation, or profane or obscene language; requesting or receiving an advance fee for credit repair, debt settlement, and recovery services or for the arrangement of a loan or other extension of credit when the telemarketer guarantees or represents a high likelihood of success; disclosing or receiving, for consideration, unencrypted consumer account numbers for use in telemarketing; causing billing information to be submitted for payment, directly or indirectly, without the express informed consent of the customer or donor; and failure to transmit Caller ID information).

[18] *Supra* note 3.

[19] 2002 Notice of Proposed Rulemaking, 67 FR at 4511.

[20] 2010 TSR Amendments, 75 FR at 48469 (discussing the Commission's use of unfairness standard in determining whether a practice is ''abusive''); *see also* 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)) (''Unfairness Policy Statement'').

[21] 15 U.S.C. 45(n).

[22] In addition to the payment methods discussed below, the Commission recognizes that there are additional noncash payment alternatives used in telemarketing transactions, including the use of billing and collection systems of mortgage, telephone, mobile phone, or utility companies and online payment intermediaries. These particular payments are not the subject of this NPRM, which focuses on payment alternatives that offer fraudulent telemarketers the most accessible and anonymous method of extracting money from consumers and for which the Commission has a record of fraud. However, the Commission continues to monitor complaints regarding the use of other billing platforms and payment methods in telemarketing fraud.

[23] Credit card transactions are processed through the credit card payment systems, operated by companies such as American Express, MasterCard, and Visa. Many debit card transactions are processed through the payment card systems, such as those operated by MasterCard and Visa. In addition, some debit card transactions, and other types of electronic fund transfers, may be cleared by the Automated Clearinghouse (''ACH'') Network, a nationwide, interbank electronic clearing house for processing and clearing electronic payments for participating financial institutions. *See infra* note 50 (describing other types of electronic fund transfers that are processed as ACH debits). ACH transactions are governed by operating rules implemented and enforced by NACHA—The Electronic Payments Association (''NACHA''), a private, self-regulatory trade association comprised of financial institutions and regional payment associations. There are two ACH operators: the Federal Reserve Bank (''FedACH'') and The Electronic Payments Network (''EPN''), the only remaining private sector operator. Terri Bradford, *The Evolution of the ACH,* Payment System Research Briefing, Federal Reserve Bank of Kansas (Dec. 2007), *available at http://www.kansascityfed.org/PUBLICAT/PSR/Briefings/PSR-BriefingDec07.pdf.*

[24] Credit card transactions are subject to the Truth-in-Lending Act (''TILA''), 15 U.S.C. 1601 *et seq.,* and Regulation Z, 12 CFR part 1026. Debit card transactions, ACH debits, and other types of electronic fund transfers involving a consumer's account at a financial institution are governed by the Electronic Fund Transfer Act (''EFTA''), 15 U.S.C. 1693 *et seq.,* and Regulation E, 12 CFR 1005.

[25] *See infra* note 35 (definition of remotely created check).

[26] *See infra* note 39 (definition of remotely created payment order).

[27] *See infra* note 122 and Section IV.A (discussing the proposed definition of cash-to-cash money transfer, which includes the electronic transfer of cash from one person to another person in a different location that is conducted through a money transfer provider and is received in cash).

[28] *See infra* Section II.B (discussing the function of a cash reload mechanism, which acts as a virtual deposit slip that a person uses to convert cash into electronic format that can be added to any existing prepaid card within the same prepaid network).

accounts, and other electronic fund transfers subject to the Electronic Fund Transfer Act (''EFTA'') and Regulation E. Unlike these conventional payment methods, novel payment methods are cleared via check clearing and money transfer networks that provide little or no systematic monitoring to detect or deter fraud. Moreover, these novel payment methods are governed principally by state laws and remittance transfer regulations that do not provide consumers with adequate recourse when unauthorized transactions or telemarketing fraud occurs.[29]

The Commission proposes amending the Rule to prohibit the use of these novel payment methods—remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms—in *all* telemarketing transactions.[30] The Commission is concerned that the TSR's provision requiring ''express verifiable authorization'' for such novel payment methods,[31] which was added to the Rule during the amendment proceeding completed in 2003, has not adequately protected consumers against fraud.[32] The Commission's continuing law enforcement experience has demonstrated that, despite the requirement of express verifiable authorization when accepting a remotely created check as payment for a telemarketing purchase, unscrupulous telemarketers have increasingly exploited remotely created checks to extract or attempt to extract hundreds of millions of dollars from defrauded consumers.[33] Fraudulent telemarketers also rely on other novel payment methods—such as remotely created payment orders, cash-to cash money transfers, and cash reload mechanisms—in their telemarketing schemes. Therefore, the Commission proposes changes to the Rule that would prohibit the use of these novel payment methods in inbound and outbound telemarketing transactions.

A. Remotely Created Checks and Remotely Created Payment Orders

Checks are written orders used to instruct a financial institution to pay money from the account of the check writer (''payor'') to the check recipient (''payee''). Traditional checks have certain requirements as to the type of paper and ink used, and what information appears on the check. Traditional checks also require the signature of the authorized signatory on the checking account, which must be verified by the bank.[34] By contrast, a remotely created check is an unsigned paper check that is created by the payee (typically a merchant, seller, or telemarketer).[35] In place of the payor's signature, the remotely created check bears a statement indicating that the account holder authorized the check or that the ''signature is on file.'' [36] Any merchant who obtains a consumer's bank routing and account number can print a remotely created check with the proper equipment or the help of a third-party payment processor, and deposit it into its bank account for collection.[37] Thus, remotely created checks are more susceptible to fraud than paper checks.

Changes in banking regulations and advances in technology now enable banks to accept and exchange electronic images of paper checks, including ''substitute checks,'' instead of sorting and transporting paper checks around the country on a daily basis.[38] As a result, telemarketers, sellers, and payment processors can deposit

---

[29] *See infra* note 54 and accompanying text (discussing the Uniform Commercial Code applicable to checks and remotely created checks); notes 129 through 134 (discussing final Remittance Transfer Rule aimed at insuring the transparency and accuracy of cross-border remittance transfers, issued by the Consumer Financial Protection Bureau (''CFPB'') in 2012).

[30] *See infra* Section IV.E (discussing proposed amendments to the general media and direct mail exemptions in sections 310.6(b)(5) and (6)).

[31] 16 CFR 310.3(a)(3). In 2003, the Commission explained that requiring express verifiable consent was necessary ''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.'' 2003 TSR Amendments, 68 FR at 4606. Thus, section 310.3(a)(3) of the TSR requires telemarketers and sellers to obtain a consumer's express verifiable authorization for all telemarketing transactions where payment is made by a method other than a credit card or a debit card. 16 CFR 310.3(a)(3). This includes ACH debits and other forms of electronic fund transfers subject to the EFTA, as well as payment methods that are not subject to the EFTA.

[32] Other law enforcers and regulators have expressed concerns about the fraudulent use of remotely created checks. *See, e.g.,* NACHA Discussion Paper, *Warranty Claims on Demand Drafts Through the ACH Network* (May 1, 2008) (noting that law enforcement and consumer protection agencies continue to alert NACHA about the fraudulent use of remotely created checks, and confirming that, ''[a]s the electronic payments networks have implemented risk management and anti-fraud programs, it appears that some fraudulent activity has migrated to this form of payment''), *available at http://www.nacha.org/c/AccomplishmentsandCurrentInitiatives.cfm;* 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) (advocating the elimination of remotely created checks in favor of electronic fund transfers covered by the EFTA); Federal Reserve Bank of Atlanta, *2008 Risk & Fraud in Retail Payments: Detection & Mitigation Conference Summary* (Oct. 6–7, 2008) (''Anecdotally, telemarketers turned to remotely created checks as better ACH risk controls came online.''), *available at http://www.frbatlanta.org/filelegacydocs/08retailpayments.pdf.*

[33] *See infra* notes 91–99 (citing injury estimates in cases brought by the Commission).

[34] Because payment for goods or services sold through telemarketing occurs immediately over the telephone, traditional paper checks are not commonly used in telemarketing transactions. Nevertheless, in most circumstances, a consumer's written signature on a check would satisfy the express verifiable authorization requirement of section 310.3(a)(3)(i) of the TSR.

[35] A remotely created check, also commonly referred to as a ''demand draft,'' ''bank check,'' or ''bank draft,'' is defined by Regulation CC (Availability of Funds and Collection of Checks), 12 CFR 229.2(fff), as ''a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn.'' Thus, checks generated by an account holder's bank on the request of the account holder through the bank's bill pay service are not remotely created checks, despite the absence of the account holder's signature.

[36] ''As a result, they are vulnerable to misuse by fraudsters who can, for example, use [a remotely created check] to debit a victim's account without receiving proper authorization or delivering the goods or services. The risk of fraudulent [remotely created checks] is amplified in one-time purchase scenarios where the merchant is relatively unknown to the customer.'' Crystal D. Carroll, Federal Reserve Bank of Atlanta, Retail Payments Risk Forum, *Remotely Created Checks: Distinguishing the Good from the Bad* (July 6, 2009), *available at http://portalsandrails.frbatlanta.org/2009/07/remotely-created-checks-distinguishing-the-good-from-the-bad.html.*

[37] To comply with processing standards at banks that use magnetic ink character recognition line data from the bottom of a check, remotely created checks must be printed using special check paper stock and magnetic ink. Telemarketers often employ third-party processing firms to create and deposit the checks, which are accepted for deposit by the firms' bank. *See, e.g., FTC* v. *Your Money Access, LLC* (*''YMA''*), Civ. No. 07–5147 (E.D. Pa. Aug. 11, 2010) (stipulated permanent injunction against payment processor that allegedly facilitated fraudulent telemarketers by debiting accounts through remotely created checks and ACH debits); *United States* v. *Payment Processing Ctr., LLC,* Civ. No. 06–0725 (E.D. Pa. Aug. 12, 2010) (Stip. Perm. Inj.) (same); *FTC* v. *Interbill, Ltd.,* Civ. No. 2:06–01644 (D. Nev. Apr. 30, 2009) (Summ. J.), *aff'd, FTC* v. *Wells,* Civ. No. 09–16179, 385 F.App'x. 712 (9th Cir. 2010) (summary judgment against payment processor that facilitated fraudulent telemarketers by debiting accounts through remotely created checks).

[38] In 2003, Congress enacted the Check Clearing for the 21st Century Act (''Check 21 Act'' or ''Check 21''), 12 U.S.C. 5001–5018, which paved the way for the use of substitute checks. Under the Act, a substitute check qualifies as the legal equivalent of the original check if:

(1) it accurately represents all of the information on the front and back of the original check as of the time it was truncated [*i.e.,* removed from the collection or return process and supplanted by an electronic image of the check] * * * (2) it bears the legend: ''This is a legal copy of your check. You can use it the same way you would use the original check,'' and (3) a bank has made the Check 21 Act warranties with respect to the substitute check.

Federal Financial Institutions Examination Council (''FFIEC''), *Check Clearing for the 21st Century Act Foundation for Check 21 Compliance Training, available at http://www.ffiec.gov/exam/check21/Check21FoundationDoc.htm.*

scanned images of paper-based checks, including remotely created checks, into the check clearing system.

Electronic image exchange also has resulted in an ''all-electronic'' version of the remotely created check—the ''remotely created payment order''—a remotely created check that *never* exists in printed paper form.[39] Like traditional checks and remotely created checks, remotely created payment orders are deposited into and cleared through the check clearing system.[40] As with remotely created checks, remotely created payment orders are created by the merchant (payee), not the consumer (payor). In the case of remotely created payment orders, a telemarketer or seller simply enters a bank account number and bank routing number into an electronic file that is transmitted to a financial institution for processing via the check clearing system.[41] As a result, remotely created payment orders are at least as susceptible to fraud as remotely created checks.[42]

The Commission previously considered the risks associated with the use of remotely created checks (then known as ''demand drafts'') in telemarketing during the initial promulgation of the Rule and subsequent rulemaking proceedings culminating in the 2003 amendments. At the time of those prior rulemaking proceedings, there were few, if any, convenient and safe payment alternatives available for consumers without access to credit cards. Consequently, prohibiting the use of remotely created checks in telemarketing would have imposed hardships on those consumers.[43] In the past decade, however, there has been a dramatic proliferation of noncash payment alternatives for consumers, and electronic payments now surpass paper checks in popularity as noncash means of payment.[44] In light of these changes in the marketplace, the Commission preliminarily finds that the risks from using these payment methods in telemarketing transactions exceed the benefits of permitting their use. At the same time, the Commission wishes to explore whether there might be legitimate reasons that telemarketers use these payment methods instead of other available payment mechanisms.[45] To understand any potential problems posed for legitimate businesses by the proposed ban on the use of remotely created checks and remotely created payment orders, the Commission welcomes comments from the public in response to the questions posed in Section VIII.

1. Absence of Federal Consumer Protection Regulation of Remotely Created Checks and Remotely Created Payment Orders

A complicated interplay between federal and state laws results in uneven regulation of different payment methods. The type of payment mechanism used by a consumer in a particular transaction determines the level of legal protection against unauthorized charges the consumer receives. Consumers generally are not aware of the differing legal protections pertaining to the various payment methods. Significantly, consumers who provide bank debiting information to a telemarketer have virtually no control over how the telemarketer chooses to process their payment. Once a telemarketer obtains a consumer's bank account and routing number, the telemarketer (not the consumer) may choose to use that information to initiate payment via ACH debit, remotely created check, or remotely created payment order[46]—a choice that determines what level of protections the consumer receives.

When a remotely created check or a remotely created payment order is cleared through the check clearing system, consumers receive none of the federal protections that safeguard conventional payments that are processed through the credit card system or the ACH Network. Consider the protections the law affords to credit card transactions and electronic fund transfers, such as debit card and ACH transactions. Federal law subjects credit card transactions to a prescribed billing error resolution process[47] and statutory limitations on a cardholder's liability for certain transactions.[48] Similarly, when

[39] The proposed definition of ''remotely created payment order,'' therefore, closely tracks the proposed definition of remotely created check:

a payment instruction or order drawn on a person's account that is initiated or created by the payee and that does not bear a signature applied, or purported to be applied, by the person on whose account the order is drawn, and which is cleared through the check clearing system. The term does not include payment orders cleared through the Automated Clearinghouse Network or subject to the Truth in Lending Act, 15 U.S.C. 1601, and Regulation Z, 12 CFR part 1026.

See infra Section IV.A.

[40] In 2011, while proposing certain amendments to Regulation CC (Availability of Funds and Collection of Checks), the Board of Governors of the Federal Reserve System (''Federal Reserve Board'') used the term ''electronically-created item'' to describe any all-electronic image of a check that is sent through the check clearing system. *Proposed Rule; Regulation CC,* 76 FR 16862, 16865 (Mar. 25, 2011), *available at http://www.gpo.gov/fdsys/pkg/FR-2011-03-25/pdf/2011-5449.pdf.* As such, the term encompasses ''remotely created payment orders'' (also known as ''electronic RCCs,'' ''virtual drafts,'' ''paperless checks,'' and ''non-check RCCs''), as well as smart-phone checks where the consumer ''signs'' a digital image of a check that can be emailed to a merchant or the merchant's bank. *Id.* Among other things, the Federal Reserve Board proposed amendments to Regulation CC that would provide such electronically-created items with the same interbank warranty and liability provisions as remotely created checks. *Id. See also supra* note 53 (explaining interbank warranty and liability provisions applicable to remotely created checks). To date, the Board has taken no further action on this proposal.

The Commission's proposed ban would extend to remotely created payment orders. Importantly, the ban would not prohibit the use of other ''electronically-created items,'' as defined by the Federal Reserve Board's proposed amendments to Regulation CC.

[41] FFIEC, *Retail Payment Systems Booklet—February 2010,* at 16 (Feb. 2010) (''*Retail Payment Systems Booklet* ''), *available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_RetailPaymentSystems.pdf.* ''Unlike traditional checks or RCCs [remotely created checks], electronically created payment orders do not begin with a paper item. However, they are similar to RCCs in that they . . . bear no direct evidence of the customer's authorization. Because these transactions are not originally captured from paper check items, the laws and regulations pertaining to check collection do not apply.'' *Id.; see also infra* notes 61–62 and accompanying text (noting the uncertain regulatory framework for remotely created payment orders deposited into the check clearing system).

[42] In inbound telemarketing calls, the same account information could be used to initiate an electronic fund transfer through the ACH Network. Fraudulent telemarketers and unscrupulous payment processors prefer, however, to use remotely created payment orders to evade the ACH Network and exploit the weaknesses inherent in the check clearing system. *See, e.g., FTC* v. *Automated Electronic Checking, Inc. (''AEC''),* Civ. No. 3:13–cv–00056–RCJ–WGC (D. Nev. Feb. 5, 2013) (Stip. Perm. Inj.); *FTC* v. *Landmark Clearing Inc.,* Civ. No. 4:11–00826 (E.D. Tex. Dec. 15, 2011) (Stip. Perm. Inj.).

[43] Original TSR, 60 FR at 43850.

[44] Federal Reserve System, *The 2010 Federal Reserve Payments Study: Noncash Payment Trends in the United States: 2006–2009,* at 4 (April 5, 2011) (''*2010 Payments Study*'') (''Electronic payments (those made with cards and by ACH) now collectively exceed three quarters of all noncash payments while payments by check are now less than one-quarter. The increase in electronic payments and the decline of checks can be attributed to technological and financial innovations that influenced the payment instrument choices of consumers and businesses.'' (Citation omitted)), *available at http://www.frbservices.org/files/communications/pdf/press/2010_payments_study.pdf.*

[45] The 2010 Federal Reserve Payments Study concluded that ''[t]he decline in [consumer-to-business] check writing reflects, among other things, the replacement of consumer checks by electronic payments, such as online bill payments through the ACH, or point-of-sale purchases with debit cards.'' *Id.* at 11.

[46] *Cf. supra* note 42.

[47] Fair Credit Billing Act, 15 U.S.C. 1666 (correction of billing errors). Within 60 days of the financial institution's transmittal of her credit card account statement, a consumer may dispute a charge for goods or services with her credit card company, and withhold payment while the dispute is pending. Billing errors include failure of a merchant to deliver goods or services as agreed.

