NACHA
The Electronic Payments Association®

13450 Sunrise Valley Drive • Suite 100 • Herndon, VA 20171
Phone: 703-561-1100 • Fax: 703-787-0996
eMail: info@nacha.org
www.nacha.org

August 7, 2013

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

RE: Telemarketing Sales Rule, 16 CFR Part 310, Project No. R411001

Dear Sirs and Madams:

NACHA—The Electronic Payments Association[1] respectfully submits this response to the Federal Trade Commission ("FTC") on proposed amendments to the FTC's Telemarketing Sales Rule ("Proposed Rule"). NACHA has been aggressively working with the banking industry and regulatory and enforcement bodies to combat abuse of the Automated Clearing House ("ACH") Network by bad actors. We appreciate the acknowledgement of those efforts in the FTC's release accompanying the Proposed Rule (the "Release"). As the perpetrators of fraudulent transactions adjust to heightened risk management within the ACH Network, however, it is important that regulatory and enforcement agencies scrutinize and regulate the entities that misuse payments mechanisms such as remotely created checks and payment orders (collectively, RCCs"), as well as ACH payments. Payments rules organizations, such as NACHA, and federal and state payments laws define ways in which proper authorizations and liability allocations can protect consumers, and we should strive for a balance between risk mitigation and compliance cost, so that incentives are not created to route transactions through less secure systems with less robust consumer protections. We, therefore, support measured and balanced efforts to prevent abuse of check and image systems through the regulation of telemarketers, as well as RCCs if necessary.

NACHA Efforts to Combat Fraud

As the governing body for the ACH Network, NACHA's mandate includes the development of rules, procedures and tools that help protect the integrity of the ACH Network and prevent its use

[1] NACHA manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data. The ACH Network serves as a safe, secure, reliable network for direct consumer, business, and government payments, and annually facilitates billions of payments such as Direct Deposit and Direct Payment. Utilized by all types of financial institutions, the ACH Network is governed by the *NACHA Operating Rules*, a set of fair and equitable rules that guide risk management and create certainty for all participants. As a not-for-profit association, NACHA represents nearly 11,000 financial institutions via 17 regional payments associations and direct membership. Through its industry councils and forums, NACHA brings together payments system stakeholders to enable innovation that strengthens the industry with creative payment solutions. To learn more, visit www.nacha.org, www.electronicpayments.org, and www.payitgreen.org.

for fraudulent purposes. As the Release acknowledges, the very structure of the ACH Network allows for centralized fraud monitoring and controls that are not present in the processing of RCCs. For this reason, we think it is informative to describe in more detail those centralized rules, processes and tools that help mitigate fraud on ACH debit transactions, including those for transactions that are the most similar to RCCs.

For the past several years NACHA has expended considerable resources to enhance its centralized risk monitoring functions and the Rules infrastructure designed to control risk within the ACH system. For example, in 2008, NACHA adopted rules regarding return rate reporting that enable NACHA to actively police the return rates experienced by its Originating Depository Financial Institutions ("ODFIs"). Because a return rate for unauthorized ACH transactions in excess of one percent is a flag for potentially problematic activity, NACHA monitors for ODFIs, Originators and Third-Party Senders whose unauthorized return rate exceeds that threshold and then takes action to require the ODFI to reduce the return rate below the threshold (among other things). Failure to do so within thirty days can subject the non-compliant ODFI to sanction under NACHA's National System of Fines.

The National System of Fines also is an important centralized systemic process for rooting out bad actors within the system without regard to the unauthorized return rate threshold. When RDFIs experience claims of unauthorized transactions, they can raise the alleged violation of the NACHA Rules (which require that all entries be duly authorized) for adjudication under the National System of Fines. Thus, even if return rate thresholds have not been exceeded, when fraudulent activity is identified NACHA is able to take action against the responsible ODFI, which in turn must address the issue with its problematic Originators.

As the Release notes, the NACHA Rules also are attentive to variations in risk among different transactions types. This includes specific requirements for telephone-initiated transactions as well as a prohibition on sharing of certain customer information by Originators, Third-Party Service Providers and ODFIs for the purpose of initiating ACH debit entries that are not covered by the original authorization (so-call "data pass" transactions). Participating depository financial institutions also must conduct risk assessments and audits that are designed to ensure that policies, procedures and systems that support ACH transactions are kept up to date with regulatory and NACHA requirements as well as evolving risks in the commercial environment.

