The Clearing House
At the Center of Banking Since 1853

THE FINANCIAL SERVICES ROUNDTABLE
Financing America's Economy

August 8, 2013

Via Electronic Delivery

Federal Trade Commission
Office of the Secretary, Room H-113 (Annex B)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Telemarketing Sales Rule, 16 C.F.R. Part 310, Project No. R411001

Dear Ms. Hobbs and Mr. Tregillus:

The Clearing House Association L.L.C. and The Financial Services Roundtable (collectively the "Associations") [1] respectfully submit this comment letter to the Federal Trade Commission ("FTC") in response to the FTC's notice and request for information regarding proposed amendments to the Telemarketing Sales Rule ("Proposed Rule").[2] Among other things, the Proposed Rule would amend the FTC's Telemarketing Sales Rule ("TSR") to prohibit sellers and telemarketers ("telemarketers") from accepting or requesting remotely created checks ("RCCs") and remotely created payment orders ("RCPOs").[3]

In addition to the comments in the letter, the Associations support the positions set forth in the letter from the Electronic Check Clearing House Organization commenting on the Proposed Rule (the "ECCHO comment letter").

I. Introduction

The Associations support the FTC's efforts to protect consumers from fraud and to enforce the laws and regulations providing consumers with protections against the bad actors that violate such laws. As part of an organization that clears and settles check images, ACH items, and wire transfers, The Clearing House has a vested interest in protecting the payments system from misuse. Similarly, the Financial Services Roundtable and the financial services companies it represents believe it is important that laws and regulations be targeted towards, and enforced against, "unscrupulous telemarketers" who withdraw funds from consumer accounts without authorization through the use of any payment method. However, the

[1] Information regarding each of the Associations is provided in Appendix A to this comment letter.
[2] Telemarketing Sales Rule, 78 Fed. Reg. 41200 (July 9, 2013).
[3] The Proposed Rule would also prohibit the use of cash-to-cash money transfers and cash reload mechanisms in telemarketing transactions, and make certain other changes to the TSR. The Associations' comments are limited to a discussion of the proposed prohibition on the use of RCCs and RCPOs.

Associations are deeply concerned by the breadth of the Proposed Rule, which would prohibit the use of RCCs and RCPOs by *all* telemarketers, both bad actors and honest businesses alike.

While we acknowledge that additional measures may be necessary to manage the risk of RCC and RCPO fraud in telemarketing, RCCs and RCPOs are not, in and of themselves, fraudulent payment mechanisms; they are also widely used for legitimate commercial purposes. The Associations believe that by focusing on particular payment *methods* rather than on the persons who misuse those methods, the FTC's approach is overly broad and potentially harmful to the U.S. payments system.

Specifically, we are concerned that the Proposed Rule will:

- not deter bad actors from initiating fraudulent transactions;
- create an unrealistic regulatory expectation that financial institutions or payment system operators police the ban on the use of RCCs and RCPOs when there is no technical means to do so;
- "taint" the use of RCCs and RCPOs by other industries in which these payment methods are widely used for legitimate purposes; and
- establish an unprecedented prohibition by a government agency on the use of a particular payment method by an entire category of merchant.[4]

Accordingly, the Associations urge the FTC not to adopt the Proposed Rule, and instead to address the misuse of RCCs and RCPOs through a targeted approach that is consistent with payment system regulation and does not eliminate the ability of legitimate businesses to use specific payment mechanisms. We believe that such an approach would include the following elements:

- *Reporting requirements*: The FTC should establish a requirement for telemarketers, or their non-depository payment processors,[5] to report to the FTC the return rates of the RCCs and RCPOs that each telemarketer originates or processes.

- *Use of existing FTC authority*: The FTC should continue to use its existing authority to bring enforcement actions against, and to increase the penalties imposed on, the wrongdoers over which the FTC has authority, particularly with respect to telemarketers that violate the "express verifiable authorization" requirement of the TSR and other persons who misuse payment methods.

[4] We note that payment networks may sometimes restrict the use of payment transaction types for certain merchants. However, as noted and further described in ECCHO's comment letter, such restrictions are market-driven, governed by agreements among the parties, and flexible to adapt over time to changing needs.

[5] We note that depository institutions, unlike non-depository institution payment processors, are currently subject to a variety of existing regulatory obligations regarding RCCs and RCPOs, as discussed in Section II. B. 1. of this comment letter. Depository institutions are also subject to routine examination by federal authorities for compliance with those regulatory obligations as well as consumer protection laws.