[48] Truth-In-Lending Act, 15 U.S.C. 1643 (liability of holder of credit card); Regulation Z, 12 CFR 1026.12(b)(2) (liability of cardholder for unauthorized use).

consumers use debit cards linked to a bank account or otherwise initiate electronic fund transfers involving a bank account, they are protected by the EFTA.[49] This is also true when consumers provide paper checks to a merchant that converts the account information from these checks into electronic ACH debits.[50] The EFTA and Regulation E provide consumers with error resolution procedures, including a requirement that funds debited in an unauthorized electronic fund transaction must be returned to the consumer's account within a maximum of ten business days, pending the outcome of further investigation,[51] and statutory limitations on a consumer's liability for unauthorized transactions.[52]

In contrast, no such federal consumer protection laws or regulations apply to remotely created checks deposited into the check clearing system.[53] These payments are governed principally by state law, Articles 3 and 4 of the Uniform Commercial Code (''UCC''), which apply to all negotiable instruments and bank deposits.[54] Unlike the dispute resolution protections provided by the TILA and Regulation Z, the UCC provides no way for a consumer to dispute or withhold payment before the funds are withdrawn from her account.[55] In addition, consumers receive superior substantive liability limits for unauthorized transactions under the TILA and, to a lesser extent, the EFTA.[56] Moreover, unlike the EFTA and Regulation E, the UCC imposes no specific obligation on a financial institution to recredit disputed funds to a consumer's account within a particular time frame,[57] and a consumer may have to pursue legal action against the bank to promptly recover money lost in telemarketing fraud.[58] Thus, consumers victimized by telemarketing schemes that deposit unauthorized remotely created checks are forced to expend a significant amount of time, effort and money to resolve disputes with their banks over unauthorized withdrawals from their accounts.[59]

The regulatory framework for remotely created payment orders is complicated and unsettled, but currently results in the same inferior protection against fraud as provided by remotely created checks. Unlike traditional checks or remotely created checks, remotely created payment orders never exist in paper form and, thus, cannot be used to create a substitute check that meets the requirements of the Check Clearing for the 21st Century Act (''Check 21 Act'').[60] The Consumer Financial

[49] The EFTA also covers payroll cards, and some prepaid debit cards (also referred to as ''general purpose reloadable'' or ''GPR'' cards) that are linked to an account at a financial institution. In addition, section 401 of the Credit Card Accountability Responsibility and Disclosure Act of 2009 (''Credit CARD Act''), 15 U.S.C. 1693l–1, created new section 915 of the EFTA, subjecting other types of non-GPR cards (*i.e.,* gift cards) to some, but not all, requirements of the EFTA.

In May 2012, the CFPB requested public comment on whether (and to what extent) EFTA coverage should be provided to all GPR cards. Advanced Notice of Proposed Rulemaking; Electronic Fund Transfers (Regulation E) and General Purpose Reloadable Prepaid Cards (''ANPR Electronic Fund Transfers and GPR Cards''), 77 FR 30923 (May 24, 2012). In a comment submitted the CFPB, Commission staff expressed support for protecting users of GPR cards and for the CFPB's proposal to solicit information about the costs and benefits of extending additional protections to these cards. Comment, Staff of the Bureau of Consumer Protection, ANPR Electronic Fund Transfers and GPR Cards, Dkt. No. CFPB–2012–00196 (July 23, 2012), *available at http://www.ftc.gov/os/2012/07/120730cfpbstaffcomment.pdf.* The Commission will continue to monitor complaints regarding the use of prepaid debit cards in telemarketing fraud to determine whether additional amendments of the TSR would protect consumers.

[50] Examples of such electronic check conversions include point-of-purchase (''POP'') and accounts receivable conversion (''ARC''). A POP entry is created for an in-person purchase of goods or services when a retailer uses a consumer's paper check as a source document to electronically enter the consumer's bank routing and account number to initiate an ACH debit to the consumer's bank account. An ARC entry also uses a consumer's paper check as a source document to initiate an ACH debit, but the check is not received at the point-of-purchase. Instead, ''a biller receives the consumer's check in the mail, or at a lockbox location for payment of goods and services.'' Karen Furst & Daniel E. Nolle, Policy Analysis Division, Office of the Comptroller of the Currency, *ACH Payments: Changing Users and Changing Uses Policy Analysis Paper #6,* at 8 (Oct. 2005), *available* at *http://www.occ.gov/topics/bank-operations/bit/ach-policy-paper-6.pdf.* ''Under a legal sleight of hand, the check is treated as an authorization for an electronic fund transfer, bringing the transaction entirely under the EFTA.'' Gail Hillebrand, *Before the Grand Rethinking: Five Things to Do Today with Payments Law and Ten Principles to Guide New Payments Products and New Payments Law,* 83 Chi.-Kent L. Rev. 769, 780 n.22 (2008).

[51] 15 U.S.C. 1693f(c) (provisional recredit of consumer's account). When a consumer disputes an electronic funds transfer as unauthorized or otherwise in error, the EFTA provides a process for error resolution. *Id.* at 1693f. The consumer must notify the financial institution, either orally or in writing, of the reasons for the error or dispute within 60 days of transmittal of an account statement bearing the disputed transaction. The EFTA gives the financial institution up to ten business days to either resolve the dispute or provide the consumer with a provisional recredit of the disputed amount. The financial institution may take up to 45 days to complete its investigation. If the dispute is resolved in the consumer's favor before the end of the ten day period, however, the recredit must be made within one business day. These time periods can be extended under certain circumstances. *Id.*

[52] Under the EFTA, consumers are not liable for unauthorized electronic fund transfers unless an accepted card or other means of access was used—*i.e.,* a card which had been received by the consumer. 15 U.S.C. 1693g(a). If an accepted card was used, and the card provides for a means to identify the user of the card, the EFTA allows the consumer to be held responsible for certain amounts, depending on the timeliness of the consumer's discovery and report of loss, theft, or unauthorized use. If the consumer reports the loss not later than two business days of discovery of the loss, a consumer's liability is limited to $50. *Id.* at 1693g(a)(1)–(2). If not, a consumer's liability can go up to $500. If the consumer fails to report an unauthorized fund transfer that appears on a statement provided to the consumer within 60 days, however, the consumer's potential loss is unlimited. *Id.*

[53] Remotely created checks are subject to Regulation CC, 12 CFR 229.34, which provides for special transfer and presentment warranties between banks. These interbank warranties ''shift liability for the loss created by an unauthorized remotely created check to the depositary bank,'' which is generally the bank for the person that initially created and deposited the remotely created check. *Final Rule; Regulations J and CC,* 70 FR 71218, 71220 (Nov. 5, 2005). ''The warranty applies only to financial institutions and does not directly create any new rights for checking account customers.'' FFIEC, *Retail Payment Systems Booklet, supra* note 41, at 9.

[54] The UCC has been adopted (in whole or in part), with some local variation, in all 50 states, the District of Columbia, and the Virgin Islands.

[55] *See supra* note 47; Hillebrand, *supra* note 50 at 776 (explaining the limited consumer protections afforded by the UCC for many consumer check disputes); Mark E. Budnitz, Lauren K. Saunders, & Margot Saunders, § 2.3.2.3 Consumer Banking and Payments Law: Credit, Debit & Stored Value Cards, Checks, Money Orders, E-Sign, Electronic Banking and Benefit Payments (4th ed., National Consumer Law Center 2009 & Supp. 2010).

[56] *See supra* notes 47–48 and 51–52.

[57] ''Thus, only weak and indirect motivations force banks to move promptly in response to such a complaint. For example, the bank that responds slowly to such a complaint might harm its reputation for providing high-quality customer service. Similarly, if the bank refuses to return the funds promptly and subsequently dishonors a check for which the customer's funds should have been adequate, the bank would be exposed to liability for wrongful dishonor. It is safe to say that those motivations are much less effective than the specific statutory deadlines for dealing with customer complaints that appear in the EFTA.'' Expert Report of Prof. Ronald Mann, ¶ 24 (Feb. 4, 2008), *filed in FTC* v. *Neovi, Inc.* (''*Neovi*''), Civ. No. 06–1952 (S.D. Cal. Sept. 16, 2008) (Summ. J.).

[58] Hillebrand, *supra* note 50, at 780 (explaining that ''check law sets no guaranteed time period for the re-credit of disputed funds'').

[59] Mann, *supra* note 57, ¶ 25 (''As a result, a typical consumer will expend a considerable amount of time getting the bank to respond to the complaint. Among other things, the consumer ordinarily will be required to submit an affidavit regarding the forgery. For consumers that are not experienced with the legal system, and who have immediate uses to which they would put the funds in their bank accounts, these problems are likely to be most burdensome.''); *see also* Expert Report of Elliott C. McEntee, at ¶ 55 (Oct. 1, 2008), *filed in YMA, supra* note 37.

[60] Budnitz & Saunders, *supra* note 55, at § 2.6.3.5; NACHA, *Remotely Created Checks and ACH Transactions: Analyzing the Differentiators* (*''RCC and ACH Differentiators''*), at 6 (Mar. 2010), *available at http://www.macha.org/Portals/0/RCC%20White%20Paper%20031110%20Final.pdf* (''[Remotely created payment orders] that are not originally captured via a paper document cause greater risk than RCCs because they are even more difficult to identify and monitor and because their legal framework is not clearly defined.''); Richard Oliver & Ana Cavazos-Wright, Federal Reserve Bank of Atlanta, Retail Payments Risk Forum, Portals and

Protection Bureau (''CFPB'') has not yet determined whether such electronically-created items not derived from checks are electronic fund transfers subject to Regulation E.[61] Notwithstanding this uncertain regulatory framework, as a practical matter, the check clearing system cannot currently distinguish remotely created payment orders from remotely created checks (or from images of traditional checks).[62] Banks, therefore, often treat returned remotely created payment orders as if they were remotely created checks covered by the UCC, which, as previously noted, provides consumers with no meaningful protection against telemarketing fraud.

Some payment processors capitalize on this confusing regulatory framework when marketing their remotely created payment order services to high-risk merchants. These entities openly promote the ''merchant-friendly'' UCC framework and avoidance of NACHA's Operating Rules, including NACHA's 1 percent monthly threshold for unauthorized returns, as reasons to use remotely created checks and remotely created payment orders instead of credit card or ACH payments.[63]

2. Lack of Centralized Fraud Monitoring and Controls

Unlike payments processed or cleared through the credit card system or the ACH Network, remotely created checks are not subject to systematic monitoring for fraud. This makes them an irresistible payment method for fraudulent telemarketers. The credit card system is designed to deter and detect fraud by requiring that a merchant be approved for a merchant account before it may accept credit card payments. In addition, the credit card system monitors all returns and refunds, to identify unusual activity associated with fraud. Specifically, the credit card payment system can analyze the chargeback volume (*i.e.* the number of chargebacks over a particular time period), chargeback rate (*i.e.,* the percentage of attempted debits that are returned out of the total number of attempted debits for a specific merchant), and chargeback reason codes (via a numeric code used to identify why a chargeback occurred) of its participants.[64] To participate in the credit card payment systems, banks and merchants agree to abide by certain operating rules, including requirements that chargeback rates remain below established thresholds,[65] and they can be expelled or otherwise sanctioned for violating these rules.[66]

Similarly, the two ACH operators (the Federal Reserve Bank and the Electronic Payments Network) systematically monitor transactions to detect and deter fraud. The ACH operators track the volume, reason code, and rate of ''returned items'' [67] sent back to originating banks where the items were originally deposited, and forward the data to NACHA—The Electronic Payments Association (''NACHA'').[68] When NACHA identifies a merchant with unusually high returns activity, it notifies the merchant's originating bank which must review the merchant's activity and compliance with the NACHA rules.[69] NACHA's rules and guidelines emphasize the responsibility of all ACH participants, including merchants, banks, and payment processors, to monitor return rates and other suspicious activity in order to detect and prevent fraud in the ACH Network. ACH participants can determine whether a merchant's return rates are excessive by comparing the merchant's return rate with the industry average return rates, which NACHA publishes in quarterly NACHA

Rails, *Going All Digital With the Check: Check 21, ACH, or an Electronic Payment Order?* (May 10, 2010), *available at http://portalsandrails.frbatlanta.org/remotely-created-checks/.*

[61] In 2011, while proposing certain amendments to Regulation CC (Availability of Funds and Collection of Checks), the Federal Reserve Board stated that it had not made a determination as to the applicability of Regulation E to electronically-created items, such as remotely created payment orders. *Proposed Rule; Regulation CC, supra* note 40 at 16865–86. Since then, the CFBP has assumed responsibility for most rulemaking authority for Regulation E, pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act (''Dodd-Frank Act''), Pub. L. 111–203, 124 Stat. 1376 (2010). The CFPB also has not made such a determination.

[62] *Proposed Rule; Regulation CC, supra* note 40, at 16866; *see also* Ana Cavazos-Wright, Federal Reserve Bank of Atlanta, Retail Payments Risk Forum, *Remotely Created Checks: Banks of First Deposit Provide Front Line of Defense* (June 7, 2010), *available at http://portalsandrails.frbatlanta.org/remotely-created-checks/.* (''RCCs that exist in [electronic-only] format may easily bypass detection because, when they are sent forward for clearing, they appear in a format indistinguishable from files of images captured from paper checks.'').

Moreover, in explaining amendments to the Federal Reserve Operating Circular 3, the Retail Payments Office of the Federal Reserve System advised depository institutions that these items ''actually fall under the requirements of the EFTA and Reg E.'' Letter from Richard Oliver, Retail Payments Product Manager, Retail Payments Office of the Federal Reserve to Chief Executive Officers of Depository Institutions (June 16, 2008); *see also* Federal Reserve Bank of New York, *Operating Circular No. 3 Revised, Circular 11962* (June 23, 2008), *available at http://www.newyorkfed.org/banking/circulars/11962.html.*

[63] For example, the defendants in *AEC* urged their merchant clients to avoid NACHA's 1 percent monthly threshold on unauthorized returns by switching from ACH debits to RCPOs. *FTC* v. *AEC, supra* note 42, at ¶29.

Similarly, the defendants in *Landmark* expressly advertised their remotely created payment order processing product as a less regulated alternative to ACH transactions. *FTC* v. *Landmark Clearing, supra* note 42, at ¶23. The defendants declared on their Web site and promotional materials that:

NACHA, the governing body over check processing rules and regulations, has stated businesses with return rates of higher than 1% unauthorized return rate cannot process ACH transactions. If your company is at risk of higher return rates, [RCPO] processing is a great solution for your business needs.

Id. at Exhibit A, *Screen Capture of Landmark Web site, Virtual Draft page.*

[64] A ''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 her account. This dispute process is governed by the Fair Credit Billing Act, TILA and Regulation Z. *See supra* notes 47 and 48.

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

Visa monitors the total volume of U.S. Domestic and International Interchange and Chargebacks for a single Merchant Outlet and identifies U.S. 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 International Operating Regulations* 756 (Apr. 15, 2013), *available at http://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf.* MasterCard maintains similar, but not identical, thresholds for its chargeback monitoring programs (at least 100 chargebacks a chargeback ratio of 1.5 percent). MasterCard, *Security Rules and Procedures: Merchant Edition* 8–13 (Feb. 22, 2013), *available at http://www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf.*

[66] MasterCard maintains the Member Alert to Control High-risk Merchants (''MATCH'') file, a database that acquiring banks and payment processors use to report merchants that they have terminated for risk-related reasons. In turn, banks and payment processors must check prospective merchants against the MATCH file as part of the underwriting process. *MasterCard Security Rules and Procedures, id.* at 11–1.

[67] A ''returned item'' is a check sent through the check clearing network or an electronic debit processed through the ACH Network that has been returned unpaid to the originating bank. Consumers may initiate returns of checks and electronic debits by disputing the payment with their bank. For traditional checks, this process is governed by the UCC; for electronic debits, it is governed by the EFTA and Regulation E.

[68] FFIEC, *Retail Payment Systems Booklet, supra* note 41, at 16.

[69] NACHA may initiate a rules enforcement proceeding against an originating depository financial institution (''ODFI'') when its merchant generates a return rate for unauthorized transactions that exceeds 1 percent in a month. NACHA Operating Rules, Art. II, § 2.17.2 (ODFI Return Rate Reporting) and § 10.4.3 (Initiation of a Rules Enforcement Proceeding) (2013). A read-only version of the 2013 edition of the NACHA Rules is available at *www.achrulesonline.org* at no cost to registered users.

On March 15, 2013, NACHA tightened the timeline from 60 days to 30 day for ODFIs to reduce a merchant's return rate for unauthorized transactions below the 1 percent threshold before initiation of a Rules enforcement proceeding. NACHA, *ODFI Return Rate Reporting (Risk Management) March 15, 2013, available at https://www.nacha.org/ODFI-Return-Rate-Reporting-(Risk%20Management)-March-15-2013.*

newsletters. NACHA rules apply additional restrictions on ''telephone-initiated'' (abbreviated as ''TEL'') transactions, which historically have been fertile ground for fraud.[70]

Merchant returns and chargebacks [71] that exceed either the thresholds set by credit card system operators or the average return rate experienced by ACH participants often may indicate either that the merchant is submitting transactions that consumers have not authorized, or that the merchant engaged in deceptive conduct to obtain any such authorization.[72] The Commission's law enforcement experience also confirms that high total return rates are a strong indicator of fraud.[73] In more than a decade of Commission enforcement actions alleging that payment processors made unauthorized debits to consumer bank accounts on behalf of fraudulent merchants, the return rates were staggeringly high and vastly out of proportion with industry norms.[74] Although telemarketers engaged in fraud obviously continue to look for ways to subvert the anti-fraud mechanisms of the credit card systems and the ACH Network,[75] the specific initial due diligence and subsequent monitoring of return activity undertaken by the operators of these systems—as well as a steady stream of law enforcement actions by the Commission and other federal and state law enforcement agencies—make it more difficult for wrongdoers to gain and, critically, to maintain access to these payment systems.[76]

Therefore, telemarketers engaged in fraud and the payment processors who assist them have increasingly turned to remotely created checks and remotely created payment orders to defraud consumers.[77] The systemic weaknesses of the check clearing system make it much more accommodating for them than the credit card system or ACH Network. It is much easier for a merchant to open an ordinary business checking account and use it to create and deposit remotely created checks or remotely created payment orders into the check clearing system than it is to establish a credit card merchant account or qualify for ACH origination services.

Moreover, based on current practices, it is impossible for banks to systematically distinguish remotely created checks from conventional checks, or to calculate their isolated rates of return. The reason for this is rooted in the structure and history of the check collection system, which is highly decentralized and originally paper-based. In these respects, it stands in marked contrast to the credit card system and the ACH Network. The interbank check clearing process involves one bank (the ''depository bank'') presenting a check to another bank (the ''payor bank'') for payment. When a depository bank receives a check, it encodes the amount of the check in magnetic ink at the bottom of the check, and forwards the magnetic ink character recognition (''MICR'') information to the payor bank for settlement.[78] Enactment of the Check 21 Act [79] permits banks now to capture an image of the front and back of the original check and exchange the image and MICR line data in the clearing and

[70] NACHA's ''TEL rule'' 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 (Telephone-Initiated Entry)) (2013). For inbound telephone orders and transactions in which the merchant has an existing business relationship with the consumer, a merchant may obtain a consumer's authorization to initiate an ACH debit. As evidence of a consumer's authorization of a TEL transaction, the merchant 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.

