



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Bureau of Consumer Protection
Bureau of Economics

January 13, 2014

Dear Ms. Bondoc:

The staffs of the Federal Trade Commission's Bureau of Economics and Bureau of Consumer Protection (collectively, "FTC staff")¹ appreciate the opportunity to comment on the proposed revisions to the *NACHA Operating Rules* ("Rules"), as described in the *Request for Comment – ACH Network Risk and Enforcement Topics* ("RFC").² FTC staff supports NACHA's proposal and offers the following comments to assist NACHA in considering the potential impact of the proposed changes on consumers.

I. Introduction

On November 11, 2013, NACHA – The Electronic Payments Association ("NACHA") published proposed revisions aimed at improving the Automated Clearing House ("ACH") process by reducing the incidence of returned ACH transactions and decreasing the costs to receiving depository financial institutions ("RDFIs") associated with handling consumer complaints and returned transactions.

The Federal Trade Commission ("FTC" or "Commission") is an independent agency responsible for safeguarding consumers throughout nearly all segments of the economy, including jurisdiction over most nonbank entities.³ To fulfill its consumer protection mandate, the Commission enforces the Federal Trade Commission Act, 15 U.S.C. 41 - 58 ("FTC Act") and other laws that prohibit businesses from engaging in practices that are deceptive or unfair to

¹ These comments represent the views of the staff of the Federal Trade Commission's Bureau of Economics and Bureau of Consumer Protection. The letter does not necessarily represent the views of the Federal Trade Commission or of any individual Commissioner. The Commission has, however, voted to authorize us to submit these comments.

² On the same date, NACHA published a "related and complementary proposed Rule to improve ACH Network quality." NACHA, *ACH Network Risk and Enforcement Topics, Request for Comment and Request for Information, Executive Summary and Rules Description*, at 1 (Nov. 11, 2013), available at <https://www.nacha.org/page/request-comment>.

³ See 15 U.S.C. 44, 45(a)(2) (excluding from the Commission's jurisdiction several types of entities, including bona fide nonprofits, bank entities (including, among others, banks, thrifts, and federally chartered credit unions), and common carriers).

consumers. In addition, the Commission engages in policy research and advocacy, public education outreach, and rulemaking.

II. The Commission's Efforts to Combat Fraud in Payments Systems

For more than a decade, the Commission has engaged in a variety of efforts to address the critical role of nonbank payment processors and other intermediaries in providing the perpetrators of fraud with the means to access and obtain payment from consumers' accounts. These efforts include aggressive law enforcement and coordination with other federal agencies and regulators.

The Commission's law enforcement cases have halted allegedly fraudulent schemes responsible for debiting or attempting to debit more than \$300 million from hundreds of thousands of consumer bank accounts.⁴ Typically, the estimates of consumer injury do not reflect the full measure of harm inflicted on consumers, who expend time and resources fighting these illegal debits. In many cases, con artists have duped victims into revealing their financial account information to pay for fraudulent goods or services, apply for bogus payday loans, or obtain "free" products. In other cases, the FTC has charged that perpetrators obtained or reused lists of consumer bank account information and began debiting accounts of consumers without any contact whatsoever.⁵ The ability of these perpetrators to electronically extract money from consumer bank accounts severely undermines confidence not just in the marketplace, but in the financial institutions that safeguard our money.

To cut off the supply of money to fraudulent operations, the Commission's law enforcement actions have targeted a variety of nonbank payment processors and other intermediaries – so-called "gatekeepers" – that allegedly engaged in unfair acts and practices in violation of the FTC Act or provided substantial assistance to telemarketers in violation of the Telemarketing Sales Rule, 16 C.F.R. 310 (2013) ("TSR"). The Commission has pursued payment processors that processed ACH debits to siphon money from consumer bank accounts on behalf of merchant clients allegedly engaged in abusive or deceptive telemarketing.⁶ Many

⁴ See, e.g., *FTC v. Ideal Financial Solutions, Inc.*, Civ. No. 13-00143-MMD-GFW (D. Nev. Feb. 15, 2013 (Prelim. Inj.)) (alleging defendants made more than \$24 million in debits and attempted debits to consumer accounts via ACH, RCPOs, and credit card charges); *FTC v. FTN Promotions, Inc.*, Civ. No. 07-1279-T-30TGW (M.D. Fla. Dec. 30, 2008) (Stip. Perm. Inj.) (same, \$172 million and \$42 million alleged in contempt); *FTC v. Group One Networks, Inc.*, Civ. No. 09-0352 (M.D. Fla. Mar. 19, 2010) (Stip. Perm. Inj.) (alleging defendants debited or attempted to debit \$17 million from consumer accounts via ACH and RCCs).