NACHA has been proactive in developing tools to help depository institutions manage risks within the ACH system. Two examples of these tools are the Terminated Originator Database and the Originator Watch List. The former is a centralized list of Originators and the Third Party Senders who have been terminated by their ODFIs. ODFIs that participate in this service can thus more easily identify entities who should be subject to heightened diligence to ensure that the customer is not a bad actor that is simply jumping from bank to bank as their problematic activities are identified. Similarly, the Originator Watch List attempts to identify Originators who should be subject to heightened scrutiny because of publicly available information indicating problems with the quality of the institution's ACH originations (including consumer or enforcement litigation, and evidence of excessive consumer complaints).

Finally, NACHA has amended the NACHA Rules to permit the use of ACH debits for two specific cases in which RCCs are also used. In 2010, NACHA adopted rules (that became effective in 2011) allowing for recurring payments to be authorized over the telephone. Prior to that, the Rules only permitted a telephone authorization for a single payment, and so businesses with a need to obtain authorization for recurring payments, such as insurance companies and utilities, could not use ACH payments for this purpose. The 2010 rule amendments also permit an Originator to obtain authorization to collect return fees, as allowed by applicable law, using an ACH debit. With these rule amendments, the NACHA Rules now allow for the use of the ACH Network, with controls, by legitimate businesses in these two instances where they might otherwise use RCCs.

<u>The Need to Address Regulatory Imbalances</u>

The activities described above have been successful at curtailing the incidence of unauthorized activity within the ACH system. For example, in the 3-year period following the implementation of the return rate threshold mentioned above, the overall unauthorized return rate within the ACH network dropped by 25 percent, from 0.04 percent of debit transactions to 0.03 percent. As the Release identifies, however, NACHA's success has in part driven bad actors to search for alternative payment methods that do not provide the same type of systemic oversight and regulatory or rules-based protections. Because RCCs are not monitored systemically (indeed, RCCs are difficult, if not impossible, for individual financial institutions to monitor as a class), fraudsters are able to use RCCs to evade the authorization requirements and strong protections that NACHA has implemented through the ACH system.

Moreover, the added compliance expense incurred by ODFIs to protect consumers and help combat fraud and abuse in the ACH system creates an unintended but very real economic incentive for even responsible players to consider using RCCs in the place of ACH transactions in some circumstances, thereby weakening the overall effectiveness of risk management through the ACH system. For example, although the *NACHA Operating Rules* were amended effective in 2011 to permit telephone authorization of recurring transactions, some Originators still use RCCs for recurring transactions in order to avoid required expenses of both the Regulation E and NACHA authorization requirements that apply to electronic ACH debits, and the possibility of receiving returns for an extended period. Among other things, as the Release notes, the Consumer Financial Protection Bureau has not yet addressed the question whether wholly electronic remotely created payment orders are electronic funds transfers subject to Regulation E. Most importantly, however, lack of Regulation E or *NACHA Operating Rule* - type protections for RCC transactions exposes RCCs to the types of heightened risks of fraud and abuse identified in the Release.

For these reasons, we believe that it is essential that the FTC and its sister agencies take appropriate action to mitigate the risks posed by RCCs and place that form of payment on more of an even regulatory playing field with ACH entries. Regardless of whether such action includes the preclusion of RCCs for specific transaction types as contained in the Proposed Rule, it is important that steps be taken to prevent the use of RCCs solely to avoid the risk mitigants and consumer protections that NACHA has worked hard to implement through the ACH Network. We recognize, however, as noted previously, that it is impossible for financial institutions receiving these transactions to identify this type of RCC and prevent it from posting. Therefore, increased scrutiny of the telemarketers themselves may be necessary.

Should the FTC ultimately adopt the Proposed Rule, it seems likely that bad actors would attempt to move activity online, as e-commerce is not covered by the telemarketing sales rule. The regulatory imbalance between RCCs and ACH debits also exists for online transactions, and would persist in that environment even with the adoption of the Proposed Rule.

* * *

Again, NACHA appreciates the opportunity to provide comments on the FTC's Proposed Rule. If you have any questions regarding our comments, please do not hesitate to call me at (703) 561-3943.

Sincerely,

/S/

William Sullivan
Senior Director and Group Manager
Government and Industry Relations

cc: Janet Estep, President, NACHA
Jane Larimer, General Counsel, NACHA