Historically, NACHA limited consumer-authorized TEL transactions to single-entry payments. However, in 2011 NACHA amended its operating rules to permit recurring TEL transactions. NACHA, *Enhancements to ACH Applications FAQs,* (Jan. 19, 2011), *available at http://admin.nacha.org/userfiles/File/ACH_Rules/Application%20Enhancements%20rule%20changes%20FAQs.pdf.* For recurring TEL entries to be compliant with NACHA's rules, a merchant must record the oral authorization and provide the consumer with a copy of the authorization. *Id.*

[71] For ease of reference, this section of the NPRM uses the term ''returns'' to refer to both chargebacks and returned items, as defined *supra* in notes 64 and 67.

[72] *See, e.g.,* Financial Crimes Enforcement Network (''FinCEN''), Advisory FIN–2012–A010, Risk Associated with Third-Party Payment Processors (October 22, 2012), *available at http://www.fincen.gov/statutes_regs/guidance/html/FIN-2012-A010.html* (noting that high numbers of consumer complaints and ''particularly high numbers of returns or charge backs (aggregate or otherwise), suggest that the originating merchant may be engaged in unfair or deceptive practices or fraud, including using consumers' account information to create unauthorized RCCs or ACH debits.''); McEntee, *supra* note 59, ¶ 32.

[73] Total return rate refers to the total number of ACH debit transactions that were returned for any reason code, divided by the total number of ACH debit transactions processed nationwide for that time period. For example, the average total return rate for all ACH debit transactions in 2011 was 1.52 percent. *FTC* v. *Ideal Financial Solutions, Inc.,* Civ. No. 2:13–00143–MMD–GWF (D. Nev. filed Jan. 28, 2013) at ¶ 37, *available at http://www.ftc.gov/os/caselist/1123211/index.shtm.*

[74] *See, e.g., Landmark, supra* note 42 (alleging defendants accepted merchants with anticipated return rates of 70 to 75 percent, and continued processing remotely created payment orders for merchant that generated return rates ranging from 50 to 80 percent); *YMA, supra* note 37 (defendants allegedly processed ACH and demand draft debits on behalf of merchants that generated return rates ranging from 32 to 82 percent); *FTC* v. *3d Union Card Serv.,* Civ. No. S–04–0712, ¶ 15 (D. Nev. July 19, 2005) (default judgment finding nearly 70 percent of defendants' debits to consumers' accounts were returned or refused by the consumers' banks); *FTC* v. *Interbill, Ltd.,* Civ. No. 2:06–01644 (D. Nev. Apr. 30, 2009) (summary judgment against defendants that continued to process transactions for merchant, Pharmacycards.com, despite a return rate of nearly 70 percent); *FTC* v. *Universal Processing, Inc.,* Civ. No. 05–6054 (C.D. Cal. Aug. 18, 2005) (stipulated permanent injunction in case with an alleged return rate exceeding 70 percent); *FTC* v. *Electronic Financial Group, Inc.,* Civ. No. 03CA0211 (W.D. Tex. Mar. 23, 2004) (stipulated permanent injunction in case with alleged return rates between 40 and 70 percent).

States also have sued payment processors that assisted fraudulent telemarketers by continuing to process transactions in spite of their high return rates and telephone sales scripts evidencing misrepresentations or violations of the law. *See, e.g., Ohio* v. *Capital Payment Sys. Inc.,* Civ. No. 08 H 5 7234 (Franklin County, OH Ct. Com. Pl. (Jan. 31, 2012) (entry of summary judgment finding defendants processed ACH debits and remotely created checks for fraudulent telemarketers that generated return rates ranging from 19 to 68 percent); *Ohio* v. *Cimicato,* Civ. No. 06 H 3 04698 (Franklin County, OH Ct. Com. Pl. Oct. 12, 2012) (Stip. J.) (alleged return rates ranging from 32 to 90 percent); *Iowa* v. *Teledraft Inc.,* Civ. No. 4:04–90507 (S.D. Iowa Dec. 9, 2005) (Stip. J.) (defendants allegedly processed ACH debits for merchants with total return rates ranging from 51 to 77 percent); *Vermont* v. *Amerinet, Inc.,* Civ. No. 642–10–05 (Super. Ct. filed Oct. 31, 2005) (defendants allegedly continued to process bank debits despite return rates as high as 80 percent).

[75] Many fraudulent telemarketers who engage in outbound telemarketing violate NACHA's TEL rule by processing payments through the ACH Network. *See, e.g., FTC* v. *Elec. Fin. Group Inc.,* Civ. No. 03–211 (W.D. Tex. Mar. 23, 2004) (Stip. Perm. Inj.); *FTC* v. *First Am. Payment Processing, Inc.,* Civ. No. 04–0074 (D. Ariz. Nov. 2, 2004) (Stip. Perm. Inj.). When compared to the check fraud losses experienced by banks, however, ''ACH transactions have had a relatively good track record.'' Furst & Nolle, *supra* note 50, at 10–11.

[76] Since 1995, the Commission has filed more than 300 cases involving violations of the TSR, many of which have included fraudulent or unauthorized charges to consumers' credit card or bank accounts.

[77] *See, e.g., FTC* v. *Landmark, supra* note 63 (describing defendants' promotion of their remotely created payment order processing product as a less regulated alternative to ACH transactions for merchants with a history of high return rates); Expert Report of Dennis M. Kiefer, ¶¶ 31–32 (Oct. 2, 2008), *filed in YMA, supra* note 37 (describing the defendants' efforts to migrate client merchants with high return rates from ACH to demand draft transactions); *see also* George F. Thomas, Digital Transactions, *It's Time to Dump Demand Drafts,* at 39 (July 2008), *available at http://www.radix consulting.com/TimetoDumpDemandDrafts.pdf* (''[Y]ou will find merchant-processing sites that advise merchants in high-risk categories or with high unauthorized-return rates to avoid the scrutiny of the ACH by using demand drafts.'').

[78] Before advances in electronic check processing, the physical processing of checks relied on high-speed reader/sorter equipment to scan the MICR line at the bottom of each check, which contains very limited information—numbers that identify the bank branch, bank routing number, check number, and account number at the payor bank.

[79] *See supra* note 38.

payment process instead of relying on the paper check.

Remotely created checks contain no unique identifier distinguishing them as such; and they are cleared in the same manner as traditional paper checks. Without examination of the signature block on each check, there is currently no feasible way for banks to analyze the volume, use, or return rate for remotely created checks.[80]

Like remotely created checks, remotely created payment orders cannot be distinguished from other check images deposited into the check clearing system.[81] Thus, the Federal Financial Institutions Examination Council notes that:

[w]hen a financial institution permits the creation of electronic [remotely created] payment orders, substantial risk-management oversight for unauthorized returns and other unlawful activity is lost because the check-clearing networks do not provide the level of technological and organizational controls of those in the ACH network [or the credit card system]. This lack of systemized monitoring of electronically created payment orders increases their susceptibility to fraud by Web-based vendors and telemarketers.[82]

As a result of these combined factors, there exists no *systemwide* transaction data available for remotely created checks or remotely created payment orders that are returned through the check clearing system,[83] and scant data on the overall number of such transactions that results in consumer complaints. Nevertheless, substantial harm resulting from unauthorized remotely created checks is documented in a number of enforcement cases.[84]

As the law enforcement cases discussed in the next section demonstrate, *individual* banks and payment processors, however, can detect remotely created checks, investigate the total return rates of their clients' check transactions, compare the percentage of returned remotely created checks to the return rate for all checks transacted through the national banking system (approximately one half of one percent or .5 percent),[85] attempt to categorize the specific reasons for returns, compare their clients' return rates to industry average return rates for other payment mechanisms (such as credit card payments and ACH debits), and watch closely for other signs of suspicious or fraudulent merchant activity. As the complaint in *United States* v. *First Bank of Delaware*[86] highlights, banks and payment processors have perverse financial incentives to begin processing remotely created checks for ''high-risk'' merchants and originators.[87] This is because they charge higher transaction fees to such merchants, and receive additional fees for each returned check.[88] Thus, unscrupulous banks and payment processors often continue to process transactions for fraudulent operations such as these, even in the face of high return rates or other *indicia* of fraud.

3. Law Enforcement Experience with Remotely Created Checks and Remotely Created Payment Orders in Fraudulent Telemarketing

There is substantial evidence that remotely created checks are being widely misused in telemarketing, resulting in very significant consumer injury.[89] The Commission's law enforcement experience demonstrates that telemarketers engaged in fraud use a variety of methods to deceive or pressure consumers into divulging their bank account information in order to debit money from their bank accounts. Wrongdoers exploiting remotely created checks have promoted any number of phony or pretextual offers,[90] including: advance fee credit cards; [91] solicitations for bogus charities; [92] purported medical

[80] In an attempt to quantify the number of remotely created checks being automatically processed through the check clearing system, in 2007, the Federal Reserve System conducted a check sampling study of 30,000 randomly-selected checks. The study required ''three independent investigators to 'interrogate,' i.e., systematically collect information from, each sampled check.'' Federal Reserve System, *The Check Sample Study: A Survey of Depository Institutions for the 2007 Federal Reserve Payments Study,* 8 (Mar. 2008) (''2007 Check Sample Study''), *available at http://www.frbservices.org/files/communications/pdf/research/2007_check_sample_study.pdf.* The study estimated that approximately 0.95 percent or 308 of the 32,448 checks sampled in 2006 were remotely created. *Id.* at 33.

[81] *See Proposed Rule; Regulation CC, supra* note 40 and accompanying text.

[82] FFIEC, *Retail Payment Systems Booklet, supra* note 41, at 16.

[83] Despite the continued decline in overall check volume, the Federal Reserve's 2010 Payments Study revealed a significant increase in the volume of remotely created checks from .95 percent in 2006 to 2.1 percent in 2009. 2010 Payments Study, *supra* note 44, at 37; 2007 Check Sample Study, *supra* note 80. *See also* Carroll, *supra* note 36 (estimating the number of remotely created checks in 2006 at 286 million items, and noting the substantial adverse consumer impact of fraudulent remotely created checks).

[84] *See, e.g., United States* v. *First Bank of Delaware,* Civ. No. 12–6500, §§ 3, 73–75 (E.D. Pa. Nov. 19, 2012) (settlement of case alleging defendant originated more than 2.6 million remotely created check transactions totaling approximately $123 million ''on behalf of third-party payment processors in cahoots with fraudulent Internet and telemarketing merchants,'' including Landmark Clearing, Check21, Check Site, and Automated Electronic Checking); *FTC* v. *FTN Promotions, Inc.* (''*Suntasia*''), Civ. No. 8:07–1279 (M.D. Fla. Dec. 30, 2008) (Stip. Perm. Inj.) (defendants allegedly caused more than $171 million in unauthorized charges to consumers' accounts for bogus travel and buyers clubs in part by using unauthorized remotely created checks); *FTC* v. *Universal Premium Servs., Inc.,* Civ. No. 06–0849 (C.D. Cal. Feb. 27, 2007), *aff'd, FTC* v. *MacGregor,* 360 F.App'x. 891 (9th Cir. 2009) (final order after summary judgment for more than $28 million against defendants that used unauthorized remotely created checks as payment in fake shopping spree scam); Dep't of Justice Press Release, *International Bank Fraud Ring Busted for Attempt to Debit 100,000 Customer Accounts for Over $20 Million,* (Jan. 13, 2009) (announcing the arrest of one of nine co-conspirators in a purported telemarketing scheme that used ACH debits and remotely created checks to make unauthorized withdrawals or attempted withdrawals from approximately 100,000 consumer bank accounts), *available at http://www.justice.gov/usao/nj/Press/files/pdffiles/2009/sale0113%20rel.pdf. See also infra* notes 91–104 and accompanying text, describing numerous enforcement actions.

[85] *See infra* note 107 and *First Bank of Delaware, supra* note 84, at § 52.

[86] *First Bank of Delaware, supra* note 84.

[87] According to bank regulators, ''[e]xamples of high-risk parties include online payment processors, certain credit-repair services, certain mail order and telephone order (MOTO) companies, illegal online gambling operations, businesses located offshore, and adult entertainment businesses. These operations are inherently more risky and incidents of unahtorized (sic) returns are more common with these businesses.'' Office of the Comptroller of the Currency (''OCC'') Bulletin 2006–39 (Sept. 1, 2006), *available at http://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html.*

[88] *See, e.g., FTC* v. *Landmark, supra* note 63 at ¶ 27 (defendants' pricing structure enabled them to earn significantly higher fee income from returned transactions than the income generated by cleared transactions); *First Bank of Delaware, supra* note 84, at ¶¶ 54 and 63 (bank allegedly took on higher risk for potential profit and earned higher fees for unauthorized returns); *see also* Kiefer, *supra* note 77, at ¶ 33 (''[YMA defendants] charged fees resulting from bad ACH and [demand] Draft transactions that were many multiples of the fees they otherwise would have charged.'').

[89] In the past, law enforcement actions primarily involved remotely created checks and not remotely created payment orders. As recent law enforcement actions demonstrate, remotely created payment orders are subject to the same, if not greater, risks as remotely created checks. *See, e.g., FTC* v. *Landmark, supra* note 63; *First Bank of Delaware, supra* note 84. The Commission, therefore, proposes that remotely created payment orders should be treated in the same way as remotely created checks.

[90] The majority of the Commission's fraud cases involving remotely created checks have involved outbound telemarketing campaigns; however, the risks associated with this payment method exist equally in the inbound telemarketing context. *See, e.g., FTC* v. *LowPay, Inc.,* Civ. No. 09–1265 (D.O. Sept. 10, 2010) (stipulated permanent injunction against advance fee credit card scheme using inbound calls).

[91] *See, e.g., FTC* v. *Group One Networks, Inc.,* Civ. No. 09–00352 (M.D. Fla. Mar. 19, 2010) (Stip. Perm. Inj.); *FTC* v. *Capital Choice Consumer Credit, Inc.,* Civ. No. 02–21050 (S.D. Fla. Feb. 19, 2004) (Stip. Perm. Inj.); *FTC* v. *Bay Area Bus. Council, Inc.,* Civ. No. 02–5762 (N.D. Ill. Apr. 14, 2003) (Summ. J.), *aff'd, FTC* v. *Bay Area Bus. Council, Inc.,* 423 F.3d 627 (7th Cir. 2005); *FTC* v. *Sainz Enters., LLC,* Civ. No. 04–2078 (D. Colo. Nov. 4, 2004) (Stip. Perm. Inj.).

[92] *See, e.g., FTC* v. *Handicapped & Disabled Workshops, Inc.,* Civ. No. 08–0908 (D. Ariz. Dec. 9,

Continued

discount plans [93] or pharmacy discount cards; [94] useless fraud-prevention services; [95] and misrepresented products or deceptive buyers club memberships.[96] In these ways, fraudulent telemarketers have bilked hundreds of millions of dollars from consumers using remotely created checks.

Numerous law enforcement actions show that telemarketers engaged in fraud frequently rely on third-party processors to create, print, and deposit remotely created checks drawn on consumers' accounts.[97] By providing the means to extract money from consumers' bank accounts via remotely created checks and remotely created payment orders, payment processors play an indispensable role in furtherance of their clients' fraudulent and deceptive schemes.[98] The Commission and the Department of Justice have sued such non-bank payment processors, alleging they engaged in unfair practices under Section 5 of the FTC Act, as well as violations of mail and wire fraud statutes and the TSR's prohibition on assisting and facilitating fraud by processing remotely created checks for telemarketers, while knowing or consciously avoiding knowledge that the telemarketers were violating the TSR.[99]

Unscrupulous merchants and third-party processors must establish relationships with banks that accept deposits of remotely created checks and remotely created payment orders. Aggressive action taken by federal prosecutors and bank regulators against banks that engaged in such fraud further illustrates the problematic use of remotely created checks and remotely created payment orders in telemarketing. Most recently, the United States Attorney for the Eastern District of Pennsylvania obtained a $15 million civil penalty against First Bank of Delaware, based on its origination of remotely created checks, remotely created payment orders, and ACH debits on behalf of merchants and payment processors engaged in fraud, including the defendants in *FTC* v. *Landmark.*[100] First Bank of Delaware allegedly ignored significant signs of fraud, including the fact that its third-party payment processors had aggregate return rates for remotely created checks exceeding 50 percent from 2009 to 2011. In an earlier action against First Bank of Delaware brought by the Federal Depository Insurance Corporation (''FDIC''), the bank agreed to terminate, among other things, ''any and all services, products and/or relationships pertaining to or involving payment processing by or through an automated clearing house, the origination and/or processing of remotely created checks and/or merchant acquiring.'' [101]

In a 2006 proceeding, the Office of the Comptroller of the Currency (''OCC'') alleged that telemarketers victimized more than 740,000 consumers using remotely created checks processed by three payment processors through Wachovia accounts.[102] All three of these payment processors allegedly knew their clients had return rates well above accepted industry standards.[103] The bank agreed to pay over $150 million in

2008) (stipulated permanent injunction against defendants that allegedly used remotely created checks to defraud elderly consumers out of nearly $10 million in connection with high-pressure, deceptive sales of products that purportedly help blind and disabled workers). In just two months, Handicapped & Disabled Workshops' telemarketers allegedly used unauthorized remotely created checks to withdraw over $5,513.55 (including $1,025.90 in a single day) from an 82 year old woman's bank account. *Id.,* Decl. of Patricia W. Bunge, ¶ 6 (Apr. 15, 2008).

[93] *See, e.g., FTC* v. *NHS Sys., Inc.,* Civ. No. 08–2215 (E.D. Pa. Mar. 28, 2013) (Summ. J.); *FTC* v. *6554962 Canada, Inc.,* Civ. No. 1:08–02309 (N.D. Ill. Aug. 19, 2009) (Default J.); *FTC* v. *9107–4021 Quebec, Inc.,* Civ. No. 08–1051 (E.D. Ohio July 17, 2009) (Stip. Perm. Inj.). *See also, e.g., United States* v. *Borden,* Cr. No. 1:08–00196 (N.D.N.Y. sentenced Dec. 3, 2009) (defendant pleaded guilty and was sentenced to 56 months' imprisonment in connection with a fake medical benefits telemarketing scheme that used remotely created checks to bilk elderly consumers).

[94] *See, e.g., FTC* v. *3d Union Card Servs., Inc.,* Civ. No. S–04–0712 (D. Nev. July 19, 2005) (Default J.) (complaint alleged telemarketers initiated $10 million in unauthorized remotely created checks and other debits from more than 90,000 consumers' accounts in three months for fraudulent discount pharmacy cards).

[95] *FTC* v. *4086465 Canada, Inc.,* Civ. No. 04–1351 (N.D. Ohio Nov. 7, 2005) (stipulated permanent injunction against telemarketers allegedly used unauthorized remotely created checks as payment for fake consumer protection service that promised to protect consumers from telemarketing and unauthorized banking).