II. Discussion

A. Background

The TSR implements the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"), which instructed the FTC to adopt regulations prohibiting deceptive or abusive practices in telemarketing.[6] In issuing the Proposed Rule, the FTC states that it "preliminarily finds that the risks from using [RCCs and RCPOs] in telemarketing transactions exceed the benefits of permitting their use" and notes that these payment methods are frequently used in schemes to defraud consumers. Thus, the Proposed Rule would amend the TSR to identify the use of RCCs and RCPOs in inbound and outbound telemarketing transactions as an abusive, and thus, prohibited, practice.

1. Definitions of RCCs and RCPOs and Existing Effective Protections against Unauthorized Use

The FTC notes that an RCC is an unsigned paper check that is created by the payee. Like a traditional paper check, it instructs a drawee bank to make payment to the order of a designated payee. The Proposed Rule would define the term to mean "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." [7] This definition is the same as the definition of RCC found in Regulation CC, which was issued by the Board of Governors of the Federal Reserve ("Board").[8] With respect to RCCs, the FTC states that "[a]ny 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," which makes RCCs more susceptible to fraud than paper checks.

The FTC describes an RCPO as an "all-electronic" version of an RCC that, unlike an RCC, never exists in paper form. The Proposed Rule would define RCPO to mean "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."[9] The FTC states that "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

---

[6] 15 U.S.C. § 6101-6108. The Telemarketing Act provides the FTC rulemaking authority both with respect to certain specified practices, as well as other practices that the FTC determines to be deceptive or abusive.

[7] 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.

[8] 12 CFR 229.2(fff). The FTC notes that pursuant to Federal Reserve commentary to amendments to Regulation CC, this definition "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."

[9] The proposed definition goes on to state that 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."

processing via the check clearing system" and that RCPOs are "at least as susceptible to fraud as remotely created checks."

RCPOs, as entirely electronic items, are not legally checks, and, thus, are not legally eligible for clearing as checks. [10] Nonetheless, RCPOs are indistinguishable within electronic check clearing systems from RCCs, which are checks. Therefore, RCPOs clear as checks and, as a practical matter, are treated as RCCs for purposes of the warranties and claims discussed below.

RCCs, which the FTC refers to as a "novel payment method," are processed electronically through the check clearing system. Accordingly, this payment form is governed principally by state law under each state's equivalent of Articles 3 and 4 of the Uniform Commercial Code ("UCC"), which apply to the deposit and clearing of checks.[11] As further explained in the ECCHO comment letter, all states have uniformly enacted UCC 4-401, which provides that consumers are not legally responsible for checks that are not properly payable, including unauthorized RCCs .[12]

Moreover, a significant number of states have adopted a UCC warranty that requires the person transferring an RCC to warrant "that the person on whose account the item is drawn authorized the issuance of the item for which the item is drawn."[13] This warranty alters the long-standing loss allocation rule for paper checks, under both common law and the UCC, which places liability for unauthorized checks on the paying bank.[14] The shift in liability from the paying bank to the depositary bank under this new warranty for RCCs is "intended to establish an economic incentive for the depositary bank to monitor its customers and limit the introduction of unauthorized RCCs into the check clearing system."[15] The shift is premised on the view that

[10]For example, the Federal Reserve Banks revised Operating Circular 3, which governs their check clearing service, to provide that "[d]ata sent to a Reserve Bank in the form of an electronic item is not an "electronic item" unless the data was captured from a check. By definition, the check from which the data was captured must be paper." Federal Reserve Banks Operating Circular No. 3 (April 11, 2012), http://www.frbservices.org/files/regulations/pdf/operating_circular_3_07122012.pdf. Depositary institutions that send such "purported electronic items" to a Reserve Bank for processing are liable for the legitimacy of the items in that file. Operating Circular # 3 further states that a Reserve Bank "may reject a purported electronic item and reverse any provisional credit that may have been given for it."

[11] Article 3 of the UCC governs negotiable instruments, including checks. Article 4 of the UCC governs bank deposits and collections.

[12] Under the UCC, a bank that pays a check drawn on the account of a customer may charge the account for a check only if it is "properly payable" (i.e., authorized by the customer). UCC § 4–401. The UCC generally requires a paying bank to recredit the customer's account for the amount of any unauthorized check that it pays, providing consumers protection from unauthorized check transactions. Id.