⁵ See, e.g., *FTC v. Ideal Financial*, *supra* note 4; *FTC v. 3d Union*, Civ. No. 04-0712-RCJ-RJJ (D. Nev. July 19, 2005) (Default J.).

⁶ E.g., *FTC v. Your Money Access, LLC ("YMA")*, Civ. No. 07-5147 (E.D. Pa. Aug. 11, 2010) (Stip. Perm. Inj.) (alleging ACH and RCC payment processor unfairly debited or attempted to debit more than \$200 million from consumer accounts on behalf of fraudulent telemarketers); *FTC v. Global Marketing Group, Inc.*, Civ. No. 06-02272 (JSM) (M.D. Fla. 2006) (same, \$5.1 million); *FTC v. First American Payment Processing, Inc., et al.*, No. CV-04-0074 (PHX) (D. Ariz. Nov. 3, 2004) (Stip. Perm. Inj.) (settlement requiring defendants to pay \$3.9 million); *FTC v. Electronic Financial Group, et al.*, No. W-03-CA-211 (W.D. Tex. Mar. 23, 2004) (Stip. Perm. Inj.) (settlement requiring defendants to pay \$1.5 million).

unscrupulous merchants and their payment processors also have taken advantage of alternative payment methods. In response, the Commission has charged that various payment processors and intermediaries provided fraudulent merchants with access to: credit and debit cards,⁷ money transfers,⁸ unsigned demand drafts known as Remotely Created Checks (“RCCs”), and electronic versions of RCCs, known as Remotely Created Payment Orders (“RCPOs”).⁹

Regardless of the type of payment method used, the Commission’s cases have highlighted the numerous red flags that put the processors (and, in many cases, the processors’ banks) on notice of the high likelihood of illegal activity. These signs include unusually high rates of returned or reversed transactions (or chargeback rates in connection with credit cards); sales scripts or websites containing statements that are facially false or highly likely to be false; consumer complaints; and inquiries from law enforcement or regulators. In some cases, payment processors not only know about underlying law violations committed by their merchant clients, but also actively help their merchant clients avoid detection. For example, the Commission has alleged that certain payment processors have urged fraudulent merchants to switch from ACH debits to RCCs and RCPOs to avoid NACHA’s one percent threshold for unauthorized returns¹⁰ or used tactics to evade compliance monitoring systems designed to flag fraud.¹¹

The Commission also works closely with other agencies and bank regulators that scrutinize the crucial role that banks and payment processors can play in providing deceptive or

⁷ E.g., FTC Press Release, *FTC Settlements Crack Down on Payment Processing Operation that Enabled “Google Money Tree” Scammers to Charge Consumers \$15 Million in Hidden Fees “Process America”* (Nov. 18, 2013) (announcing proposed settlement against credit card payment processor); *FTC v. Loewen*, 2013 WL 5816420 (W.D.Wash. Oct. 29, 2013) (Summ. J.) (finding defendants’ activities, including credit card processing, violated the TSR); *FTC v. WV Universal Management, LLC*, Civ. No. 12-CV-1618 (M.D. Fla. June 18, 2012) (alleging credit card payment processor assisted and facilitated violations of the TSR); *Innovative Wealth Builders*, Civ. No. 13-CV-00123 (M.D. Fla. June 4, 2013) (same).

⁸ *FTC v. MoneyGram*, Civ. No. 09-6576 (N.D. Ill. Oct. 19, 2009) (Stip. Perm. Inj.) (resolving allegations that defendant allowed its money transfer system to be used for fraud).

⁹ E.g., *FTC v. Automated Electronic Checking, Inc. (“AEC”)*, Civ. No. 13-00056-RCJ-WGC (D. Nev. Feb. 5, 2013) (Stip. Perm. Inj.) (payment processor of RCCs and RCPOs); *FTC v. Landmark Clearing Inc.*, Civ. No. 4:11-00826 (E.D. Tex. Dec. 15, 2011) (Stip. Perm. Inj.) (payment processor of RCCs and RCPOs); *FTC v. YMA*, Civ. No. 07-5147 (payment processor of RCCs and ACH debits); *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) (Perm. Inj.) (Internet-based check creation and delivery service).

¹⁰ *FTC v. AEC*, *supra* note 9, Complaint ¶ 29 (defendants allegedly urged merchant clients to avoid NACHA’s threshold by switching from ACH debits to RCPOs); *FTC v. Landmark Clearing*, *supra* note 9, Complaint ¶ 23 (alleging that defendants expressly advertised their RCPO processing product as a less regulated alternative to ACH transactions).