[96] *See supra* note 84.

[97] *United States* v. *Cimicato,* Cr. No. 1:10–0012 (W.D.N.Y. Jan. 26, 2010) (defendant pled guilty to wire fraud in connection with Integrated Check Technologies' processing of remotely created checks for fraudulent Canadian telemarketers); *United States* v. *Guastaferro,* Cr. No. 1:09–347 (W.D.N.Y. Jun. 27, 2011) (sentenced to 24 months in prison and fined $100,000 for his involvement in Integrated Check Technologies' payment processing scheme); *United States* v. *Whitworth,* Cr. No. 1:10–324 (W.D.N.Y. Jan 6, 2012) (same, sentenced to 18 months); *YMA, supra* note 37; *Payment Processing Ctr., supra* note 37; *FTC* v. *Interbill, Ltd.,* Civ. No. 2:06–01644 (D. Nev. 2007); *FTC* v. *Windward Mktg., Ltd.,* Civ. No. 1:96–615 (N.D. Ga. 1996); *see also Capital Payment Sys., supra* note 74; *Ohio* v. *Cimicato, supra* note 74; *Iowa* v. *Teledraft, Inc.,* Civ. No. 04–90507 (S.D. Iowa filed Sept. 17, 2004). *Cf., 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) (defendants' Internet-based business facilitated fraudulent operations that created more than 150,000 unauthorized checks totaling more than $400 million).

[98] As the FFIEC has advised, ''[s]ome higher-risk merchants routinely use third parties to process their transactions because of the difficulty they have in establishing a direct bank relationship.'' FFEIC, *Bank Secrecy Act Anti-Money Laundering Examination Manual: Third-Party Payment Processors—Overview (2010),* at 240. *See also* George F. Thomas, *Not Your Father's ACH,* ICBA Indep. Banker (July 2007), *available at http://www.radixconsulting.com/icbaarticle.pdf* (''Many of the merchants that use third-party processors do so because they could not pass the standard know-your-customer procedure if they approached [a] financial institution directly. Like cockroaches, these merchants cannot withstand the light of scrutiny.'').

[99] For example, between June 23, 2004 and March 31, 2006, the YMA defendants allegedly processed over $200 million in debits and attempted debits to consumers' bank accounts, more than $69 million of which were returned or rejected by consumers or their banks. *YMA, supra* note 37, Compl. at ¶ 29; McEntee, *supra* note 59, ¶¶ 44–46. One of the Commission's experts in the case uncovered evidence that the defendants intentionally shifted merchants with excessive return rates from ACH debits to remotely created checks in order to continue assisting merchants in defrauding consumers. Kiefer, *supra* note 77, at ¶ 31.

In yet another case, the United States Attorney for the Eastern District of Pennsylvania alleged that during a ten-month period, a payment processor assisted telemarketers in attempting to withdraw $142 million from consumers' accounts using unauthorized remotely created checks, causing more than $50 million in consumer losses. *Payment Processing Ctr., supra* note 37.

[100] *First Bank of Delaware, supra* note 84; *Landmark, supra* note 42. According to the complaint filed by the Commission in *FTC* v. *Leanspa,* First Bank of Delaware also processed payments for the defendants, who allegedly used fake news Web sites to promote their products, made deceptive weight-loss claims, and misrepresented the terms of their ''free trial'' offers. *FTC* v. *LeanSpa,* Civ. No. 3:11–1715 (Nov. 22, 2011) (Stip. Prelim. Inj.). *See also, e.g. In the Matter of Meridian Bank,* FDIC 12–367b (Oct. 19, 2012) (consent order requiring, among other things, cessation of all third party payment processing unless and until bank completes comprehensive due diligence on each payment processor and its merchant-clients), *available at http://www.fdic.gov/news/news/press/2012/pr12136a.html*; *In the Matter of Metro Phoenix Bank,* FDIC 111–083b (Jun. 21, 2011) (same, including cessation of all third party payment processing for CheckGateway LLC and Teledraft, Inc.), *available at http://www.fdic.gov/bank/individual/enforcement/2011-06-001.pdf.*

[101] *In the Matter of First Bank of Delaware,* FDIC–11–669b, 2 (Dec. 3, 2011), *available at http://fdic.gov/bank/individual/enforcement/2011-12-03.pdf.*

[102] OCC Press Release, *OCC, Wachovia Enter Revised Agreement to Reimburse Consumers Directly* (Dec. 11, 2008), *available at http://www.occ.gov/ftp/release/2008-143.htm.*

[103] The FTC previously had sued two of the three payment processors (YMA and Suntasia) and the U.S. Department of Justice sued the third (Payment Processing Center). The FTC also brought cases against many of the telemarketers that worked with the three processors. *See, e.g., Universal Premium Servs. supra* note 84; *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) (Perm. Inj.); *FTC* v. *Frankly Speaking, Inc.,* Civ. No. 1:05–60 (M.D. Ga. May 14, 2005) (Stip. Perm. Inj.).

restitution to resolve the matter. Based on these and other allegations, the U.S. Attorney's Office in the Southern District of Florida and the Asset Forfeiture and Money Laundering Section of the Criminal Division of the Department of Justice filed a criminal case against Wachovia.[104] The case resulted in a deferred prosecution agreement and payment of $160 million in restitution and other penalties.[105]

In another case, the OCC entered into a settlement agreement with T Bank, N.A. in which it agreed to pay a $100,000 civil penalty and make payments totaling $5.1 million in restitution to more than 60,000 consumers affected by the bank's relationships with a third-party payment processor, Giact Systems Inc. The OCC alleged that Giact and several of Giact's merchant-clients (telemarketers and Internet merchants) used remotely created checks to make unauthorized withdrawals from consumers' accounts.[106] The OCC's investigation revealed that over 60 percent of these remotely created checks were returned to the bank by or on behalf of individuals who said they never authorized the checks or that they had never received the products or services promised by the telemarketers or merchants.[107]

State Attorneys General also have sued payment processors along with the telemarketers who have swindled consumers using remotely created checks.[108] In addition, state and Canadian law enforcement authorities have been active in attempting to regulate and halt abuses of remotely created checks. To combat the vulnerability of remotely created checks to fraud, several states and the Canadian Payments Authority (''CPA'') have restricted or prohibited the use of remotely created checks in telemarketing transactions.[109] In May 2005, thirty-seven Attorneys General also signed a letter urging the Board of Governors of the Federal Reserve to prohibit remotely created checks.[110]

Despite these efforts, telemarketers engaged in fraud face no effective impediment to their use of remotely created checks and remotely created payment orders. And, as the credit card systems and ACH Network have redoubled their efforts to detect and deter fraud—by monitoring returns and transaction data, imposing fines and penalties on participants that violate their operating rules, and requiring banks to conduct more robust up-front due diligence on client merchants—wrongdoers are forced to turn to more novel payment methods that fall outside this zone of increased scrutiny. To close off this avenue to fraudulent telemarketers, the Commission therefore proposes to prohibit the use of remotely created checks and remotely created payment orders in all telemarketing transactions.

In doing so, the Commission recognizes that, for certain transactions, remotely created checks and remotely created payment orders may offer advantages over electronic fund transfers via the ACH Network,[111] such as same-day availability of funds for merchants.[112] In light of significant changes in the marketplace, and to ensure that the rulemaking record adequately reflects the potential impact of the proposed ban against remotely created checks and remotely created payment orders on legitimate telemarketing businesses, the Commission encourages the submission of comments describing the types of telemarketing transactions in which remotely created checks or remotely created payment orders are essential, including the types of products or services involved, whether the telemarketing calls are inbound or outbound, whether certain telemarketing transactions could be processed via the ACH Network under NACHA's rules for recurring TEL transactions, as well as the resulting cost increase or savings, if any, from the use or avoidance of the ACH Network.

4. The Use of Remotely Created Checks and Remotely Created Payment Orders Is an Abusive Telemarketing Act or Practice

As explained in Section I.B above, when the Commission considers identifying a telemarketing practice as abusive, it does so within the purview of the Commission's traditional unfairness analysis.[113] An act or

[104] *United States* v. *Wachovia, N.A.,* Cr. No. 10–20165 (S.D. Fla. Mar. 16, 2010) (alleging that defendant maintained account relationships with certain payment processors that deposited more than $418 million using remotely-created checks into Wachovia accounts on behalf of fraudulent telemarketers).

[105] According to the press release announcing the deferred prosecution, ''Wachovia admitted that it failed to identify, detect, and report the suspicious transactions in the third-party payment processor accounts, as required by the BSA [Bank Secrecy Act, 31 U.S.C 1051 *et seq.*], due to deficiencies in its anti-money laundering program. Specifically, Wachovia failed to conduct appropriate customer due diligence by delegating most of this responsibility to business units instead of compliance personnel. Wachovia also failed to monitor high return rates for remotely-created checks and report suspicious wire transfer activity from the processors' accounts.'' U.S. Att'y's Office (S.D. Fla.) Press Release, *Wachovia Enters Into Deferred Prosecution Agreement* (Mar. 17, 2010), *available at http://www.justice.gov/usao/fls/Press Releases/100317-02.html.*

[106] *In the Matter of T Bank, N.A.,* #2010–068, AA–EC 09–103 (Apr. 15, 2010) (in addition, the formal agreement requires the bank to develop and adhere to strict ''policies, procedures, and standards for payment processor relationships'' before entering into a banking relationship with a payment processor), *available at http://www.occ.gov/news-issuances/news-releases/2010/nr-occ-2010-45a.pdf. See also* OCC Press Release, *OCC, T Bank Enter Agreement to Reimburse Consumers* (Apr. 19, 2010), *available at http://www.occ.gov/news-issuances/news-releases/2010/index-2010-news-releases.html.*

[107] To provide context for the return rates identified above, in the 2010 Payments Study, the Federal Reserve Board estimated that from 2006 to 2009, ''[t]he ratio of [unpaid] returned checks to paid checks by value declined from 0.44 percent to 0.40 percent.'' *Supra* note 44, at 9. In previous years, the Board estimated the return rate for checks at 0.6 percent in 2000, and 0.5 percent in 2003. Federal Reserve System, *2004 Federal Reserve Board Payments Study* 6 (Dec. 15, 2004), *available at http://www.frbservices.org/files/communications/pdf/research/2004Payment ResearchReport.pdf.* Like the return rates expected for legitimate merchants in the credit card systems and ACH Network, the return rate for checks (including remotely created checks) should be very low. McEntee, *supra* note 59, & 44 (''[T]here is no legitimate business reason why there would be a significant difference between ACH and demand draft return rates, assuming the merchant is engaged in the same line of business.'').

[108] *See, e.g., Capital Payment Sys., supra* note 74; *Ohio* v. *Cimicato, supra* note 74; *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 J.).

[109] In 2003, the CPA adopted a policy prohibiting the use of remotely created checks (or ''tele-cheques'') as a preemptive measure based on the heightened risk of fraud and unauthorized payments. Ana Cavazos-Wright, Federal Reserve Bank of Atlanta, *An Examination of Remotely Created Checks,* at n.8, *available at http://www.frbatlanta.org/documents/rprf/rprf_resources/RPRF_wp_0510.pdf; see also, e.g.,* ARK. CODE ANN. § 4–99–203 (1987) (prohibiting telemarketers from obtaining or submitting for payment a check drawn on a person's bank account without the consumer's express written authorization); N.Y. GEN. BUS. LAW § 399-pp (McKinney 2006) (same); VT. STAT. ANN. tit. 9, § 2464 (2006 & Supp. 2010) (same).

[110] Comment, National Association of Attorneys General, *Proposed Amendment to Regulation CC Remotely Created Checks,* FRB Dkt. No. R–1226 (May 9, 2005), *available at http://www.federalreserve.gov/SECRS/2005/May/20050512/R-1226/R-1226_264_1.pdf.*

[111] Electronic fund transfers via the ACH Network are available to all inbound telemarketers and to those outbound telemarketers who have a pre-existing relationship with the consumer. *See supra* note 70 (explaining NACHA's TEL rule).

[112] NACHA, *RCC and ACH Differentiators, supra* note 60, at 9 (describing the advantage of using remotely created checks in effectuating insurance coverage on the same day the payment is submitted). The current ACH settlement schedules are next-day or, for some credits, two days. NACHA has been exploring ways to reduce the settlement times for certain types of ACH entries. Letter from NACHA to Regional Payments Associations Direct Financial Institution Members (revised July 10, 2012), *available at https://www.nacha.org/EPS_SupplementalInfoandMaterials#epsattachments.*

[113] *Supra* notes 3, 19—20 and accompanying text.

practice is unfair under Section 5 of the FTC Act if it causes or is likely to cause substantial injury to consumers, if the harm is not outweighed by any countervailing benefits to consumers or competition, and if the harm is not reasonably avoidable.[114] The Commission preliminarily concludes that the use of remotely created checks and remotely created payment orders in telemarketing transactions meets this unfairness test.

As discussed above, the Commission's law enforcement experience demonstrates the substantial consumer injury that results from telemarketers' use of remotely created checks and remotely created payment orders.[115] Second, the economic harm from the use of remotely created checks and remotely created payment orders in telemarketing outweighs any countervailing benefits to consumers or competition.[116] The Commission is aware that remotely created checks and remotely created payment orders processed through the bank clearing system may make funds available to merchants more quickly than certain types of electronic fund transfers, such as ACH debits, and are used for recurring payments authorized by telephone.[117] However, it is the Commission's understanding that this advantage is less critical in telemarketing transactions than in other contexts, such as making last minute bill payments and collecting debts owed by consumers. Innovations in payment cards and access devices have increased the number and availability of convenient, fast, noncash payment alternatives to the use of remotely created checks.[118] These alternatives offer both dispute resolution rights and protection against unlimited liability for unauthorized charges to consumers and are available to consumers who do not possess or do not wish to use credit cards.[119] Thus, it appears that the significant injury and risk of harm to consumers is not outweighed by the benefits of using remotely created checks and remotely created payment orders in telemarketing transactions.[120]

Finally, it appears that consumers cannot reasonably avoid the injury. When consumers give their bank account numbers to a telemarketer to make a purchase, they have little or no ability to control whether the telemarketer will process the charge via the ACH system, which is monitored for fraud and provides EFTA and Regulation E protections, or as a remotely created check or remotely created payment order. In addition, consumers do not understand the differences in protections they have with a payment that clears through the ACH system and those that are available when a payment is processed as a remotely created check or remotely created payment order. Finally, consumers cannot avoid injury by checking their account records and disputing any unauthorized charges that may be there. As discussed above, disputing an unauthorized remotely created check or remotely created payment order is a long and time-consuming process that may be futile, since the UCC lacks significant consumer protections.

Telemarketers that choose to use remotely created checks and remotely created payment orders effectively deprive consumers of the anti-fraud monitoring, accountability, and dispute resolution mechanisms of other payment methods.[121] Thus, the harm to consumers is unavoidable; and the harm, in the form of unauthorized charges and limited consumer protections against fraud, is significant and does not appear to be outweighed by any countervailing benefits to consumers or competition given the widespread availability of alternative payment methods that provide greater consumer protection.

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

Cash-to-cash money transfers offer individuals a fast and convenient method for sending funds to someone they know and trust in a different location.[122] This speed and ease, however, make these money transfers a preferred payment method in telemarketing to perpetrate cross-border fraud. To initiate a cash-to-cash money transfer, a sender provides currency to a money transfer provider (such as Western Union or MoneyGram), fills out a ''send form'' designating the name and address of the recipient to whom the money transfer is to be sent, and pays a transaction fee.[123] The money transfer provider's employee or agent inputs the transaction information into a computer network, whereupon the value of the money the sender paid is made available within minutes to the recipient. At that point, the recipient can claim the funds in cash at any of the money transfer provider's locations, with little or no need to provide any personal identification or identifying

[114] 15 U.S.C. 45(n).

[115] Remotely created checks are subject to the UCC and lack both dispute resolution rights and protection against unlimited liability for unauthorized charges, which compounds the injury caused by fraudulent telemarketing. As previously discussed, it remains unclear whether remotely created payment orders are subject to the EFTA. Regardless, without changes to the interbank clearing system that would enable banks to distinguish remotely created payment orders from remotely created checks, banks may continue to treat remotely created payment orders as if they are remotely created checks covered by the UCC. *See supra* note 62 and accompanying text.

[116] *Neovi, supra* note 97, at 1116 (finding this prong of unfairness test satisfied ''[w]hen a practice produces clear adverse consequences for consumers that are not accompanied by an increase in services or benefits to consumers or by benefits to competition'').

[117] *See supra* notes 70 and 112 (discussing NACHA operating rules that permit recurring TEL transactions). Any person initiating recurring electronic debits from a consumer's bank account must comply with the preauthorized transfer rules of Regulation E, 12 CFR 1005.10(b). Regulation E requires the person to: (1) Obtain the consumer's authorization for the recurring debits in a writing signed or similarly authenticated; (2) provide the consumer a clear and readily understandable statement of the terms of the agreement; and (3) give to the consumer a copy of the signed authorization. *Id.*

[118] According to the Federal Reserve Bank of Boston, 94.4 percent of American consumers have adopted one or more types of payment card: credit (72.2 percent), debit (77.0 percent), or prepaid (32.3 percent). Federal Reserve Bank of Boston, *2009 Survey of Consumer Payment Choice,* 41–42 (Apr. 2011).

[119] See supra notes 49—52 (discussing EFTA protections for various debit cards and ACH payments) and infra note 122 (discussing protections for consumers using payment intermediaries, such as PayPal).

[120] In March 2010, NACHA's Risk Management Advisory Group concluded: ACH debit transactions, such as TEL transactions, offer a payment choice where the safeguards to [consumers] outweigh the conveniences that RCCs currently offer to [merchants]. This conclusion is based on the following factors: (1) The heightened risk profile of RCC transactions that bear no evidence of authorization, (2) the fact that ACH transactions can be identified and monitored with relative ease, and (3) the fact that the Rules include clear and explicit authorization requirements for capturing evidence of a consumer's authorization of a transaction.

NACHA, *RCC and ACH Differentiators, supra* note 60, at 12.

[121] 2003 TSR Amendments, 68 FR at 4605.

[122] As explained below in Section IV.A, and used in this NPRM, the term ''cash-to-cash money transfer'' describes a transfer of cash from one person to another person in a different location that is sent by a money transfer provider and received in cash. This term would include a ''remittance transfer,'' as defined in section 919(g)(2) of the EFTA, that is a cash-to-cash transaction. *See infra* note 129 (discussing Remittance Transfer Rule). It does *not* include a remittance transfer or other transfer—such as a transfer from a consumer's account balance with a payment service provider or at a financial institution—that is an electronic fund transfer subject to the EFTA or Regulation E, or a transaction subject to the TILA or Regulation Z. *See* Ronald J. Mann, *Regulating Internet Payment Intermediaries,* 82 Tex. L. Rev. 681, 695 (2004) (noting that payments made via an online payment intermediary (*e.g.,* PayPal) may be covered by the TILA (when funded by a credit card) or the EFTA (when funded by a consumer's account at a financial institution)).