[13] UCC § 3-416(a)(6); *see also* UCC § 4-207(a)(6). At least twenty states have adopted laws with similar warranty provisions in their state version of the UCC, including Minnesota, Arkansas, Nevada, California, Colorado, Hawaii, Idaho, Iowa, Maine, Missouri, Nebraska, New Hampshire, North Dakota, Oregon, Tennessee, Texas, Utah, Vermont, West Virginia, and Wisconsin.

[14] *See*, *e.g., Price v. Neal*, 97 Eng. Rep. 871 (K.B. 1762). Generally, liability for an unauthorized check will rest with the paying bank unless it returns the check to the bank of first deposit by midnight of the banking day after the check was presented to the paying bank. UCC §§ 4-301, 4-302.

[15] Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire and Availability of Funds and Collection of Checks, 70 Fed. Reg. 71218, 71219 (Nov. 28, 2005).

the bank of first deposit is in the best position to know its customer and to identify fraudulent or unauthorized RCCs.

In addition, RCCs are governed at the federal level by the Board's Regulation CC, which contains a similar transfer warranty (and resulting allocation of risk of loss) as the UCC.[16] The Board amended Regulation CC in 2005 to establish this warranty and stated that it believes that the warranty, which will encourage the bank of first deposit to conduct due diligence on its customers and monitor for fraudulent transactions, "provides effective protections against unauthorized remotely created checks while still allowing for the legitimate use of those checks."[17] Also, as explained in ECCHO's comment letter, Federal Reserve Operating Circular #3, which applies to all checks cleared through the Reserve Banks, and the ECCHO Rules, which apply to most other electronic image check clearing arrangements, provide complementary adjustment processes to facilitate RCC warranty claims between a consumer's bank and a bank of first deposit.[18] Thus, although the UCC and Regulation CC do not contain specific recredit procedures that a financial institution must follow, customers are not legally responsible for unauthorized RCCs under the UCC and there are inter-bank adjustment processes that enable and incent banks to recredit a consumer's account.

2. FTC's "Preliminary" Determination that Use of RCCs and RCPOs by Telemarketers is an "abusive" Practice under the TSR

The Telemarketing Act provides the FTC with authority to address by regulation those telemarketing acts or practices that it determines to be deceptive or abusive.[19] The FTC uses its traditional unfairness analysis under Section 5 of the FTC Act when identifying a telemarketing practice as abusive. Under this standard, an act or practice is unfair 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. The FTC states in the Proposed Rule that with respect to RCCs and RCPOs, it "preliminarily finds that the risks from using these payment methods in telemarketing transactions exceed the benefits of permitting their use."

In light of this standard, the FTC identifies a number of factors in support of its determination that the use of RCCs and RCPOs by telemarketers is an abusive practice under the Telemarketing Act. According to the FTC, the "novel payment methods" that would be banned under the Proposed Rule differ significantly from "conventional payment methods" (e.g., credit card, debit card, and automated clearinghouse ("ACH") debit transactions), which federal law subjects to a prescribed error resolution process and statutory limitations on a consumer's liability for certain transactions (under the Truth in Lending Act and Regulation Z (for credit card transactions) or the Electronic Fund Transfer Act and Regulation E (for debit card and ACH

[16] 12 C.F.R. § 229.34(d)(1).
[17] 70 Fed. Reg. 71218, 71220.
[18] The adjustment processes under Operating Circular #3 and the ECCHO Rules provide a 90 day period from the date of presentment during which a consumer's bank can assert the claim. Federal Reserve Banks Operating Circular No. 3, subparagraph 20.10. ECCHO Operating Rules, Adjustment #12, Appendix II.
[19] 15 U.S.C. § 6101-6108.

transactions)). In contrast, RCCs and RCPOs are "governed principally by state laws," which the FTC believes, "do not provide consumers with adequate recourse when unauthorized transactions or telemarketing fraud occurs." Moreover, the FTC is concerned that RCCs and RCPOs are cleared via check clearing networks that "provide little or no systematic monitoring to detect or deter fraud."