¹¹ *Process America*, *supra* note 7 (alleging defendants used multiple merchant accounts, shell corporations, and a manipulation of transaction volume to help fraudulent merchant evade detection by credit card associations); *FTC v. AEC*, *supra* note 9, Complaint ¶ 58 (alleging defendants advised merchants to use different billing descriptors, customer service email accounts and phone numbers, as well as corporate names or DBAs, to “fly under the bank radar”).

fraudulent merchants with access to consumers' bank accounts through ACH debits, RCCs, RCPOs, and other payment methods.¹² For example, as part of the Consumer Protection Working Group of President Obama's Financial Fraud Enforcement Task Force led by the U.S. Department of Justice, the Commission coordinates with a broad coalition of law enforcement, investigatory, and regulatory agencies assembled to combat fraud in all aspects of the economy.¹³ One result of this coordination is the series of actions taken by the Commission, bank regulators, and federal prosecutors involving First Bank of Delaware,¹⁴ which culminated in a \$15 million civil penalty against the bank based on its origination of RCCs, RCPOs, and ACH debits on behalf of merchants and payment processors engaged in fraud.¹⁵

III. FTC Staff Supports NACHA's Proposals

FTC staff supports NACHA's proposal to strengthen its risk management oversight to reduce the incidence of returned ACH debits, including those that have been most closely associated with consumer fraud, and offers the following comments based on its experience in combating fraud. By improving the quality of ACH debits and origination practices, increasing oversight of payment processors, and expanding NACHA's enforcement authority, the Rules

¹² See, e.g., *In the Matter of Bay Cities Bank*, FDIC-13-026b (May 20, 2013) (consent order requiring, among other things, cessation of all third-party payment processing unless and until bank submits an approved plan showing adequate policies and procedures for oversight); *In the Matter of Meridian Bank*, FDIC 12-367b (Oct. 19, 2012) (same, unless and until bank completes comprehensive due diligence on each payment processor and its merchant-clients); *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.); see also *United States v. Payment Processing Ctr., LLC*, Civ. No. 06-0725 (E.D. Pa. Feb. 12, 2007) (Stip. Perm. Inj.) (alleging mail and wire fraud in connection with defendants' processing of RCCs).

¹³ A description of the Financial Fraud Enforcement Task Force and a list of participants is available at <http://www.stopfraud.gov/about.html>.

¹⁴ In July 2011, the Commission filed suit against Direct Benefits Group, LLC and its principals for engaging in an online payday lending scheme to debit consumers' bank accounts without their knowledge or consent. *FTC v. Direct Benefits Group, LLC*, 2013 WL 3771322 (M.D. Fla. July 18, 2013) (permanent injunction and \$9,512,172 judgment entered against defendants). The Direct Benefits defendants processed debits to consumer accounts through several payment processors, including Landmark Clearing, Inc. *Id.* at *10. In turn, Landmark Clearing established merchant accounts for Direct Benefits Group and other fraudulent merchants through First Bank of Delaware. In December 2011, the Commission entered into a stipulated permanent injunction against Landmark Clearing, based on its payment processing activities for Direct Benefits. *FTC v. Landmark Clearing*, *supra* note 9. At the same time, the Federal Deposit Insurance Corporation ("FDIC") entered into a Consent Order with First Bank of Delaware in which the bank agreed to terminate all E-Payment Programs, including the processing of RCCs and similar instruments. *In the Matter of First Bank of Delaware*, FDIC-11-669b, 2 (Dec. 3, 2011).

¹⁵ On November 19, 2012, First Bank of Delaware entered into a settlement with the U.S. Department of Justice, U.S. Attorney's Office for the Eastern District of Pennsylvania, which included a concurrent assessment of a civil money penalty of \$15 million with the FDIC and the Financial Crimes Enforcement Network. *United States v. First Bank of Delaware*, Civ. No. 12-65000 (E.D. Pa. Nov. 19, 2012); *In the Matter of First Bank of Delaware*, FDIC-12-306k (Nov. 16, 2012). In its civil complaint, the Department of Justice alleged that the bank violated the Financial Institutions Reform, Recovery and Enforcement Act by, among other things, debiting the bank accounts of consumer victims on behalf of fraudulent merchants and payment processors working with such fraudulent merchants. On October 23, 2012, the bank's shareholders approved the bank's dissolution.

described in the RFC have the potential to provide critical guidance for all ACH participants and protection for consumers.