[123] U.S. Gov't Accountability Office, Rep. to the S. Comm. on Banking, Hous., and Urban Affairs, *International Remittances: Information on Products, Costs, and Consumer Disclosures,* 10–11 (Nov. 2005) (''GAO Report''), *available at http://www.gao.gov/new.items/d06204.pdf.*

information in order to do so.[124] For example, when initiating money transfers of less than $900 at MoneyGram, the sender has the option of using a ''Test Question and Answer,'' which enables the recipient to claim the funds without presenting photo identification by instead correctly answering the sender's test question.[125]

Like a cash-to-cash money transfer, a cash reload mechanism offers a convenient method for consumers to convert cash into electronic form. A cash reload mechanism acts as a virtual deposit slip for consumers who wish to load funds onto a general-use prepaid debit card without the use of a bank transfer or direct deposit. A consumer simply pays cash, plus a small fee, to a retailer that sells cash load mechanisms such as MoneyPak or REloadit. In exchange, the consumer receives a unique access or authorization code that corresponds with the specific amount of funds paid. Using the authorization code, a consumer can load the funds onto any existing prepaid debit card within the same prepaid network or an online account with a payment intermediary (*e.g.,* PayPal) using the phone or Internet.[126] The primary function of a cash reload mechanism is to provide a method for consumers to add money to their own prepaid cards and online accounts, or to transfer money to a relative or friend by supplying the authorization code that corresponds to the funds.[127] The consumer's relative or friend simply uses the authorization code to load the funds onto her own prepaid card or online account. Thus, the cash reload mechanism itself is not a general-use prepaid card that can be swiped or redeemed at a retail location or automated teller machine (''ATM'').

Fraudulent telemarketers demand or request payment by cash-to-cash money transfer and cash reload mechanism because they are essentially equivalent to a cash payment B once the money is picked up or offloaded from a prepaid card, there is virtually no chance for the sender to recover the money, obtain a refund, or even verify the identity of the recipient.[128] When a consumer is deceived into transferring money in these ways—particularly across national borders—a telemarketer can receive it anonymously. A cash-to-cash money transfer can be picked up at any one of multiple locations within minutes. Similarly, once a scam artist obtains the authorization code for a cash reload mechanism from a consumer over the phone, he can quickly load the funds onto an existing prepaid card and withdraw the funds immediately at an ATM. This makes it difficult to identify or track down the perpetrator of the fraud and return funds to defrauded consumers.

1. Existing Regulation of Money Transfers Fails to Protect Consumers Against Telemarketing Fraud

New federal remittance transfer rules, as well as existing federal and state laws pertaining to money transfers, are designed to regulate money transfer providers, not to protect consumers from telemarketing fraud. Specifically, the Remittance Transfer Rule is aimed at preventing money transfer providers from taking advantage of their customers, many of whom are foreign-born workers sending payments back to their home country.[129] As a result, the Rule's disclosure and error resolution procedures apply only to covered ''remittance transfers'' B those transfers that originate in the United States and are received in another country.[130] In addition, the definition of remittance transfer excludes cash reload mechanisms, which are not ''sent by a remittance transfer provider'' [131] to a ''designated recipient,'' [132] but instead are provided directly to consumers by a retailer at the point of sale. Moreover, the disclosure and error resolution procedures in the Remittance Rule focus on the transparency and accuracy of the transaction between the remittance sender and the remittance provider.[133]

[124] GAO Report, *supra* note 123, at 10–11.

[125] MoneyGram's Web site states: ''In the absence of a proper ID, test questions can serve as an identification method for most transaction[s] below a certain dollar amount. Test questions can be included in a transaction, and should address something only the receiver could answer.'' MoneyGram, *Money Transfers, Receiving a Money Transfer, What if my receiver doesn't have identification?, available at https://www.moneygram.com/wps/portal/moneygramonline/home/CustomerService/FAQs* (located under the ''MoneyGram'' tab and ''Receiving a Money Transfer'').

[126] Currently, Green Dot's MoneyPak is the only cash reload mechanism accepted by PayPal as a funding source. PayPal, *Now There's A New Way to Add Cash* to Your PayPal Account With MoneyPak, available at https://www.paypal.com/webapps/mpp/greendot-moneypak.*

[127] Green Dot also enables MoneyPak consumers to make same-day payments to certain billers using a MoneyPak. However, only approved billing partners are authorized to accept MoneyPak authorization codes directly from consumers as a method of payment. *See, e.g.,* GreenDot MoneyPak, *Where can I use a MoneyPak? available at https://www.moneypak.com/WhoAccepts.aspx.* In contrast, scam artists must load the funds onto a prepaid card before they can withdraw the money at an ATM or spend down the balance.

[128] Unlike cash-to-cash money transfers which can be completely anonymous, electronic fund transfers to and from accounts maintained at financial institutions or with online payment service providers require senders and recipients to open and maintain accounts, which may be identified and traced to a particular person or entity. *See, e.g.,* FFEIC, *Bank Secrecy Act Anti-Money Laundering Examination Manual, Customer Identification Program—Overview, available at http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_011.htm* (describing the Customer Identification Program rules requiring banks to obtain, at a minimum, the name, date of birth, address, and identification number from each customer before opening an account). Similarly, bank secrecy and anti-money laundering laws require issuers of prepaid cards to verify the identity of each prepaid cardholder. Fraudulent telemarketers, however, frequently register cards using the personal information of identity theft victims. *See infra* note 135 (discussing the new Prepaid Access Rule).

[129] Section 1073 of the Dodd-Frank Act mandated changes to the EFTA that resulted in some coverage of cross-border money transfers (*i.e.,* ''remittance transfers'' initiated in the United States and sent to recipients in other countries). In 2012, the CFPB issued the Remittance Rule in three parts to implement the remittance transfer provisions of the Dodd-Frank Act by adding a new Subpart B to Regulation E (12 CFR 1005.30–36). *Final Rule; Remittance Transfer Rule, Electronic Fund Transfers (Regulation E),* 77 FR 6194 (Feb. 7, 2012); *Technical Correction to Final Remittance Transfer Rule; Electronic Fund Transfers (Regulation E),* 77 FR 40459 (Jul. 10, 2012); *Final Remittance Transfer Rule; Official Interpretation,* 77 FR 50244 (Aug. 20, 2012). The Rule covers these cross-border remittance transfers, whether or not the sender holds an account with the remittance transfer provider and whether or not the remittance transfer is also an ''electronic fund transfer,'' as defined in section 903 of the EFTA.

On January 22, 2013, the CFPB announced that it would continue to temporarily postpone the original February 2013 effective date for the Rule until after the Bureau issued a new proposal to refine three elements of the Rule: ''(1) errors resulting from incorrect account numbers provided by senders of remittance transfers; (2) the disclosure of certain foreign taxes and third-party fees; and (3) the disclosure of sub-national, foreign taxes.'' David Silberman, CFPB, *Temporarily Delaying the Implementation of Our International Remittance Transfer Rule* (Jan. 22, 2013), *available at http://www.consumerfinance.gov/blog/temporarily-delaying-the-implementation-of-our-international-remittance-transfer-rule/;* CFPB, *CFPB Bulletin 2012–08 Re: Remittance Rule Implementation (Subpart B of Regulation E)* (Nov. 27, 2012), *available at http://files.consumerfinance.gov/f/201211_cfpb_remittance-rule-bulletin.pdf.* On April 30, 2013, the CFPB announced final revisions to the Rule with an effective date of October 28, 2013. The text of the final rule is available at *http://files.consumerfinance.gov/f/201211_cfpb_remittance-rule-bulletin.pdf.*

[130] 12 CFR 1005.30(e) (definition of remittance transfer).

[131] *Official Staff Commentary,* 12 CFR part 1005 (Supp. I), Comment 30(e)(2) (explaining that ''sent by a remittance transfer provider'' ''means that there must be an intermediary that is directly engaged with the sender to send an electronic transfer of funds on behalf of the sender to a designated recipient.'').

[132] *Official Staff Commentary,* 12 CFR part 1005 (Supp. I), Comment 30(c)(2)(iii) (clarifying that when a remittance transfer provider mails or delivers a prepaid card (for example) directly to the consumer, there is no ''designated recipient'' because ''the provider does not know whether the consumer will subsequently send the prepaid card to a recipient in a foreign country.'').

[133] Among other things, remittance transfer providers must disclose transfer fees and exchange rates, and provide error resolution procedures in

Continued

Thus, the Rule fails to ameliorate the need for restrictions on cash-to-cash money transfers and cash reload mechanisms in telemarketing, where a telemarketer fraudulently induces the consumer to initiate the money transfer or provide access to a cash reload mechanism.[134]

Similarly, other federal and state laws pertaining to cash-to-cash money transfers and cash reload mechanisms do not address the abuse of these payment methods by fraudulent telemarketers and con artists, and fail to provide consumers with the means to recoup their money once they discover the fraud. The Bank Secrecy Act and related laws target terrorism financing, tax evasion, and money laundering activity,[135] and state statutes provide licensing requirements for money transfer providers.[136] The proposed TSR ban on cash-to-cash money transfers and cash reload mechanisms would serve to close this regulatory gap and fortify the existing regulatory regime. The Commission's experience in combating telemarketing fraud operators that use these transfers to pocket consumers' money, and pursuing the third parties that assist and facilitate them, suggests that the use of these transfers in telemarketing is an unfair practice, and that prohibiting them would serve the public interest.

2. Survey Data Linking Cash-to-Cash Money Transfers to Telemarketing Fraud

The Commission has observed a striking correlation between cash-to-cash money transfers and telemarketing fraud through its survey of consumers who sent money transfers via MoneyGram, one of the largest commercial money transfer services in the United States. The FTC survey demonstrated that at least 79 percent of all MoneyGram transfers of $1,000 or more from the United States to Canada over a four-month period in 2007 were fraud-induced.[137] A similar survey of Western Union customers, conducted by Attorneys General in several states, concluded that approximately one-third of the person-to-person transfers of over $300 to Canada were fraud-induced.[138] The Western Union survey revealed that fraud-induced transfers represented 58 percent of the total dollars transferred by the surveyed consumers, and that the average transfer by a defrauded consumer was $1,500.[139]

In addition, the Commission, consumer advocates, AARP, and the Better Business Bureau have observed a significant increase in the number of scams involving cash reload mechanisms.[140] These schemes have involved payments made to cover taxes on purported lottery winnings, settle phony debts, pay for advertised goods and services, and obtain advance fee loans. Consumers have reported that telemarketers required them to purchase a cash reload mechanism from a local retailer and provide the authorization code as payment for the promised goods or services. With the authorization code in hand, the scam artist can quickly load the funds to existing prepaid card and withdraw the money at an ATM or by spending down the balance. Despite fraud warnings provided by two major cash reload networks on their Web sites [141] and packaging,[142] telemarketers engaged in fraud continue to extract money from consumers using cash reload mechanisms.

3. Law Enforcement Experience With Cash-to-Cash Money Transfers and Cash Reload Mechanisms Used in Telemarketing Fraud

The experience of the Commission and other federal and state law enforcers further documents the high risk to consumers and widespread injury caused by fraud-induced money transfers and cash reload mechanisms in inbound and outbound telemarketing. The Commission has sued telemarketers for using a variety of means to dupe or pressure consumers into sending cash-to-cash money transfers, including fake foreign lottery or sweepstakes prizes,[143] phony mystery shopper scams,[144] and

---

the event the provider transmitted funds in error (*e.g.,* to the wrong recipient or in the wrong amount). 12 CFR 1005.31–33. In addition, for covered remittance transfers, a provider must comply with a sender's timely request to cancel a transfer, as long as the funds have not been picked up by the recipient or deposited into an account held by the recipient. *Id.* at 1005.34.

[134] Unless the remittance provider commits an error (*i.e.,* sending the wrong amount, transferring to the wrong recipient, etc.), the victim of telemarketing fraud would have little recourse under the Remittance Rule.

[135] The Financial Crimes Enforcement Network (''FinCEN'') provides the following explanation of the Bank Secrecy Act regulations:

The Currency and Foreign Transactions Reporting Act of 1970 (which legislative framework is commonly referred to as the ''Bank Secrecy Act'' or ''BSA'') . . . requires [financial institutions] to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. It was passed by the Congress of the United States in 1970. The BSA is sometimes referred to as an 'anti-money laundering' law (>AML=) or jointly as >BSA/AML=. Several AML acts, including provisions in Title III of the USA PATRIOT Act of 2001, have been enacted up to the present to amend the BSA. (See 31 USC 5311–5330 and 31 CFR Chapter X [formerly 31 CFR Part 103]).

U.S. Department of Treasury, FinCEN, *Statutes & Regulations: Bank Secrecy Act, available at http://www.fincen.gov/statutes_regs/bsa/.* In 2011, FinCEN issued the Prepaid Access Rule, which amended the money services businesses rules of the Bank Secrecy Act regulations to mandate similar reporting and transactional information collection requirements on providers and sellers of certain types of prepaid access. *Final Rule; Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access,* 76 FR 45403–02 (Jul. 29, 2011).

[136] *See, e.g.,* Ariz. Rev. Stat. § 6–1202 (2011) (licensing requirements for money transfer providers); Kan. Stat. Ann. § 9–509 (2010 Supp.) (same).

[137] *FTC* v. *MoneyGram Int'l., Inc.,* Civ. No. 1:09–06576, § 27 (N.D. Ill. Oct. 19, 2009) (Stip. Perm. Inj.).

[138] The survey was conducted by the Attorneys General of North Carolina and six other states in 2003. Virginia H. Templeton & David N. Kirkman, *Fraud, Vulnerability and Aging, published in* 8 ALZHEIMER'S CARE TODAY 265–277 (2007), *available at http://www.ftc.gov/bcp/workshops/fraudforum/docs/ACTElderFraudArticle9-07.pdf.*

[139] *Id.*

[140] *See, e.g.,* 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;* 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.*

[141] On its Web site, Blackhawk Network, Inc. warns its REloadit Pack customers:

REloadit should ONLY be used to reload your prepaid cards or for accounts that YOU control.

Beware of any offers that do not accept a VISA or MasterCard payment and asks for you to purchase a REloadit Pack where you provide the REloadit Pack number and PIN in an email or over the phone.

Never use a REloadit Pack to pay for taxes or fees on foreign lottery winnings, grants, or any offer that requires you to pay first before getting something back.

REloadit, *Frequently Asked Questions: What is the best way to protect my REloadit Pack?, available at https://reloadit.com/faqs2.aspx#safe.* GreenDot Corporation includes similar warnings to consumers on its Web site. GreenDot MoneyPak, *MoneyPak FAQs: 7 Tips on How to Protect Yourself From Fraud, available at https://www.moneypak.com/ProtectYourMoney.aspx.*

[142] On the back of each MoneyPak card, Green Dot posts the following warning:

FRAUD ALERT: Use your MoneyPak number **only** with businesses listed at *moneypak.com.* If anyone else asks for your MoneyPak number, it's probably a scam. If a criminal gets your money, Green Dot is not responsible to pay you back. (Emphasis original.)

[143] *See, e.g., FTC* v. *Bezeredi,* Civ. No 05–1739 (W.D. Wash. Apr. 3, 2007) (Summ. J.); *FTC* v. *627867 B.C. Ltd.,* No C03–3166 (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.).

[144] In mystery shopping scams, fraud artists call U.S. consumers or send them direct mail in which they claim to be hiring consumers to visit well-known retail stores to evaluate MoneyGram's money transfer operations. The telemarketers send consumers a cashier's check, and instruct them to deposit it in their checking account and send most of the money back to the telemarketer using a cash-to-cash money transfer. By the time the counterfeit checks bounce, however, the scam artists have

work-at-home opportunities.[145] In some of the scams, wrongdoers used counterfeit checks to trick consumers into sending money back to them via money transfer.[146] In all of these cases, consumers received nothing in exchange for their payments, and had no ability to reclaim their money once they discovered the fraud.

For example, in the *Cash Corner* case,[147] the defendants sent letters to consumers with fake checks and instructions on how to claim a cash prize the consumers had purportedly won. When a consumer called, as instructed, to claim her prize, a Cash Corner representative directed her to deposit the check she had received, which appeared to be drawn on a legitimate U.S. bank in an amount ranging from $2,500 to $3,800. The representative then instructed the consumer to send Cash Corner a MoneyGram transfer to cover the fees or taxes associated with her ''winnings.'' Only after depositing the check and wiring the money, did consumers later find out that the checks they had deposited and had been posted to their accounts failed to clear because the checks were counterfeit. In some cases, instead of sending counterfeit checks, Cash Corner's telemarketers cold-called consumers and persuaded them to send the ''required'' taxes or fees in advance via money transfer to receive their prize winnings. Despite sending thousands of dollars via money transfers, none of these consumers received anything in return for their payments.

The Department of Justice and state Attorneys General also have targeted telemarketing operations that used fraud-induced money transfers to steal millions of dollars from consumers.[148] For example, in 2006 and 2007, the Department of Justice indicted 45 individuals involved in an enormous Costa Rican telemarketing scam targeting American senior citizens.[149] The defendants operating the scheme defrauded consumers of millions of dollars by telling them that each had won a large monetary prize in a sweepstakes contest. The telemarketers claimed they were from the ''Sweepstakes Security Commission'' and told consumers that to receive their prize, they had to send a money transfer to Costa Rica for a refundable ''insurance fee.'' The telemarketers made their calls from Costa Rica using Voice over Internet Protocol (''VoIP''), which disguised the originating location of the calls. To date, the case has yielded at least 34 guilty pleas and more than 280 years in combined prison sentences.

In some cases, the receiving agents of the money transfer company may be complicit in the fraud.[150] These agents have a strong financial incentive to continue facilitating such transactions despite unmistakable signs of fraud. In November 2012, the U.S. Attorney for the Middle District of Pennsylvania filed a criminal case against MoneyGram charging the company with knowingly and intentionally aiding and abetting wire fraud and failing to implement an effective anti-money laundering program from early 2003 through 2009.[151] The charges were based on MoneyGram's willful disregard of obvious signs that its money transfer network was being used by fraudulent telemarketers and other con-artists, including its own money transfer agents. To resolve the case, MoneyGram entered into a deferred prosecution agreement that, among other things, required the company to forfeit $100 million, undertake enhanced compliance monitoring procedures, and employ a corporate compliance monitor.[152]

The Commission previously sued MoneyGram, alleging that from 2004 through 2009, the company's money transfer agents helped fraudulent telemarketers trick U.S. consumers into sending more than $84 million to wrongdoers located in Canada and within the United States.[153] The Commission claimed that MoneyGram knew that its system was being used to defraud people but did very little about it, and that in some cases its agents in Canada actually participated in these schemes. MoneyGram agreed to a permanent injunction to settle the case, and paid $18 million which was distributed by the Commission to consumers.[154] Attorneys General in

already vanished with the money. *See, e.g.,* FTC Consumer Alert, *Mystery Shopper Scams* (Nov. 2012), *available at http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt151.shtm.*

[145] *See, e.g., FTC* v. *USS Elder Enters., Inc.,* Civ. No. 04–1039 (C.D. Cal. Jul. 26, 2005) (default judgment against defendants using telemarketing sales pitches and ads in various Spanish-language newspapers and magazines to lure consumers to transfer money for a bogus work-at-home opportunity, causing at least $885,196 in consumer injury).

