National Consumer Law Center
Fighting Together for Economic Justice

NATIONAL HEADQUARTERS
7 Winthrop Square, Boston, MA 02110
(617) 542-8010

WASHINGTON OFFICE
Spanogle Institute for Consumer Advocacy
1001 Connecticut Avenue, NW, Suite 510
Washington, DC 20036
(202) 452-6252

NCLC.ORG

June 15, 2023

Submitted online
Nacha
2550 Wasser Terrace, Suite 400
Herndon, Virginia 20171

Dear Sir or Madam,

Re: Request For Comment - ACH Risk Management 2023

Thank you for the opportunity to submit comments on proposals to amend the Nacha Operating Rules as part of implementing NACHA's Risk Management Framework objectives.

Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law and policy to work for consumer justice and economic security for low-income and other disadvantaged people in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law publications; litigation; expert witness services, and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness. NCLC publishes a series of consumer law treatises, including Consumer Banking and Payments Law.

Overview

We support the proposals and make some suggestions for strengthening them. In particular, we support the ability of originating depository institutions (ODFIs) to reverse fraudulently induced credit entries and the emphasis on the responsibilities of receiving depository financial institutions (RDFIs) in connection with fraudulently induced credit push payments. Reverse entries are an important mechanism to remedy fraudulent transactions and prevent the fraudster from keeping stolen funds. Greater direct responsibilities for RDFIs are also important, as RDFIs hold the accounts of the bad actors involved in perpetuating the fraud schemes, and RDFIs have a duty to ensure that those accounts are not used for unlawful purposes. As a result, RDFIs play a

critical role in enabling fraudsters to receive stolen funds and must play a bigger role in stopping and remedying frauds.

NCLC has an interest in ensuring that the ACH Network is safe for consumer use and that consumers are protected from the exploding incidence of fraud, scams, and schemes. Consequently, NCLC wholeheartedly supports NACHA's proposed objectives to increase awareness of fraud schemes that utilize credit-push payments; reduce the incidence of successful fraud attempts; and improve the recovery of funds after frauds have occurred.

Proposed Amendments No. 1 and No. 2

NCLC applauds NACHA's efforts to address fraud, particularly its focus on the role RDFIs play in credit push fraud. Rather than hope that vulnerable consumers will protect themselves, a much more effective way to ensure that payment systems are safe for consumers is to incentivize those designing and operating the system to use all available tools to make the system safe. Both ODFIs and RDFIs have important roles to play in achieving all three of NACHA's identified objectives, yet the role of RDFIs has been especially overlooked. RDFIs should ultimately bear responsibility when their customers commit fraud. Loss-prevention systems are far more effective in limiting fraud losses than simple warnings to consumers, and when required, will lead institutions to invest in ever-improving fraud detection and prevention systems that stop losses before they happen.

As such, we support proposed amendments to (1) expand the existing requirement for commercially reasonable fraud detection to other parties in the ACH network to non-Consumer Originators, ODFIs, Third-Party Service Providers, and Third-Party Senders and (2) require RDFIs to establish commercially reasonable fraud detection systems to monitor received ACH credit transactions.

As NACHA explained, other parties in the ACH network, especially RDFIs, may be in a better position to detect and stop fraud than ODFIs. These other parties must do their part to keep the payment system safe. This is especially true considering RDFIs are already required to comply with know-your-customer (KYC) and anti-money laundering (AML) obligations to ensure that accounts are not opened with fraudulent identities and that an institution's customers are not using an account for illegal purposes.[1]

RDFIs, whose customers fraudulently received funds to which they were not entitled, should bear more responsibility for fraudulent payments. Imposing liability on the receiving institution – even if it cannot recover from its customer – will incentivize RDFIs to adopt more effective fraud prevention systems that will prevent losses in the first instance and also aligns with their existing "Know Your Customer" (KYC) obligations under the Bank Secrecy Act (BSA) and anti-money laundering (AML) requirements.

[1] *See* Federal Fin. Inst. Examinations Council, Authentication and Access to Financial Institution Services and Systems (Aug. 11, 2021). This guidance, as well as others mentioned, identify the myriad of ways that institutions should be monitoring and protecting themselves from "high risk users" and potential threats to security.

At a minimum, requiring RDFIs to use commercially reasonable fraud detection methods is both manageable and proportionate to the anticipated benefit of fraud prevention on the ACH network. Because RDFIs already have a responsibility to prevent their customers from committing fraud, requiring them to use commercially reasonable fraud detection methods also leads to the additional benefit of improved compliance with KYC/AML rules. It also advances the Risk Framework objective to reduce the incidence of successful fraud attempts.

Institutions also use commercially reasonable fraud detection to comply with other legal obligations under the Electronic Funds Transfer Act and its implementing regulations. In this modern era of big data, artificial intelligence, and machine learning, we know that institutions that bear the cost of losses from fraud or errors will develop or seek sophisticated, ever-improving methods of detecting and limiting those losses.