In addition, the FTC points out the increased incidence of RCC and RCPO use in fraudulent transactions initiated by telemarketers; and that the choice to process a transaction as an RCC or RCPO as opposed to via ACH is the merchant's not the consumer's, and therefore "[c]onsumers cannot reasonably avoid the injury" of fraudulent RCC or RCPO transactions. The FTC states further that RCCs and RCPOs are the payment methods that "offer fraudulent telemarketers the most accessible and anonymous method of extracting money from consumers and for which the [FTC] has a record of fraud."[20]

The Associations do not agree with the FTC's assessment that consumer protections with respect to unauthorized RCCs and RCPOs are inadequate or with the characterization of RCCs and RCPOs as an anonymous means of extracting money. As discussed above in Section II. A. 1. of this letter, consumers are not legally responsible for unauthorized RCCs under UCC § 4-401, and interbank warranties and adjustment processes exist that enable and incent banks to recredit a consumer's account in the event an unauthorized RCC transaction occurs. We further note that RCCs and RCPOs are not "anonymous" payment methods given that (i) checks (including RCCs and RCPOs) cannot be anonymously deposited since there must an account to which a deposit is credited and an identified owner of the account with a depository bank relationship and (ii) an RCC or RCPO must identify a payee in order for payment to be made. Moreover, with the advances in online and mobile banking services, many institutions provide their customers with the ability to view images of the checks (including RCCs and RCPOs) that post to their account, allowing the customer to quickly identify the payee of any unauthorized item.

B. The Associations' Concerns Regarding the Proposed Rule

The Associations support the FTC in its efforts to protect consumers from unauthorized transactions, and share its interest in eliminating fraudsters from the payments system. However, we are concerned by the FTC's approach, which focuses on particular payment methods as opposed to the wrongdoers who misuse them. We also believe that the Proposed Rule is unlikely to have the intended effect of providing consumers with additional protection from unscrupulous telemarketers.

---

[20] The FTC also refers to a letter signed by thirty-seven state Attorneys General that urged the Board to prohibit RCCs. However, this letter was sent prior to the amendments to Regulation CC, which created the new transfer warranties with respect to RCCs. Notably, in issuing the final rule to establish these warranties, the Board stated that it "believes its rule provides effective protections against unauthorized remotely created checks while still allowing for the legitimate use of those checks." 70 Fed. Reg. 71218, 71220.

1. Overly Broad Prohibition and Inconsistency with Existing Payment System Regulatory Regime

The Associations are highly concerned that the FTC is taking an overly broad approach in its attempt to deter fraudulent telemarketers. We believe that if the Proposed Rule were to be adopted, it would set a new and unhealthy precedent with respect to the regulation of payment systems and their participants. To elaborate, we are not aware of any other instance in which a regulatory agency prohibited the use of a particular payment method by a particular category of merchant. We are concerned that the Proposed Rule represents the creation of a new enforcement tool, namely, the denial of access to a legitimate payment method by an entire industry segment.

Moreover, prohibiting a payment type is inconsistent with the current regulatory regime which applies to the U.S. payment system. The current laws and regulations that seek to prevent misuse of the payment system do not prohibit specific payment methods but rather mandate risk management. For example, the Bank Secrecy Act ("BSA") and its accompanying regulations require, among other things, identification of persons who transfer value, reporting of certain transactions and events, screening of certain payments against named persons, implementation of anti-money laundering policies, and record keeping. Complementing these BSA requirements, banking regulators also seek to minimize misuse of payment systems by requiring upfront due diligence on entities that wish to originate payments through insured institutions, ongoing monitoring of the activities of such entities, including their return rates, and prompt action to stop improper activity when it is found. Examination and enforcement authority as well as prosecution powers supplement this statutory and regulatory regime.

In addition to these foundational risk management principles embedded in payment system regulation, financial institutions are also subject to guidance issued by federal banking regulators that obligates them to specifically manage the risks associated with their customers' use of RCCs and RCPOs and third party payment processors, including through up front due diligence and ongoing monitoring.[21] For example, guidance issued by the Federal Financial Institutions Examination Council ("FFIEC") emphasizes that "[a]s with all payment systems and mechanisms, a financial institution must also assume responsibility for an effective system of internal controls and ongoing account monitoring related to RCCs."[22] Similarly, guidance issued by the FDIC provides that "[f]inancial institutions should understand, verify, and monitor the activities and the entities related to the account relationship [with a payment processor]" that process RCCs on behalf of merchants. The guidance also provides that:

> "[f]inancial institutions should ensure that their contractual agreements with payment processors provide them with access to necessary information in a timely manner. These agreements should also protect financial institutions by providing for immediate

[21] *See, e.g.*, FDIC Revised Guidance on Payment Processor Relationships (January 31, 2012), http://www.fdic.gov/news/news/financial/2012/fil12003.pdf.