[146] *See, e.g., United States* v. *Alexander,* Cr. No. 1:2008–00105 (D.R.I. Apr. 23, 2009) (defendant sentenced to a year in prison for participating in a $1.7 million fraud scheme in which wrongdoers sent victims counterfeit checks, instructed them to cash the checks, keep some of the money, and wire the balance of the money to the perpetrators of the scam). *See also Neovi, supra* note 97 (defendants' Internet-based business facilitated fraud by, among other things, creating unauthorized checks that malefactors could send to victims, instructing them to cash the checks, keep some of the money, and wire the balance back to the wrongdoer).

[147] *FTC* v. *B.C. Ltd. 0763496,* Civ. No. 07–1755 (W.D. Wash. Jan. 30, 2009) (default judgment against foreign lottery). The U.S. Attorney in Los Angeles filed a criminal action against *Cash Corner* defendant Odowa Roland Okuomose, who was arrested in British Columbia on November 6, 2007, on a U.S. warrant based on a criminal indictment for mail and wire fraud filed in federal court in Los Angeles. *See United States* v. *Okuomose,* Cr. No. 2:10–00507 (C.D. Cal. May 20, 2010). *See also* FTC Consumer Alert, *Customized Cons* (June 2002), warning consumers about calls from telemarketers posing as Customs agents and requesting payment by money transfer of taxes and fees in order to release a prize or package supposedly being held at the U.S.-Canada border for the consumer. The alert was prompted by the proliferation of the scheme, based on evidence collected by a U.S. Customs officer assigned to Project Colt in Montreal and confirmed by data compiled in the FTC's Consumer Sentinel system.

[148] *See, e.g., United States* v. *Porcelli,* Cr. No. 3:07–30037 (S.D. Ill. Oct. 29, 2007) (defendant sentenced to 13 years imprisonment for his role in an advance fee credit card telemarketing scheme that used money transfers to defraud individuals throughout the United States of approximately $12 million); Dep't. of Justice Press Release, *Four Defendants Indicted In Nigerian ''Advance-Fee'' Fraud Scam* (Mar. 23, 2006), *available at http://www.justice.gov/opa/pr/2006/March/06_crm_167.html*; Dep't. of Justice Press Release, *Eleven Arrested in Israel on U.S. Charges for Phony ''Lottery Prize'' Scheme that Targeted Elderly Victims in U.S.* (Jul. 21, 2009), *available at http://newyork.fbi.gov/dojpressrel/pressrel09/nyfo072109.htm.*

[149] A description of the cases and links to case summaries is available on the Department of Justice Web site at *http://www.justice.gov/criminal/vns/caseup/costarican.html.*

[150] *See, e.g.,* Press Release, U.S. Attorney for the Middle District of Pennsylvania, *Three Receive Prison Sentences, Nine Indicted in Continuing Federal Prosecution of Mass-marketing Schemes* (Mar. 1, 2012), *available at http://www.justice.gov/usao/pam/news/2012/MoneyGram_3_1_2012.htm* (announcing the sentencing of three Moneygram agents to imprisonment of up to 135 months and new indictments of nine others as part of investigation of fraudulent telemarketing schemes using MoneyGram and Western Union money transfer systems to defraud thousands of U.S. citizens); *Cash Corner, supra* note 147 (foreign lottery scheme perpetrated by defendant who was a money transfer agent); *Okuomose, supra* note 147 (indictment of defendant in *Cash Corner* for mail and wire fraud); *United States* v. *Asieru,* Cr. No. 2:09–00457– (C.D. Cal. Jan. 25, 2010) (former MoneyGram agent sentenced to 97 months in federal prison for his role in a scheme that bilked hundreds of victims out of more than $1.5 million in lottery scam); *United States* v. *Bellini,* Cr. No. 2:07–01402 (C.D. Cal. July 21, 2010) (guilty plea of defendant who was one of at least 22 defendants indicted on federal fraud-related criminal charges for their roles in a Canadian cross-border sweepstakes fraud; five of the defendants allegedly operated money transfer stores to which some of the victims were instructed to wire money).

[151] *United States* v. *MoneyGram Int'l, Inc.,* Cr. No. 1:12–291 (M.D. Pa. Nov. 9, 2012).

[152] *Id.*

[153] *FTC* v. *MoneyGram, supra* note 137.

[154] *Id.* MoneyGram's settlement with the Commission requires it to implement a comprehensive anti-fraud program and to provide important disclosures to consumers. As a part of this anti-fraud program, MoneyGram must conduct background checks on prospective agents; educate and train its employees about consumer fraud; and review and analyze transaction data to flag MoneyGram agents with any unusual or suspicious

Continued

forty-six states separately reached a settlement with MoneyGram requiring the company to implement an extensive anti-fraud program and notify consumers about fraud-induced money transfers.[155]

Similarly, in 2005, Attorneys General in forty-seven states and the District of Columbia entered into a settlement with Western Union, resolving allegations of consumer fraud involving the company's money transfer system.[156] The settlement required Western Union to pay more than $8 million for consumer education programs, take steps to discipline wayward agents, track fraud complaints, cancel transactions and refund fees (if the recipient had not yet picked up the money), and warn consumers about the risks of fraud-induced money transfers in telemarketing.

Although the Commission's law enforcement record primarily involves cash-to-cash money transfers, federal and state criminal authorities have prosecuted individuals who tricked consumers into providing the authorization codes for cash reload mechanisms over the phone.[157] Telemarketers engaged in fraud are using familiar tactics and schemes to induce consumers to provide cash reload mechanisms, including phony prizes or sweepstakes winnings, fake debt collection, and bogus sales of goods advertised online.[158] Cash reload mechanisms offer a quick and irreversible method of payment, and are subject to the same risks as cash-to-cash money transfers. The Commission, therefore, proposes that cash reload mechanisms should be treated in the same way as cash-to-cash money transfers.

4. The Use of Cash-to-Cash Money Transfers and Cash Reload Mechanisms in Telemarketing Is an Abusive and Unfair Act or Practice

The Commission has preliminarily determined that the use of cash-to-cash money transfers and cash reload mechanisms in telemarketing is an abusive practice under the TSR and an unfair act or practice in violation of Section 5 of the FTC Act because it causes or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits and is not reasonably avoidable.[159] First, there has been substantial injury to consumers resulting from the misuse of cash-to-cash money transfers in telemarketing, and the injury resulting from cash reload mechanisms is mounting. As survey data and recent law enforcement cases demonstrate, consumers have paid hundreds of millions of irretrievable dollars to fraudulent telemarketers and con artists via such transfers.

Second, this enormous economic harm is not outweighed by countervailing benefits to consumers or competition. Although the benefits of cash-to-cash money transfers and cash reload mechanisms in other contexts may be clear (*e.g.,* when sending money to family members located abroad and reloading a consumer's own prepaid debit card), the use of these payment methods in telemarketing appears to be unnecessary and to generate only harm to consumers. Today, there are numerous low-cost and electronic payment alternatives that offer the same or more convenience as cash-to-cash money transfers and cash reload mechanisms, but with better consumer protection features or, at the very least, that provide less anonymity for a wrongdoer. These payment alternatives may include credit cards, electronic fund transfers, such as debit cards (including certain prepaid debit cards), ACH debits, and the use of online payment intermediaries (*e.g.,* PayPal) to facilitate transfers from a consumer's online account balance. Despite the availability of these lower cost and time-saving payment alternatives, the Commission's law enforcement experience and consumer complaint data suggest that fraudulent telemarketers frequently request or demand payment by money transfers. ''[W]hen a practice produces clear adverse consequences for consumers that are not accompanied by an increase in services or benefits to consumers or by benefits to competition,'' the second prong of the unfairness test is satisfied.[160]

Finally, consumers cannot reasonably avoid the economic injury caused by the use of these types of payments in telemarketing. Telemarketers that direct consumers to pay via cash-to-cash money transfers and cash reload mechanisms effectively and deliberately deprive consumers of the anti-fraud monitoring, accountability, and dispute resolution rights of other payment methods. Given the complexity of regulations governing various payment methods, consumers do not understand the effect of the telemarketer's choice on their important consumer protections. Furthermore, the Commission's law enforcement record shows that telemarketers often use these payment mechanisms in connection with deceptive and high-pressure sales pitches, which are orchestrated to distract consumers from fully appreciating the risks associated with sending a cash-to-cash money transfer or providing a cash reload mechanism to a telemarketer.[161] Thus, the substantial and unavoidable injury to consumers resulting from the use of cash-to-cash money transfers and cash

money transfer activities. The settlement also requires MoneyGram to provide clear and conspicuous fraud warnings on the front of all its money transfer forms and on its Web site. These notifications urge consumers not to send money to strangers; describe the most common types of scams currently utilizing MoneyGram's money transfer system; and warn consumers that after the money is collected by the recipient, consumers cannot obtain a refund from MoneyGram even if the transfer was the result of fraud. The settlement also requires MoneyGram to cancel and refund money transfers if consumers claim the transfer was the result of fraud and if the recipient has not yet picked up the money.

[155] A copy of the 2008 Assurance of Voluntary Compliance between these states and MoneyGram can be found on the Web site of the Texas Attorney General at *https://www.oag.state.tx.us/newspubs/releases/2008/070208moneygram_avc.pdf.*

[156] *See, e.g.,* State of Alaska Department of Law Press Release, *Western Union Enters Agreement with Majority of States' Attorneys General to Fund a Consumer Protection Awareness Program Aimed at Reducing Risks of Fraudulent Wire Transfers* (Nov. 14, 2005), *available at http://www.law.state.ak.us/press/releases/2005/111405-WesternUnion.html.*

[157] *See, e.g., United States* v. *Moynihan,* 2:12–cr–00248–JAM (E.D. Cal. Jul. 31, 2012) (guilty plea to access device fraud involving use of MoneyPak to obtain money from victims); K. Dickers, News, *Couple gets prison time for ticket scam,* Coshocton Trib. (Feb. 9, 2012), *available at* 2012 WLNR 2797286; Jeremy Hunt, *Police Investigating Phone Scam in City,* Daily News-Rec. (Sept. 21, 2011), *available at* 2011 WLNR 22028079.

[158] *See, e.g.,* North Dakota Attorney General's Office, *Green Dot MoneyPak Card Scam Involving Phony Publishers Clearinghouse Calls* (Nov. 12, 2012), *available at http://www.ag.nd.gov/NewsReleases/2012/11-20-12.pdf*; Idaho Attorney General's Office, *Consumer Alert: Prepaid Cash Cards Lottery Scam Won't End With the First Loss* (Jul. 9, 2012), *available at http://www.ag.idaho.gov/media/consumerAlerts/2012/ca_07092012.html;* Oklahoma Attorney General's Office, *Attorney General Issues Green Dot Card Scam Warning* (Jun. 21, 2012), *available at http://www.oag.state.ok.us/oagweb.nsf/srch/DAFA7D5B8A59BDC98625 7A24007325B8?OpenDocument.*

[159] *See supra* notes 19–20 (discussing the Commission's use of its unfairness analysis when identifying certain telemarketing practices as abusive).

[160] *FTC* v. *J.K. Publ'ns, Inc.,* 99 F. Supp. 2d 1176, 1201 (C.D. Cal. 2000) *(citing FTC* v. *Windward Mktg., Ltd.,* 1997 WL 33642380, at *11 (N.D. Ga. 1997)).

[161] As the Commission explained in its 1980 Policy Statement on Unfairness: However, it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. . . . [Such cases] are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking.

Unfairness Policy Statement, *In re Int'l Harvester Co., supra* note 20, at *97.

reload mechanisms in telemarketing is not outweighed by the benefit to consumers or competition.

As discussed above, the enforcement experience of the Commission and other federal and state authorities, as well as consumer complaint evidence and industry guidance to consumers, indicate that telemarketers committing fraud engage in the prevalent and widespread use of cash-to-cash money transfers [162] and they are increasingly turning to cash reload mechanisms.[163] At the same time, the Commission wishes to explore whether there might be legitimate reasons that telemarketers use these payment methods instead of other available payment alternatives. To understand any potential problems posed for legitimate businesses by the proposed ban on the use of cash-to-cash money transfers and cash reload mechanisms, the Commission welcomes comments from the public in response to the questions posed in Section VIII. In particular, the Commission seeks information and data describing any type of legitimate commercial telemarketing transactions for which these payment methods are needed, including the types of products involved, whether the telemarketing calls are inbound or outbound, and whether the need is limited to certain groups of consumers—*e.g.,* those who do not have bank accounts. In addition, the Commission seeks information as to why these transactions could not be conducted using safer and less anonymous payment alternatives, including what additional costs, if any, would result from using such payment methods.

[162] Because of the well-documented abuse of money transfers in telemarketing, the Commission, law enforcement, and consumer advocates contend that consumers should never use money transfers to send money to a stranger or in response to a telemarketing offer. *See, e.g.,* FTC Videos, *Scam Watch: Money Transfer Scams* (Aug. 22, 2012), *available at http://www.ftc.gov/video-library/index.php/for-consumers/scam-watch/money-transfer-scams/1402334883001*; FTC Consumer Alert, *Money Transfers Can Be Risky Business* (Oct. 2009), *available at http://permanent.access.gpo.gov/gpo17968/alt034.pdf*; FBI, *Common Fraud Schemes, available at http://www.fbi.gov/majcases/fraud/fraudschemes.htm*; Texas Att'y Gen. Gregg Abbott, *Avoid Fraudulent Check-Cashing Scheme* (Aug. 2008), *available at http://www.oag.state.tx.us/agency/weeklyag/2008/0808ckcashing.pdf*; Kayce T. Ataiyero & Jon Yates, AARP, *Con men see an opportune time to prey on desperate public* (Jan. 1, 2009), *available at http://www.aarp.org/money/scams-fraud/info-01-2009/con_men_see_an_opportune_time_to_prey_on_a_desperate_public.html.*

[163] *See supra* notes 140–142 (alerts and consumer warnings about the risks of fraud-induced cash reload mechanisms in telemarketing schemes).

III. Abusive Telemarketing of Recovery Services

Telemarketers pitching ''recovery services'' contact consumers who have lost money, failed to win a promised prize, or never received merchandise purchased in a previous scam. They promise to recover the lost money, or obtain the promised prize or merchandise, in exchange for a fee paid in advance. After the fee is paid, consumers rarely receive the promised services or recoup their losses. To protect consumers from this abusive practice, the Rule prohibits any telemarketer or seller from requesting or receiving payment for such recovery services ''until seven (7) business days after such money or other item is delivered to that person.'' [164]

As originally proposed in the 1995 Notice of Proposed Rulemaking, the recovery services provision was not limited to the recovery of money or value lost as the result of a telemarketing transaction.[165] The provision was revised in the Final Rule, however, to address the concerns of several commenters, including one who opined that this section, as proposed, could impair the ability of newspapers to accept classified advertisements for lost and found items.[166] Moreover, at the time the original Rule was promulgated, the Commission's experience with recovery services was limited to the recovery of money lost through telemarketing fraud.[167] Thus, the scope of this provision was restricted to services claiming to recover money consumers lost ''in a previous telemarketing transaction.'' [168]

Since then, numerous advances in technology, including the widespread commercial use of the Internet, have increased the communication channels used by wrongdoers to defraud their victims.[169] Consumer complaints and the Commission's law enforcement experience reveal that such Internet transactions are susceptible to the same unfair and deceptive acts and practices as telemarketing transactions. For example, in 2011 the Department of Justice (upon referral from the Commission) sued Business Recovery Services and its principal, Brian Hessler, for allegedly telemarketing recovery services to consumers who lost money to business opportunity and work-at-home scams.[170] Although the defendants targeted victims of both online and telemarketing scams, the TSR counts of the complaint were necessarily limited to the victims of prior telemarketing fraud.

The Commission's Consumer Sentinel data show that the vast majority of companies identified in those complaints use the Internet to reach their victims. In 2012, for example, the Internet—including email and Web sites—was the method of contacting consumer victims in 50 percent of fraud complaints.[171] Similarly, in 2011 the Internet Crime Complaint Center (''IC3''),[172] a clearinghouse for receiving, developing, and referring complaints regarding Internet crime, reported receiving 314,246 complaints of online crime and fraud involving money loss, including work-at-home scams, non-delivery of merchandise, and auto-auction frauds.[173] Like victims of telemarketing fraud, consumers who lose money in these online schemes are susceptible to telemarketing pitches for advance fee recovery services.

Today, telemarketers selling recovery services are just as likely to obtain lists of victims of online scams as they are to obtain lists of victims of telemarketing fraud. In fact, telemarketers engaged in recovery frauds now can easily avoid the Rule's advance fee prohibition simply by targeting only victims of online scams. Moreover, as with the original provision, the impact of this proposed change would not be to ban the telemarketing of such recovery services,

[164] 16 CFR 310.4(a)(3).

[165] 1995 Notice of Proposed Rulemaking, 60 FR 8313, 8330 (Feb. 14, 1995).

[166] 1995 Revised Notice of Proposed Rulemaking, 60 FR 30406, 30416 (June 8, 1995).

[167] *Id.* During 1995 and 1996, the Commission initiated or settled lawsuits involving nearly a dozen recovery services operations. 68 FR at 4614 n.403. *See, e.g., FTC* v. *Meridian Capital Mgmt., Inc.,* Civ. No. S–96–63 (D. Nev. Nov. 20, 1996) (Stip. Perm. Inj.); *FTC* v. *Fraud Action Network, Inc.,* Civ. No. S–96–191 (D. Nev. July 30, 1996) (Default J.); *FTC* v. *Telecomm. Prot. Agency, Inc.,* Civ. No. 96–344 (E.D. Okla. Dec. 9, 1996) (Stip. Perm. Inj.).

[168] 16 CFR 310.4(a)(3).