NACHA's rules and guidelines already emphasize the responsibility of all ACH participants, including Originators (merchants), Third-Party Senders (payment processors), and Originating Depository Financial Institutions or "ODFIs" (merchants' banks), to monitor return rates and other suspicious activity in order to detect and prevent fraud in the ACH Network. For example, ACH participants must identify return rates for debits returned as unauthorized ("unauthorized returns") that exceed the industry average return rates, which NACHA publishes in quarterly NACHA newsletters. NACHA's rules require banks to report and investigate any merchant with an unauthorized return rate of one percent or above. To provide further guidance regarding acceptable origination practices, NACHA proposes to modify existing Rules concerning debit return rate thresholds used to trigger Network inquiries and enforcement proceedings.

A. Unauthorized Returns Threshold

First, NACHA proposes to reduce the threshold for unauthorized returns from one percent to 0.5 percent. In March 2008, NACHA first implemented the existing one percent unauthorized return rate threshold as part of the Network Enforcement Rule. At that time, NACHA also modified the structure and amount of fines imposed by the ACH Rules Enforcement Panel and enabled the initiation of a rules enforcement proceeding specifically targeting Originators or Third-Party Senders generating an excessive volume of unauthorized debits into the ACH Network. As these and other improvements to the Network Enforcement Rule and risk management have taken hold, the average unauthorized return rate experienced by the ACH Network in the aggregate has consistently declined, while the one percent threshold has remained static. To identify outliers with excessive unauthorized returns, the proposed threshold would account for the new, lower average unauthorized return rates experienced by the ACH Network. The average unauthorized return rate was 0.06 percent in 2005 but declined to 0.03 percent in 2012. NACHA's existing one percent threshold is now 33 times higher than the average unauthorized return rate for calendar year 2012.

FTC staff supports NACHA's proposal to lower the threshold for unauthorized returns. NACHA proposes to cut the rate to 0.5 percent, which NACHA estimates to be more than 16 times higher than the average unauthorized return rate for 2012.¹⁶ This change would provide a useful tool for payment processors, banks, and NACHA to identify conduct that falls substantially outside the norm that legitimate businesses experience. The Commission's law enforcement experience shows that businesses engaged in hiding their unlawful practices have worked to bring their return rates in alignment with the upper bounds of the one percent threshold.¹⁷ As a result, a decrease in the threshold will make it more difficult for these entities to go unnoticed.

¹⁶ RFC at 4.

¹⁷ *FTC v. AEC*, *supra* note 9, Complaint ¶ 29 (AEC's principal notified one client merchant "NACHA is going to a 1% threshold for unauthorized transactions . . ."); *FTC v. Landmark*, *supra* note 9, Complaint ¶ 23 (defendants

As a general matter, the debiting of consumer bank accounts via RCCs and RCPOs raises analogous concerns regarding authorization and fraud as ACH debits.¹⁸ Entities that debit consumer bank accounts using RCCs or RCPOs that are cleared through the check system should not be held by industry members to a dramatically different standard for return rates. As a result, FTC staff has looked to NACHA's guidelines when assessing the return rates of potentially fraudulent operations using RCCs and RCPOs. Staff has referenced NACHA's return rate thresholds in challenging the conduct of payment processors that allegedly advised fraudulent merchants how to fly under the bank's radar by employing tactics that manipulate and mask their clients' return rates for RCCs and RCPOs.¹⁹

In sum, the abuse of the one percent threshold rate suggests that lowering it to 0.5 percent, as NACHA proposes, could have a beneficial prophylactic effect in curbing fraud, by strengthening a useful tool to monitor for unusual spikes in unauthorized activity. As described below, elevated unauthorized return rates are not the only, or even necessarily the most significant, indicia of potential fraud, which is why FTC staff also supports NACHA's proposals to establish two additional return rate thresholds.

B. Data Quality Returns Threshold

Second, NACHA proposes to implement a 3.0 percent threshold for returns based on "account data issues" (*i.e.*, debits returned for invalid account numbers or an inability to locate the account). NACHA proposes the threshold, which is more than 10 times higher than the recent average of 0.28 percent, to address questionable origination practices or high risk activities that have increased costs and burdens on RDFIs, which must expend time and resources on each return. FTC staff commends NACHA for recognizing that account data return thresholds should be subject to regular scrutiny by ACH participants.

The Commission's experience confirms that a high rate of account data returns can be a reliable indicator of fraud.²⁰ This is because excessive account data returns frequently spike when an Originator uses a list of old consumer account information or attempts to randomly debit consumer accounts by phishing for account numbers.²¹ FTC staff supports the proposed threshold as an important component to NACHA's risk management and oversight of ACH participants.

charged with explicitly invoking NACHA's one percent threshold in advertising the benefits of RCPO processing for merchants at risk of higher return rates).