[22] FFIEC IT Examination Handbook – Remotely Created Checks, http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/payment-instruments,-clearing,-and-settlement/check-based-payments/remotely-created-checks.aspx.

account closure, contract termination, or similar action, as well as establishing adequate reserve requirements to cover anticipated charge backs."

Furthermore, the guidance indicates that "[f]inancial institutions that fail to adequately manage [relationships with payment processors] may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity and, thus, may be liable for such acts or practices." Thus, the FDIC states that "[f]inancial institutions should implement policies and procedures designed to reduce the likelihood of establishing or maintaining inappropriate relationships with payment processors used by unscrupulous merchants."

Additionally, last October FinCEN issued an advisory regarding risks associated with payment processors and specifically identified telemarketing and RCC transactions as having "relatively higher incidences of consumer fraud or potentially illegal activities."[23] The advisory suggests that financial institutions that have payment processing customers may need to update their anti-money laundering programs. Parallel to the FFIEC guidance, FinCEN also suggests that financial institutions perform initial and on-going due diligence on payment processors. The advisory also informs financial institutions that they may be required to file suspicious activity reports if they know, suspect, or have reason to suspect that a payment processor has conducted a transaction involving funds derived from an illegal activity, including consumer fraud.

These recent agency communications demonstrate that the financial and banking regulatory community is well attuned to the issues associated with telemarketers, payment processors, and RCCs. Additionally, the transfer warranties for RCCs under Regulation CC, which shifted liability for unauthorized RCCs to depository banks, has added a very effective economic incentive on top of the enhanced regulatory mandate for financial institutions to take steps to know and monitor their customers in order to prevent unauthorized RCCs from entering the payment stream. We believe financial institutions have paid careful attention to the new guidance and that there is a renewed focus on preventing abusive telemarketers from misusing the payment system.

Nevertheless, we recognize the FTC's recent experiences with the misuse of RCCs and RCPOs and understand its desire to use its authority to prevent future misuse in the telemarketing space. However, we believe that a more appropriate and effective approach to such prevention would be to require reporting to the FTC by telemarketers that issue RCCs and RCPOs or their non-depository payment processors as well as ongoing fraud monitoring by non-depository payment processors with respect to the activities of telemarketers. This would assist the FTC in identifying bad actors at earlier stages of misconduct.

We discuss this potential alternative in further detail in Section II. D. 1 of this letter.

2. Likelihood of Continuing Fraudulent Conduct

The FTC states that a prohibition on the use of RCCs and RCPOs in all telemarketing transactions would "close off this avenue to fraudulent telemarketers" and, thus, force them to

[23] FIN-2012-A010, Risk Associated with Third-Party Payment Processors.

use ACH Network or credit card systems that have central monitoring capabilities that can assist in the detection of fraudulent activity. However, this outcome is only possible if bad actors voluntarily comply with the prohibition or there is some operational means to enforce the prohibition.

With regard to bad actors complying with the prohibition, we think such a change in conduct is highly unlikely. The FTC notes that fraudsters that misuse RCCs and RCPOs do not comply with the TSR's existing express verifiable authorization requirement. We believe it is likely that the same criminal actors that violate the existing rules regarding express verifiable authorization would violate any new rules that the FTC enacts to prohibit the use of these payment mechanisms altogether.[24]

With regard to an operational means to enforce the prohibition, we note that there is currently no operational or technical means to block RCCs and RCPOs. As further explained in the ECCHO comment letter, RCCs and RCPOs do not have unique identifiers and even if they did, existing systems do not distinguish a telemarketer's RCC from a non-telemarketer's RCC. Accordingly, while the Associations support the efforts of the FTC to eliminate the fraudulent use of RCCs and RCPOs and to punish telemarketers that misuse these items, we believe that the current check clearing system does not operate in a manner that would allow the Proposed Rule to be effective in reducing fraudulent conduct.