[169] For example, Internet (E-commerce) sales accounted for 50.6 percent of the more than $260 billion of 2010 non-store merchandise sales, indicating how common such purchases have become. U.S. Census Bureau, *2010 E-commerce Multi-sector Report, Table 6—U.S. Electronic Shopping and Mail-Order Houses (NAICS 4541)—Total and E-Commerce Sales by Merchandise Line: 2010 and 2009* (May 10, 2012), *available at http://www.census.gov/econ/estats/2010/all2010tables.html.*

[170] *United States* v. *Business Recovery Services LLC,* Civ. No. 2:11–0390–PHX–JAT (D. Ariz. Apr. 15, 2011) (Prelim. Inj.).

[171] FTC, *Consumer Sentinel Network Data Book for January–December 2012,* at 9 (Feb. 2013), (''*2012 Consumer Sentinel Data Book*''), *available at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf.* In 2012, 608,958 (57 percent) of consumers reported this information in their Consumer Sentinel Network complaints. *Id.*

[172] IC3 is a joint operation of the National White Collar Crime Network and the FBI.

[173] IC3, *2011 Internet Crime Report, Appendix II,* at 2 (2011), *available at http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf.*

but instead would require telemarketers to abstain from requesting or receiving payment for recouping money, value, or non-delivered merchandise until seven business days after the consumer received the recovered money or merchandise.[174]

As the Commission determined in prior rulemaking proceedings, including in particular the 2002 Notice of Proposed Rulemaking, the abusive practices relating to recovery services meet the criteria for unfairness. The same analysis supports expanding the scope of the Rule's current restriction on when telemarketers can ask for and accept payment from consumers for recovery services. The Commission therefore proposes to amend section 310.4(a)(3) to prohibit telemarketers and sellers of recovery services from accepting advance fees from consumers who have lost money in any prior transaction until seven business days after the consumers receive the recovered money or item, without regard to whether the loss occurred in a telemarketing transaction, on the Internet, or through some other means or medium.

IV. Proposed Revisions

In view of changes in the marketplace, and the harmful ways in which unscrupulous telemarketers have adapted their schemes to take advantage of consumers, the Commission is proposing to amend the TSR in the manner and for the reasons discussed in Sections II and III above.[175] The Commission invites written comments on the proposed amendments, and, in particular, seeks answers to the specific questions set forth in Section VIII below to assist it in determining whether it should amend the TSR as proposed, and whether the amendments under consideration strike an appropriate balance between protecting consumers from deceptive and abusive telemarketing and imposing unnecessary compliance burdens on legitimate businesses.

In addition, as discussed below, the Commission proposes to amend the TSR to make explicit five requirements of the TSR that have been overlooked or inadequately understood by the industry. These proposed amendments would: (1) Expressly state 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); (2) clarify that any recording made to memorialize a customer's or donor's express verifiable authorization 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; (3) 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; (4) modify the prohibition against sellers sharing the cost of registry fees to emphasize that the prohibition is absolute; and (5) illustrate the types of impermissible burdens on consumers that violate section 310.4(b)(1)(ii) by denying or interfering with their right to be placed on a seller's or telemarketer's entity-specific do-not-call list. A related amendment would 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 section 310.4(b)(1)(ii) will disqualify it from relying on the safe harbor for isolated or inadvertent violations in section 310.4(b)(3).

A. Section 310.2—Proposed Amendments of Definitions

The proposed Rule would retain all of the definitions from the original Rule, as amended in 2010.[176] The Commission proposes adding four new definitions: ''remotely created check,'' ''remotely created payment order,'' ''cash-to-cash money transfer,'' and ''cash reload mechanism'' in connection with the proposed amendments to section 310.4(a)(9) and (10), which would prohibit telemarketers or sellers from using these payment methods in telemarketing.

The proposed Rule would define ''remotely created check'' as a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn. For purposes of this definition, account means an account as defined in Regulation CC, Availability of Funds and Collection of Checks, 12 CFR part 229, as well as a credit or other arrangement that allows a person to draw checks that are payable by, through, or at a bank.[177]

This definition is the same as the definition of ''remotely created check'' found in Regulation CC, 12 CFR 229.2(fff). The Federal Reserve Commentary to the 2005 amendments to Regulation CC clarifies that the inclusion of the phrase ''signature applied by, or purported to be applied by, the person on whose account the check is drawn'' refers to ''the physical act of placing the signature on the check.'' [178] This proposed definition thus includes unsigned checks that have been converted into electronic form, but excludes all *signed* checks, even those that have been converted into electronic form pursuant to Check 21 standards.[179]

The proposed Rule would define a ''remotely created payment order'' as a payment instruction or order drawn on a person's account that is initiated or created by the payee and that does not bear a signature applied, or purported to be applied, by the person on whose account the order is drawn, and which is cleared through the check clearing system. The term does not include payment orders cleared through the Automated Clearinghouse Network or subject to the Truth in Lending Act, 15 U.S.C. 1601 *et seq.,* and Regulation Z, 12 CFR part 1026.

This definition is limited to electronic payment orders that most closely resemble remotely created checks—payment orders that are unsigned, created by the payee, and sent through the check clearing system. Thus, a payment order sent through the ACH Network would not qualify as a remotely created payment order. Similarly, a payment order or electronic

---

[174] Lost and found advertisements are not likely to qualify for coverage under the Rule, which applies to sellers or telemarketers engaged in ''telemarketing,'' as defined in section 310.2(dd).

[175] Section IV of the preamble was edited to meet the requirements for official publication in the **Federal Register**. Text setting out verbatim proposed changes to the current TSR text can be viewed at *http://www.ftc.gov/os/2013/05/130521telemarketingsalesrulefrn.pdf.*

[176] In 2011, the Commission issued a technical amendment to make minor corrections to the text of TSR. *TSR Correcting Amendments,* 76 FR 58716 (Sept. 22, 2011), *available at http://www.gpo.gov/fdsys/pkg/FR-2011-09-22/pdf/2011-24361.pdf.*

[177] Regulation CC, 12 CFR 229.2(a).

[178] Commentary to Regulations J and CC, 12 CFR parts 210 and 229, at 8 (Nov. 21, 2005), *available at http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20051121/attachment.pdf* (''The term signature as used in this definition has the meaning set forth at U.C.C. 3–401. The term 'applied by' refers to the physical act of placing the signature on the check.''). *Id.* at 16. The Electronic Signatures in Global and National Commerce Act (''ESIGN Act''), 15 U.S.C. 7001 *et seq.,* governs, among other things, the acceptance of electronic signatures in contracts and many commercial transactions. The ESIGN Act, however, expressly exempts from coverage, among other things, negotiable instruments governed by the UCC. *Id.* at 7003(a)(3).

[179] Commentary to Regulations J and CC, *supra* note 178, at 16 (''A check that bears the signature applied, or purported to be applied, by the person on whose account the check is drawn is not a remotely created check . . . The definition of a remotely created check includes a remotely created check that has been reconverted to a substitute check.'').

check that is either initiated or signed by a consumer, for example, via a smartphone application, would not be covered by the definition because it is not created by the merchant and it is signed by the consumer.

The terms ''cash-to-cash money transfer'' and ''cash reload mechanism'' are referenced in proposed section 310.4(a)(10), which would prohibit telemarketers or sellers from accepting or receiving payment via a cash-to-cash money transfer or cash reload mechanism for goods or services or charitable contributions in telemarketing. The proposed definition of ''cash-to-cash money transfer'' is limited to transfers of cash—and excludes any transfers that are electronic fund transfers under the EFTA, and thus subject to the full protections of that Act, as amended by section 1073 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (''Dodd-Frank Act'').[180] Unlike the transfers covered by the new Remittance Rule, however, the proposed TSR provision includes no geographic limitations. Thus, the proposed ban against the receipt of such money transfers in telemarketing would extend to those sent within or outside of the U.S., whether or not such transfers are also covered by the Remittance Rule.

Accordingly, the Commission proposes to define ''cash-to-cash money transfer'' as 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 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 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.

The proposed definition of ''cash reload mechanism'' would include virtual deposit slips that enable consumers to convert cash into electronic form, so that it can be loaded onto an existing prepaid card or an online account with a payment intermediary, such as PayPal. As described above, the cash reload mechanism does not function as a prepaid card that can be swiped at retail locations or ATMs, and it is not intended for use in purchasing goods and services. To implement the proposed ban against the use of cash reload instruments in telemarketing, the Commission proposes to define ''cash reload mechanism'' as a mechanism that makes it possible 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 a person can use to add money to a general-use prepaid card, as defined in Regulation E, 12 CFR 1005.2, or an online account with a payment intermediary. For purposes of this definition, a cash reload mechanism (1) is purchased by a person on a prepaid basis, (2) enables access to the funds via an authorization code or other security measure, and (3) is not itself a general-use prepaid card.

B. Section 310.3(a)(3)(ii)—Proposed Amendment of Oral Verification Recording Requirements

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,'' unless payment is made by a credit or debit card. Section 310.3(a)(3)(ii) permits the use of an audio recording to produce the required verification of an express oral authorization, provided 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.[181]

Although 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, Commission staff have found that sellers and telemarketers often omit this information from their audio recordings, contrary to this provision's mandate to include it. In fact, the Commission's law enforcement record indicates that in some cases the omission has been intentional and has concealed from consumers the real purpose of the verification recording and the fact that they will be charged.[182]

Accordingly, in order to make explicit the requirement that a verification recording describe the goods, services or charitable contribution for which payment authorization is sought, the Commission proposes to amend section 310.3(a)(3)(ii) by adding a requirement that the telemarketer or seller include an accurate description, clearly and conspicuously stated, of the goods or services or charitable contribution for which payment authorization is sought.

C. Section 310.4(a)—Abusive Practices in Telemarketing

1. Proposed Section 310.4(a)(3)—Expansion of Advance Fee Ban on Recovery Services

To protect consumers from unscrupulous telemarketers that have adapted their methods to defraud consumers, the Commission proposes to expand the scope of the Rule's advance fee ban on recovery services. Accordingly, the text of the proposed amended section 310.4(a)(3) would be amended to eliminate the word ''telemarketing'' from the phrase ''previous telemarketing transaction''.

[180] *See supra* note 129 and accompanying text (explaining the new Remittance Transfer Rule).

[181] 16 CFR 310.3(a)(3)(ii). This section also specifies additional disclosures the seller or telemarketer must make and include in the recording; namely, the number of debits, charge 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 contraction 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. *Id.* at 310.3(a)(3)(ii)(A)–(G).

[182] *See, e.g., FTC* v. *Integrity Fin. Enters., LLC,* Civ. No. 8:08–914 (M.D. Fla. Dec. 5, 2008) (stipulated permanent injunction preventing corporate defendants from allegedly changing pre-sale description of promised general purpose credit cards in their verification recordings); *FTC* v. *NHS Sys., Inc., supra* note 93 (defendants used deception to obtain recorded verifications from defrauded consumers); *FTC* v. *Publishers Bus. Servs., Inc.,* Civ. No. 2:08–00620 (D. Nev. Apr. 7, 2010) (summary judgment against defendants that allegedly changed material terms of initial offer of free or low-cost magazine subscriptions in verification call); *FTC* v. *4086465 Canada, Inc.,* Civ. No. 10:4–1351 (N.D. Ohio Nov. 7, 2005) (stipulated permanent injunction preventing defendants from allegedly misrepresenting themselves as government or bank officials to obtain recorded authorizations after falsely representing that goods or services were free or would be charged in low monthly payments).

2. Proposed Sections 310.4(a)(9) and (10)—Prohibitions Against Use of Certain Retail Payment Methods

As discussed above in Section II, telemarketers engaged in fraudulent practices are exploiting the systematic and regulatory weaknesses of certain payment methods to siphon money from the consumers they defraud. The Commission's law enforcement experience demonstrates that neither the TSR's prohibition against false and misleading statements to induce payment,[183] nor its authorization requirements,[184] have prevented the substantial consumer injury that results from the use of remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms. In view of the significant consumer injury involved, and the alternative payment mechanisms now widely available that afford greater protections to consumers, the Commission has preliminarily concluded that the unavoidable harm associated with remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms in telemarketing outweighs the benefits to consumers or competition.

For these reasons, the Commission believes that section 310.4(a) of the Rule should be amended to include new subsections (9) and (10) that would provide that it is an abusive practice for a seller or telemarketer to engage in (1) creating or causing to be created, directly or indirectly, a remotely created check or 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 (2) 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.

D. Section 310.4(b)—Proposed Amendments of Do Not Call Provisions

1. Proposed Section 310.4(b)(1)(ii)—Amendment of Prohibition Against Denying or Interfering With A Consumer's Right to Opt-Out

Section 310.4(b)(1)(ii) 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.[185] Although the TSR Compliance Guide provides some examples of actions that ''deny or interfere with'' a consumer's right to be placed on such an entity-specific do-not-call list, such as harassing consumers who make such a request, hanging up on them, and failing to honor the request,[186] the Commission has received recurring consumer complaints about these very practices. The Commission also has received complaints about companies that require consumers to listen to a sales pitch before accepting a do-not-call request, requiring a person to call a different number to submit the request, refuse to accept such a request unless the consumer can identify the seller responsible for the call, and fail to honor a request because they neglected to ask for (or, where an automated opt-out system is used, give the consumer an opportunity to speak or key in) the telephone number that received the call.

In the Commission's view, all of these practices violate section 310.4(b)(1)(ii). Consumers are often uncertain about the identity of the seller on whose behalf a call is made. Even telemarketers with multiple clients are in a better position than consumers to determine from their calling lists or other call records the seller on whose behalf the call was made. The Commission believes there is no reason why a multi-client telemarketer could not determine which of its clients' calls prompted the request. Such a determination could easily be made, for example, by obtaining the telephone number of the consumer making the request.

Because telemarketers place calls pitching specific products on behalf of specific sellers, they obviously are in a better position than consumers to have or be able to obtain the information they need to honor a do-not-call request. Thus, the TSR places the burden of doing so squarely on the telemarketer. The telemarketer must be able to identify the seller on whose behalf it is placing a call. Consequently, if a telemarketer with multiple clients lacks the means to identify the sellers on whose behalf it has placed calls that result in do-not-call requests, the TSR withholds from such a telemarketer the benefits of the safe harbor provided by section 310.4(b)(3).

For these reasons, in order to make the prohibition more explicit and to put sellers and telemarketers clearly on notice of the practices it prohibits, the Commission proposes to amend section 310.4(b)(1)(ii) to prohibit sellers and telemarketers from 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; terminating a telephone call with a person making such a request; 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; or requiring the person to identify the seller making the call or on whose behalf the call is made.

In addition, in order to clarify that the burden of obtaining the information necessary to honor an opt-out request falls on sellers and telemarketers, the Commission proposes to amend Section 310.4(b)(3)(vi) as follows: 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.

2. Proposed Section 310.4(b)(1)(iii)(B)—Amendment of Outbound Call Ban Exception for Express Written Agreements and Established Business Relationships

The Commission proposes to amend section 310.4(b)(1)(iii)(B) to make it unmistakably clear that the burden of proof for establishing an express written agreement (''EWA'') or existing business relationship (''EBR'') falls on the seller or telemarketer relying on it. As exceptions to the general prohibition against outbound calls to consumers whose numbers are on the Registry, the EWA and EBR exemptions each provide a defense on which a seller or telemarketer is entitled to rely if—and only if—it can demonstrate that the exemption applies to the telemarketing calls it has made to consumers whose numbers are on the Registry. Reliance on either exemption thus serves as an affirmative defense to a Commission complaint alleging that a seller or telemarketer has placed calls to numbers on the Registry in violation of section 310.4(b)(1)(iii)(B). Accordingly, as the Commission has previously stated, the burden of proof of that

[183] 16 CFR 310.3(a)(4).

[184] 16 CFR 310.3(a)(3).

[185] 16 CFR 310.4(b)(1)(ii) (emphasis added).

[186] FTC, *Complying with the Telemarketing Sales Rule* (February 2011), *available at http://business.ftc.gov/documents/bus27-complying-telemarketing-sales-rule.*

affirmative defense falls on the seller or telemarketer asserting it.[187]

For these reasons, the Commission proposes to amend section 310.4(b)(1)(iii)(B) to clarify that calls are permitted to a person listed on the Registry only if the seller or telemarketer (1) 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 of that person; or (2) 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.

Although the Commission believes that the current TSR language is clear, and that no amendment therefore is necessary for transparency, the Commission also wishes to emphasize that neither the EWA nor EBR exception is available to sellers or telemarketers with respect to calls to numbers on the Registry resulting from the use of calling lists purchased from third-party list brokers. Section 310.4(b)(1)(iii)(B)(i) plainly states that an EWA is limited to the ''specific party'' from which a person listed on the Registry wishes to receive calls, permitting such calls only if 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 of that person.[188]

Similarly, section 310.4(b)(1)(iii)(B)(ii) states that an EBR is limited to the ''seller'' that has an EBR with a person whose number is on the Registry, allowing calls only if 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.[189]

Consequently, the use of calling lists obtained from a third-party for ''cold calls'' to consumers whose numbers are on the Registry is not permitted by either of these two exceptions to the prohibition against outbound calls to numbers on the Registry.

E. Section 310.6—Proposed Amendments of Exemptions to the TSR

Sections 310.6(b)(5) and (b)(6) of the TSR exempt consumer-initiated calls responding, respectively, to general media advertisements (such as ads appearing in newspapers or on radio, television, or the Internet), or to direct mail solicitations that clearly, conspicuously, and truthfully disclose all material information required by section 310.3(a)(1).[190] Each of these exemptions, however, excludes several types of offers that have been susceptible to fraud—advance fee loans, credit card loss protection plans, credit repair services, investment opportunities, business opportunities other than business arrangements covered by the Franchise or Business Opportunity Rules, debt settlement services, and prize promotions.[191] In addition, the Rule expressly excludes upsell transactions from each of these two exemptions.[192]

The Commission proposes to add four new exclusions to the general media and direct mail exemptions that would prohibit sellers and telemarketers from accepting payment by remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms. Specifically, these new exclusions would require telemarketers and sellers that receive inbound calls from consumers in response to general media advertisements and direct mail solicitations to comply with the proposed prohibitions on payment enumerated in sections 310.4(a)(9) and (10). Thus, the direct mail and general media exemptions would be available to a seller or telemarketer only if the seller or telemarketer did not accept these novel payment methods during an otherwise exempt inbound telemarketing call.

As discussed above, in the outbound or inbound context, remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms are fraught with fraud monitoring and consumer protection weaknesses, and have been misused to harm consumers. Given the widespread availability of other payment mechanisms for inbound telemarketers and sellers, the Commission believes there is no evident justification for limiting the protections of proposed sections 310.4(a)(9) and (10) to outbound telemarketing calls; however, the Commission seeks comment on that question in Section VIII and expects these proposed amendments will be among the topics examined in detail.

In sum, to implement the proposed changes discussed above, the text of the direct mail and general media exemptions in section 310.6(b) would be amended to exclude calls that do not comply with the new prohibition on accepting remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms.