¹⁸ Expert Report of Elliott C. McEntee, at ¶ 44 (Oct. 1, 2008), filed in *FTC v. YMA*, *supra* note 6.

¹⁹ See generally, *FTC v. AEC* and *FTC v. Landmark Clearing*, *supra* note 9; *FTC v. YMA*, *supra* note 6.

²⁰ *FTC v. AEC*, *supra* note 9, Complaint ¶ 36 (describing similar returns for RCC and RCPO transactions returned); *FTC v. Landmark*, *supra* note 9, Complaint ¶ 45 (same).

²¹ Expert Report of Elliott C. McEntee, at ¶ 55 (Oct. 1, 2008), filed in *FTC v. YMA*, *supra* note 6.

C. Total Return Threshold

Third, NACHA proposes to set a 15 percent total return threshold for all ACH debits, regardless of the return reason code, as a trigger for further investigation and possible enforcement action. FTC staff commends NACHA for recognizing the importance of monitoring and flagging excessive total return rates, in addition to unauthorized and administrative return rates. In the Commission's experience, whenever an Originator's total return rate is significantly higher than the industry average, it is a strong indication of problematic business practices that warrant further investigation. Indeed, the Office of the Comptroller of Currency has advised that banks "should not accept high levels of returns regardless of the return reason."²²

FTC staff supports NACHA's proposal to implement a new return rate threshold, but urges NACHA to make clear that the threshold – whether it is set at 10 times the average industry total return rate of approximately 1.5 percent or lower – must not be used to condone rates below the threshold. As noted above, FTC staff is aware that fraudulent merchants and payment processors have interpreted NACHA's existing one percent unauthorized return rate trigger as a permissive threshold, concluding that any unauthorized rate that falls below one percent is acceptable.²³ Accordingly, it is imperative that NACHA explicitly state that the total return threshold does not represent an acceptable level of returns, but rather, the moment at which the most stringent level of scrutiny should be applied. Furthermore, NACHA should be clear that return rates below any of the established thresholds do not qualify as any sort of "safe harbor."

The Commission's law enforcement experience also demonstrates that perpetrators of fraud are increasingly employing techniques designed to mask and artificially reduce their actual return rates to avoid scrutiny. One of these tactics is the use of "micro-charges" to inflate the number of debit transactions used to calculate the rate of returns.²⁴ In one case, a processor allegedly advised its client to put through attempted debits multiple times even though each would be returned due to insufficient funds (or "NSF"), for the purpose of artificially masking the ratio of attempted debits to returns.²⁵ These and other tactics that manipulate return rates also

²² OCC Bulletin 2008-12 (emphasis added); see also *FFIEC BSA/AML Examination Manual, Third-Party Payment Processors – Overview*, 241 (Apr. 29, 2010) ("a bank should thoroughly investigate high levels of returns and should not accept high levels of returns on the basis that the processor has provided collateral or other security to the bank. . .").

²³ See *supra* note 17.

²⁴ For example, in *FTC v. Ideal Financial*, the Commission explained how the defendants allegedly manipulated return rates with penny debits and credits: "Defendants take multiple \$0.01, \$0.03, or \$0.04 debits from consumer accounts and then return them before debiting approximately \$30. Defendants refund all of the penny debits as a new, single transactions (presumably so it is not coded as a "return" by the financial institutions). This increases the total number of debits against the total returns for a particular merchant account, thereby lowering the total return rate." *FTC v. Ideal Financial*, *supra* note 4, Pl.'s Mem. Supp. TRO 11 (citations omitted).

²⁵ *FTC v. AEC*, *supra* note 9, Complaint ¶ 59c.

should be considered by NACHA in setting the appropriate threshold for total returns, unauthorized returns, and data quality returns.

Finally, FTC staff encourages NACHA to monitor carefully the reactions to changes in any of the thresholds and to stand ready to make further adjustments as suggested by additional data.

D. Additional Proposals to Improve Network Risk and Enforcement

NACHA outlines additional initiatives to complement the proposals on returns thresholds. In general, FTC staff supports NACHA's efforts to implement improvements that will aid in the prevention and detection of fraud, provide NACHA with stronger enforcement tools, and streamline the compliance reporting process.

IV. Conclusion

FTC staff appreciates the opportunity to comment on the NACHA RFC and encourages NACHA to adopt the proposed rules.

Respectfully submitted,

Jessica L. Rich, Director
Bureau of Consumer Protection

Martin Gaynor, Director
Bureau of Economics