3. Legitimate Uses of RCCs

The Proposed Rule would deprive legitimate businesses of a payment form that provides those businesses with certain advantages, including that RCCs are inexpensive, simple and provide same day funds availability for merchants and same day payment for consumers. RCCs are commonly used by merchants to provide a same day credit for a bill payment that is due (in order to promptly pay a bill that would otherwise be late if it was paid via ACH, a traditional paper check or in some other manner). Also, as the FTC noted in its notice of proposed rulemaking, ACH TEL entries can only be used when there is an existing relationship between a merchant and a consumer or when a consumer initiates a call to a merchant. [25] Hence, not all telemarketing transactions can be conducted via ACH. Further, we are concerned that by designating the use of RCCs and RCPOs by telemarketers an "abusive" practice, the Proposed Rule will "taint" these payment mechanisms and discourage their use by legitimate

[24] An existing provision of the TSR requiring "express verifiable authorization" is designed to mitigate the risk of the fraudulent misuse of certain payment methods in telemarketing transactions, including RCCs and RCPOs. Under this provision of the TSR, telemarketers must obtain a consumer's express verifiable authorization for all telemarketing transactions where the consumer's payment is made by a method other than a credit card subject to Regulation Z or a debit card subject to Regulation E. 16 C.F.R. 310.3(a)(3). The FTC states in the Proposed Rule, however, that it is concerned that the express verifiable authorization requirement has not adequately protected consumers against fraud when RCCs and RCPOs are used to make payment for a telemarketing purchase. Specifically, the FTC explains that its "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."

[25] NACHA Operating Rules § 2.5.15.

actors in other industries. Such an outcome could be harmful to consumers, particularly in situations where same day payment for the consumer and same day funds availability for the merchant are crucial.

C. FTC's Role in Enforcing Consumer Protections

We note that the FTC's enforcement authority with respect to participants in the payments system is limited to non-bank entities and does not extend to depository institutions. Historically, banking regulators have sought to penalize banks for allowing their non-bank, downstream payment processors to process fraudulent or unauthorized RCCs and RCPOs on behalf of retailers. However, given the increasing predominance of non-bank entities as frontline participants in the payments industry, the FTC's role as an enforcer of consumer protections is becoming more important. In its discussion of the Proposed Rule, the FTC highlights some of the successes it has had in bringing enforcement actions against bad actors.

While recognizing that there have been banks that have not met their regulatory responsibilities to stop fraudulent activity by their depositing customers when they became aware of the fraud, we believe that the instances of financial institutions knowingly facilitating fraudulent activity are extremely rare and have been ultimately addressed by the banking regulators.[26] Nevertheless, we understand the FTC's desire to prevent any further failures in the banking community from causing widespread harm to consumers in the future. Therefore we welcome the FTC's attention to and enforcement actions against non-bank wrongdoers who misuse payment methods.

However, we again stress that we do not believe that banning particular payment methods is an appropriate or effective approach to enforcing consumer protections or to preventing dishonest telemarketers from committing fraud. As such, we urge the FTC to focus on identifying and holding accountable the bad actors that engage in fraudulent acts, rather than enacting an industry-wide ban on particular payment methods that in and of themselves, are not per se abusive or fraudulent.

D. Suggested Alternative Approaches

1. Reporting Requirements

Rather than prohibiting the use of RCCs and RCPOs by telemarketers altogether, we believe the FTC should impose return reporting requirements on telemarketers and their processors that use RCCs and RCPOs. Successfully managing this risk and enforcing existing laws against wrongdoers will reduce the incidences of fraud against consumers while continuing to

[26] We note that in some cases even when a financial institution recognizes that a payment processor is engaged in suspicious activity, the processor may move its account relationship to a different institution before its account relationship is terminated. *See, e.g.,* FDIC Revised Guidance on Payment Processor Relationships (stating that "[f]inancial institutions should be alert for payment processors that use more than one financial institution to process merchant client payments or that have a history of moving from one financial institution to another within a short period. Processors may use multiple financial institutions because they recognize that one or more of the relationships may be terminated as a result of suspicious activity").

permit legitimate businesses to continue to use payment methods that are convenient, inexpensive and provide same-day funds availability.

We note that in its discussion of the Proposed Rule, the FTC recognizes that the development of fraud monitoring and detection systems has discouraged fraudulent telemarketers from using the ACH or credit card systems to defraud consumers. The FTC states that "telemarketers engaged in fraud face no effective impediment to their use of remotely created checks and remotely created payment orders." However, the FTC explains that "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."

Consistent with the efforts of operators of the ACH and credit card systems to reduce fraud, the Associations believe that expanding the "zone of increased scrutiny" to apply to RCC and RCPO transactions, by requiring telemarketers and non-depository payment processors that do business with telemarketers, to monitor and provide reports on the return rates of RCC and RCPO transactions, is a better way to protect consumers and to identify fraudsters that misuse RCCs and RCPOs. Such monitoring and reporting would help the FTC to determine when an investigation, enforcement action, or some other measure is warranted.