1. Section 310.6(b)(7)—Proposed Amendment of Business Exemption

The exemption in section 310.6(b)(7) for telephone calls between a telemarketer and a business is designed to exempt only business-to-business solicitations. It has never been construed by the Commission to exempt calls to a business to solicit its individual employees to buy products or services for their own use, or to make a personal charitable contribution. Indeed, the Commission has permitted business telephone numbers to be listed in the National Do Not Call Registry, because, among other reasons, telemarketers who seek to circumvent the Registry have solicited employees at their places of business to buy goods or services such as dietary products, auto warranties, and credit assistance. Thus, in order to emphasize that this exemption is limited to business-to-business solicitations, the Commission proposes to amend the provision so that 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.

[187] Denial of Petition for Proposed Rulemaking, 71 FR 58716, 58723 & n.89 (Oct. 5, 2006); *see also* 71 FR at 58719; 2008 TSR Amendments, 73 FR at 51181.

[188] 16 CFR 310.4(b)(1)(iii)(B)(i).

[189] 16 CFR 310.4(b)(1)(iii)(B)(ii).

[190] Direct mail solicitations include, but are not limited to, postcards, letters, or other advertisements sent ''via facsimile transmission or similar electronic mail, and other methods of delivery in which a solicitation is directed to specific address(es) or person(s).'' 16 CFR 310.6(b)(6).

[191] Franchise Rule, 16 CFR part 436; Business Opportunity Rule, 16 CFR part 437.

[192] The Rule's definition of ''upselling'' encompasses any solicitation for goods or services that follows an initial transaction of any sort in a single telephone call—whether or not the subsequent solicitation is made by or on behalf of the same seller involved in the initial transaction. Thus, the Rule covers both internal and external upsells. 2003 TSR Amendments, 68 FR at 4596.

F. Section 310.8(c)—Proposed Amendment of Fee Sharing Prohibition

Section 310.8(c), which specifies the fees sellers and telemarketers must pay to access the National Do Not Call Registry, also prohibits them from sharing the cost of Registry access.[193]

The Commission adopted this prohibition to conform the TSR's fee requirements to the Do Not Call Registry fee provisions previously adopted by the Federal Communications Commission (''FCC''). The FCC provisions absolutely ban any sharing or division of costs for accessing the Do Not Call Registry,[194] and that was also the Commission's intent.

The Commission proposes to amend this prohibition to prevent any possibility that it might 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 wishing to share the cost of Registry access, contrary to the Commission's intent. Accordingly, the Commission proposes to clarify that 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.

V. Regulatory Flexibility Act

The Regulatory Flexibility Act of 1980 (''RFA'') [195] requires a description and analysis of proposed and final rules that will have a significant economic impact on a substantial number of small entities.[196] The RFA requires an agency to provide an Initial Regulatory Flexibility Analysis (''IRFA'') [197] with the proposed Rule and a Final Regulatory Flexibility Analysis (''FRFA'') [198] with the final rule, if any. The Commission is not required to make such analyses if a rule would not have such an economic effect,[199] or if the rule is exempt from notice-and-comment requirements.[200]

The Commission does not have sufficient empirical data at this time regarding the industry to determine whether the proposed amendments to the Rule may affect a substantial number of small entities as defined in the RFA. It is also unclear whether the proposed amendments to the Rule would have a significant economic impact on small entities. Thus, to obtain more information about the impact of the proposed rule on small entities, the Commission has decided to publish the following IRFA pursuant to the RFA and to request public comment on the impact on small businesses of the proposed amendments.

A. Description of the Reasons Why Action by the Agency Is Being Considered

As described in Section II above, the proposed 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 proposed amendments would clarify several TSR requirements in order to reflect longstanding Commission enforcement policy.

B. Succinct Statement of the Objectives of, and Legal Basis for, the Proposed Amendments

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

C. Description and Estimate of the Number of Small Entities To Which the Proposed Amendments Will Apply

The proposed 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.'' [201] For the majority of entities subject to the proposed amendments—sellers and telemarketers—a small business is defined by the Small Business Administration as one whose average annual receipts do not exceed $7 million.[202]

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 invites comment and information on this issue.

D. Description of the Projected Reporting, Recordkeeping and Other Compliance Requirements of the Proposed 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 proposed amendments impose any new disclosure, reporting, recordkeeping or other compliance burdens. Rather, the proposed amendments do no more than add to or revise existing TSR prohibitions and clarify existing requirements. The new prohibitions would: (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 proposed 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 existing TSR requirements to reflect Commission enforcement policy. These amendments would 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

[193] 16 CFR 310.8(c).

[194] 2003 TSR Amendments, 68 FR at 45136 n.27 (citing 47 CFR 64.1200(c)(2)(i)(E), as amended July 3, 2003).

[195] 5 U.S.C. 603(a), 604(a).

[196] 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).

[197] 5 U.S.C. 603.

[198] 5 U.S.C. 604.

[199] 5 U.S.C. 605(b).

[200] *See supra* note 195.

[201] 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.

[202] 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.*

by the Commission; (2) 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 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) the types of impermissible burdens on consumers that violate 16 CFR 310.4(b)(1)(ii) by denying or interfering with their right to be placed on a seller's or telemarketer's entity-specific do-not-call list. A related amendment would 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 16 CFR 310.4(b)(1)(ii) will disqualify 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 proposed amendments include telemarketers or sellers engaged in acts or practices covered by the Rule. The Commission does not believe that any professional skills would be required for compliance with the proposed amendments because the amendments do not impose any new reporting, recordkeeping, disclosures or other compliance requirements, and do not extend the scope of the TSR to cover additional entities. The Commission invites comment on this issue.

E. Identification, to the Extent Practicable, of All Relevant Federal Rules That May Duplicate, Overlap or Conflict With the Proposed Amendments

The FTC has not identified any other federal statutes, rules, or policies currently in effect that may duplicate, overlap or conflict with the proposed rule. The Commission invites comment and information regarding any potentially duplicative, overlapping, or conflicting federal statutes, rules, or policies.

F. Description of any Significant Alternatives to the Proposed Amendments

The Commission believes that there are no significant alternatives to the proposed amendments. Nonetheless, in formulating the proposed amendments, the Commission has made every effort to avoid imposing unduly burdensome requirements on sellers and telemarketers. To that end, the Commission has limited the applicability of the TSR to inbound calls that violate the proposed prohibitions on the use of remotely created checks and payment orders, cash-to-cash money transfers, and cash reload mechanisms, so that inbound marketers that comply with these prohibitions will remain otherwise exempt from the TSR's requirements. The Commission believes that the proposed 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.

The Commission seeks comments on the ways in which the proposed amendments could be modified to reduce any costs or burdens for small entities.

VI. Paperwork Reduction Act

The proposed amendments would 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.[203]

The new prohibitions on the use of remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms would 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. Although these inbound calls are now exempt from the TSR,[204] these proposed amendments would cover them only to the extent that one of the new proposed prohibitions is violated, but this would not trigger the TSR's disclosure or recordkeeping obligations.

The proposed expansion of the current TSR 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 proposed 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 do-not-call list. Nothing in this proposed amendment requires any disclosure or recordkeeping.[205] Likewise, the Commission believes that the five proposed technical amendments intended to make explicit the existing requirements of the TSR would not impose any new disclosure or recordkeeping obligations.

VII. Communications by Outside Parties to the Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding from any outside party to any Commissioner or Commissioner's advisor will be placed on the public record.[206]

VIII. Request for Comments

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before July 29, 2013. Write ''Telemarketing Sales Rule, 16 CFR Part 310, Project No. R411001,'' on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the public Commission Web site, at *http://www.ftc.gov/os/publiccomments.shtm*. As a matter of discretion, the Commission tries to remove individuals' home contact information from comments before placing them on the Commission Web site.

Because your comment will be made public, you are solely responsible for making sure that your comment does not include any sensitive personal information, such as anyone's Social Security number, date of birth, driver's license number or other state identification number or foreign country equivalent, passport number, financial account number, or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, do not include any ''[t]rade secret or any commercial or

[203] 44 U.S.C. 3501–3521. The PRA also addresses reporting requirements, but neither the TSR nor the proposed amendments present them.

[204] 16 CFR 310.6(b)(5)–(6).

[205] 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 proposed amendment nor the TSR requires them to do so.

[206] *See* 16 CFR 1.26(b)(5).

financial information which is obtained from any person and which is privileged or confidential,'' as provided in Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2). In particular, do not include competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

If you want the Commission to give your comment confidential treatment, you must file it in paper form, with a request for confidential treatment, and you have to follow the procedure explained in FTC Rule 4.9(c), 16 CFR 4.9(c).[207] Your comment will be kept confidential only if the FTC General Counsel, in his or her sole discretion, grants your request in accordance with the law and the public interest.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online. To make sure that the Commission considers your online comment, you must file it at *https://ftcpublic.commentworks.com/FTC/tsrantifraudnprm* by following the instructions on the web-based form. If this Notice appears at *http://www.regulations.gov/#!home,* you also may file a comment through that Web site.

If you file your comment on paper, write ''Telemarketing Sales Rule, 16 CFR Part 310, Project No. R411001'' on your comment and on the envelope, and mail or deliver it to the following address: Federal Trade Commission, Office of the Secretary, Room H–113 (Annex B), 600 Pennsylvania Avenue NW., Washington, DC 20580. If possible, submit your paper comment to the Commission by courier or overnight service.

Visit the Commission Web site at *http://www.ftc.gov* to read this NPRM and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before July 29, 2013. You can find more information, including routine uses permitted by the Privacy Act, in the Commission's privacy policy, at *http://www.ftc.gov/ftc/privacy.htm.*

[207] In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c), 16 CFR 4.9(c).

A. General Questions for Comment

The Commission invites members of the public to comment on any issues or concerns they believe are relevant or appropriate to the Commission's consideration of proposed amendments to the TSR. The Commission requests that comments provide factual data upon which they are based. In addition to the issues raised above, the Commission solicits public comment on the costs and benefits to industry members and consumers of each of the proposals as well as the specific questions identified below. These questions are designed to assist the public and should not be construed as a limitation on the issues on which public comment may be submitted.

1. What would be the impact (including any benefits and costs), if any, of the proposed amendments on consumers?

2. What would be the impact (including any benefits and costs), if any, of the proposed amendments on individual firms (including small businesses) that must comply with them?

3. What would be the impact (including any benefits and costs), if any, on industry, including those who may be affected by the proposed amendments but not obligated to comply with the Rule?

4. What changes, if any, should be made to the proposed amendments to minimize any costs to consumers or to industry and individual firms (including small businesses) that must comply with the Rule?

5. How would each change suggested in response to Question 4 affect the benefits that might be provided by the proposed amendment to consumers or to industry and individual firms (including small businesses) that must comply with the Rule?

6. How would the proposed amendments impact small businesses with respect to costs, profitability, competitiveness, and employment? What other burdens, if any, would the proposed amendments impose on small businesses, and in what ways could the proposed amendments be modified to reduce any such costs or burdens?

7. How many small businesses would be affected by each of the proposed amendments?

8. With respect to each of the proposed amendments, are there any potentially duplicative, overlapping, or conflicting federal statutes, rules, or policies that are currently in effect?

B. Questions on Specific Issues

In response to each of the following questions, please provide: (1) Detailed comment, including data, statistics, consumer complaint information, and other evidence, regarding the issue referred to in the question; (2) comment as to whether the proposed amendment adequately solves the problem it is intended to address, and why or why not; and (3) suggestions for additional changes that might better maximize consumer protections or minimize the burden on industry and on small businesses within the industry.

Novel Payment Methods: Remotely Created Checks, Remotely Created Payment Orders, Cash-to-Cash Money Transfers, and Cash Reload Mechanisms

9. Does the proposed definition of ''remotely created check'' adequately, precisely, and correctly describe this payment alternative? If not, please provide alternative language or suggestions as to how the Commission could improve the definition.

10. Does the proposed definition of ''remotely created payment order'' adequately, precisely, and correctly describe this payment mechanism? If not, please provide alternative language or suggestions as to how the Commission could improve the definition.

11. Does the proposed definition of ''cash-to-cash money transfer'' adequately, precisely, and correctly describe this payment mechanism? If not, please provide alternative language or suggestions as to how the Commission could improve the definition.

12. Does the proposed definition of ''cash reload mechanism'' adequately, precisely, and correctly describe this payment mechanism? If not, please provide alternative language or suggestions as to how the Commission could improve the definition.

13. Should the Commission amend the TSR to prohibit the use in telemarketing of remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms as payment options?

14. What, if any, systematic fraud monitoring exists for remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms?

15. What, if any, dispute resolution rights for consumers are provided in connection with remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms?

16. Are there widely available payment alternatives to remotely created checks, remotely created payment orders, cash-to-cash money

transfers, and cash reload mechanisms sufficient for use in telemarketing by consumers who lack access to credit or traditional debit cards? If not, please describe the reasons why these novel payment methods are necessary and the types of telemarketing transactions for which these novel payment methods are necessary, including the types of products or services involved, whether the telemarketing calls are inbound or outbound, etc.

17. What, if any, adverse effect would a prohibition on the use of remotely created checks and remotely created payment orders in telemarketing have on legitimate electronic bill payment transactions?

18. Do banks have any feasible way of distinguishing among traditional checks, remotely created checks, images of remotely created checks and remotely created payment orders flowing through the check clearing system?

19. Is it feasible to obtain systematic, centralized monitoring of the volume, use, or return rates of remotely created checks and remotely created payment orders flowing through the check clearing system?

20. Do payment processors and depositary banks typically receive additional fees when processing payments and returns for merchants with high return rates? Do they incur additional costs in dealing with merchants with high return rates? Please describe the nature and amount of any such fees and costs, including how the additional fees charged compare to the increased costs incurred by the payment processors and banks.

21. Do consumers generally understand the differences among different payment options for purchases with regard to their dispute resolution rights and ability to recover payments procured by fraud?

22. Are there legitimate uses for cash-to-cash money transfers and cash reload mechanisms in telemarketing? If so, please describe the reasons why such transfers are necessary and the types of telemarketing transactions for which such transfers are necessary, including the types of products involved, whether the telemarketing calls are inbound or outbound, and whether the need is limited to certain groups of consumers—*e.g.,* those who do not have bank accounts. In addition, please provide information as to why these transactions could not be conducted using alternative payment mechanisms such as electronic fund transfers or debit or credit cards, including what additional costs, if any, would result from using such payment alternatives.

23. What specific costs and burdens would the proposed prohibition on the use of remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms in telemarketing impose on industry and individual firms (including small businesses) that would be required to comply with the prohibition, or on consumers?

24. Is the harm caused by remotely created checks, remotely created payment orders, cash-to-cash money transfers, and cash reload mechanisms in telemarketing outweighed by countervailing benefits to consumers or competition? If so, please identify and quantify the countervailing benefits.

25. Are there other payment mechanisms used in telemarketing that cause or are likely to cause unavoidable consumer harm without countervailing benefits to consumers or competition that the Commission should consider prohibiting or restricting?

Advance Fees for Recovery Services

26. Is there any material difference between telemarketing sales and Internet sales that would require the use of advance fees for recovery services aimed at victims of Internet fraud?

27. What, if any, specific costs and burdens would the proposed expansion of the advance fee ban on recovery services impose on industry and individual firms (including small businesses)?

28. Please describe the types of businesses that seek advance fees for recovery services, and whether these businesses require significant capital or labor outlays prior to providing the services.

General Media Exemption

29. How many sellers and how many telemarketers that accept payment by remotely created checks, remotely created payment orders, cash-to-cash money transfers, or cash reload mechanisms solicit calls from consumers by means of general media advertisements?

30. What specific costs or burdens, if any, would the proposed exclusion from the general media exemption for calls to sellers or telemarketers that accept payment by remotely created checks, remotely created payment orders, cash-to-cash money transfers, or cash reload mechanisms impose on industry, on individual firms (including small businesses) that would be required to comply with the prohibition, or on consumers?

31. Does the TSR's general media exemption have so many exclusions that the Commission should consider eliminating the exemption entirely?

Direct Mail Exemption

32. How many sellers and how many telemarketers that accept payment by remotely created checks, remotely created payment orders, cash-to-cash money transfers, or cash reload mechanisms solicit calls from consumers by means of direct mail offers?

33. What specific costs or burdens, if any, would the proposed amendment to the direct mail exemption impose on industry, on individual firms (including small businesses) that would be required to comply with the prohibition, or on consumers?

34. Should the proposed changes to the direct mail exemption be limited to certain types of industries (or goods or services) that are susceptible to abuse?

IX. Proposed Rule

List of Subjects in 16 CFR Part 310

Telemarketing, trade practices.

For the reasons set forth in the preamble, the Federal Trade Commission proposes to amend 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 (ee) through (ii), and adding new paragraphs (f) through (g) and (cc) through (dd), 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 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 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* makes it possible 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 a person can use to add money to a general-use prepaid card, as defined in Regulation E, 12 CFR 1005.2, or an online account with a payment intermediary. For purposes of this definition, a cash reload mechanism:

(1) Is purchased by a person on a prepaid basis;

(2) Enables access to the funds via an authorization code or other security measure; and

(3) Is not itself a general-use prepaid card.

* * * * *

(cc) *Remotely created check* means a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn. For purposes of this definition, *account* means an account as defined in Regulation CC, Availability of Funds and Collection of Checks, 12 CFR part 229, as well as a credit or other arrangement that allows a person to draw checks that are payable by, through, or at a bank.

(dd) *Remotely created payment order* means a payment instruction or order drawn on a person's account that is initiated or created by the payee and that does not bear a signature applied, or purported to be applied, by the person on whose account the order is drawn, and which is deposited into or cleared through the check clearing system. The term does not include payment orders cleared through the Automated Clearinghouse Network or subject to the Truth in Lending Act, 15 U.S.C. 1601 *et seq.,* and Regulation Z, 12 CFR part 1026.

* * * * *

■ 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. Amending paragraph (b)(7)(ii)(B) by removing ''or'' from the end of the paragraph;

■ c. Amending paragraph (b)(8) by removing the final period and adding a semicolon in its place;

■ d. Adding new paragraphs (a)(9) and (10); and

■ e. Revising paragraphs (b)(1)(ii), (b)(1)(iii)(B), and (b)(3)(vi), 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 check or 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) * * *

(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) Calls to sellers or telemarketers that do not comply with the prohibitions in §§ 310.4(a)(9) or (10); or

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

[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.

(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), 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) 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) Calls to sellers or telemarketers that do not comply with the prohibitions in § 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 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 $54 for each area code of data accessed, up to a maximum of $14,850; 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.

Donald S. Clark,

Secretary.

[FR Doc. 2013–12886 Filed 7–8–13; 8:45 am]

BILLING CODE 6750–01–P