We note that this reporting requirement would need to address the use of return consolidators, which is a practice used by many legitimate businesses to have returned checks received by a different financial institution than the one at which the checks were deposited. Because the forward and return activity is split between different financial institutions, the use of return consolidators makes it difficult to determine if return rates are unusually high. Some unscrupulous payment processors will use return consolidators to "conceal high return or chargeback rates from originating financial institutions and regulators."[27]

Although the authority to require reporting of this type may not exist under Telemarketing Act , the FTC could require such reports under Section 6 of the FTC Act, which authorizes the FTC to "gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce" and to require persons, partnerships, and corporations to file "annual or special reports" … "furnishing to the [FTC] such information as it may require as to the organization, business, conduct, practices,

[27] FIN-2012-A010: Risk Associated with Third-Party Payment Processors (October 22, 2012), http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2012-A010.pdf. Recent guidance by the Financial Crimes Enforcement Network ("FinCEN") states that "Returned Check Consolidation Accounts are legitimate and commonly used by commercial enterprises to facilitate processing of returned checks. Recently, however, some Payment Processors have used these accounts to establish separate deposit accounts to disposition their returned check items for the purpose of making it difficult for financial institutions to identify and evaluate 'return/error' rates for the Payment Processor. In some instances, both the deposit account and the returned check consolidation account are held at the same institution but in different accounts. In other instances, the accounts are held at separate institutions. In either case, this account relationship structure severely inhibits a financial institution's ability to monitor and report suspicious activity."

management, and relation to other corporations, partnerships, and individuals of the respective persons, partnerships, and corporations filing such reports or answers in writing."[28]

2. Use of Existing FTC Authority

As noted in Section II. C. of this letter, we welcome the FTC's attention to and enforcement actions against non-bank wrongdoers who misuse any payment method. We believe that the Telemarketing Act and the TSR, as well as Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, provide the FTC with extensive authority to bring enforcement actions against bad actors that misuse RCCs and RCPOs. We encourage the FTC to continue to use this authority in a robust manner, particularly with respect to telemarketers that violate the existing "express verifiable authorization" requirement of the TSR. We believe that the FTC's role in protecting consumers from the misuse of payment methods is becoming increasingly important as nonbank entities become more predominant in the payments industry. Accordingly, the Associations would be in favor of increased financial penalties and other punitive measures as a tool to minimize the occurrence of unauthorized RCCs and the removal of unscrupulous telemarketing companies, and their principals, from the payment system.

III. Conclusion

In sum, while the Associations strongly support the FTC's goal of reducing fraud in the payments system and protecting consumers from unauthorized transactions, we are concerned by the particular approach the FTC has proposed and encourage the FTC to adopt a more targeted approach that focuses on bad actors, rather than particular payment methods.

Thank you for your consideration and review of our suggestions regarding the Proposed Rule. If you have any questions or wish to discuss our comments, please do not hesitate to contact us using the contact information provided below.

Yours very truly,

The Clearing House Association, LLC

/s/
Robert C. Hunter
Executive Managing Director and Deputy General Counsel
(336) 769-5314
Rob.Hunter@TheClearingHouse.org

The Financial Services Roundtable

/s/
Richard M. Whiting
Executive Director and General Counsel
(202) 289-4322
rich@fsround.org

---

[28] 15 USC § 46(a)-(b).

Appendix A – Association Descriptions

The Clearing House

Established in 1853, The Clearing House is the nation's oldest payments company and banking association. The Clearing House is owned by 21 of the largest commercial banks in America, which employ 1.4 million people domestically and hold more than half of all U.S. deposits. The Payments Company within The Clearing House clears and settles approximately $2 trillion daily, representing nearly half of the U.S. volume of ACH, wire and check image transactions. The Clearing House Association is a nonpartisan advocacy organization within The Clearing House that represents, through regulatory comment letters, amicus briefs and white papers, the interests of its owner banks on a variety of systemically important bank policy issues.

The Financial Services Roundtable

The Financial Services Roundtable represents 100 integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. Roundtable member companies provide fuel for America's economic engine, accounting directly for $98.4 trillion in managed assets, $1.1 trillion in revenue, and 2.4 million jobs.