Many vendors are eager to assist with fraud prevention for RDFIs. For example, NICE Actimize recently published a report IFM-X Mule Defense: Real-Time Money Mule Coverage Across the Customer Life Cycle highlighting its approach to identify and stop money mule activity.[2]

Accordingly, NACHA's proposal to require RDFI's to monitor incoming credits is an important first step in enhancing the role of RDFIs in fraud prevention and detection.

ACH participants should also be required to report detected incidents of fraud to NACHA and their bank regulator, including the volume and value of fraudulent ACH payments. This will further the Risk Framework objectives of increased awareness of fraud schemes that utilize credit-push payments. It will also ultimately lead to the reduction of successful fraud attempts because both FIs and regulators will have the data needed to detect patterns of fraud schemes, identify red flags pursuant to those schemes, and pursue the actors perpetuating the fraud.

Proposed Amendments No. 3 and No. 4

NCLC generally supports proposed amendment No. 3 that allows an RDFI to use code R17 to return an entry it thinks is fraudulent. We also support proposed amendment No. 4 that allows an ODFI to reverse fraudulently induced credit push transactions, in addition to unauthorized ones, and to request a return from an RDFI for a broader range of reasons. Both proposals appropriately emphasize that there needs to be an increased emphasis on remedying push credit scenarios where the payment was initiated by the consumer/sender but was fraudulently induced.

It is often the case that a victim of a fraud scheme is unable to recover the funds lost because the fraud actor quickly withdraws the money transferred to their account. This quick withdrawal occurs regardless of the type of fraud scheme- whether the money was obtained through a transfer that was originated without the accountholder's authorization or whether the transfer was fraudulently induced. Several actions by the RDFIs and the ODFIs could put a roadblock to the quick withdrawal of fraudulently received payments.

[2] https://www.niceactimize.com/mule_defense/. We express no opinion on the effectiveness of NICE Actimize's products.

First, it is necessary for the RDFI to catch the fraud and return the stolen funds before the fraudster withdraws the money. Therefore, when an RDFI is required to monitor incoming credits and collects information associated with those transactions, the RDFI will then be able to timely spot suspicious transactions and initiate a return. Use of return reason code R17, combined with the label "questionable," gives the ODFI important information about why an entry is being returned, which may alert the ODFI to the fact that an account has been compromised and other actions should be taken. Indeed, we are not sure why use of this code should be discretionary. Requiring use of the code would promote important communication and consistency.

Likewise, when an ODFI can quickly reverse fraudulent transactions, the fraudster will be prevented from withdrawing the stolen money. ODFIs need to have the ability to reverse fraudulent transactions on their own. We strongly support giving ODFIs the ability to reverse the transaction rather than waiting for the RDFI to respond to a request to return an entry, which can waste valuable time and impede recovery of the funds. If a transaction was fraudulent and the receiver is not entitled to the funds, it should be reversed. By being able to reverse fraudulent entries, the ODFI will help reduce successful fraud and enable recovery of funds when fraud has occurred. In turn, these steps will increase the likelihood of recovery of funds after the occurrence of fraud and advance the Risk Framework objective to improve the recovery of funds.

Because it is not always possible for an ODFI to reverse an entry within the time required, we support proposed amendment No. 4, which would allow an ODFI to request a return payment from an RDFI at any time, for any reason, including for fraud. However, we believe that an RDFI should be required to return funds when it receives a request to return due to an unauthorized transaction or a fraudulently induced transaction unless the RDFI can establish that the receiver was entitled to the funds. Proposed amendment No. 4 only requires an RDFI to respond to an ODFI's request to return the entry, but the RDFI does not have to return the funds.

We are also unsure whether the requirement for an ODFI to indemnify the RDFI from any costs, fees, etc. when sending a reversal or request for return will have a chilling effect on an ODFI initiating the request. If a transaction is unauthorized at its inception, then it is understandable that the ODFI indemnify the RDFI. However, when a transaction is fraudulently induced, both the ODFI and the RDFI bear a responsibility to prevent and stop the transaction, but the RDFI bears a greater responsibility in preventing the bad actor from successfully completing the fraud scheme. As such, the ODFI should not bear a greater responsibility in indemnifying the RDFI for these types of transactions.

If an ODFI is ***required*** to request a reversal or return based on any claim of fraud (whether unauthorized or fraudulently induced) and an RDFI is ***required*** to return the funds based on the same request, then it makes sense for the ODFI to indemnify the RDFI. But if the requests for reversals and returns based on fraud are completely voluntary, then the cost of a potential indemnification may deter or disincentivize ODFIs from sending the request in the first place.

Finally, though NCLC is not in a position to answer whether current methods and tools are sufficient for RDFIs to communicate with ODFIs about suspicious transactions, we believe that

improvement is needed based on anecdotal evidence. We have been told that fraud staff at financial institutions do not have contact information for their counterparts at other financial institutions if they identify a problem and wish to resolve it. Likewise, they admitted they would not accept a call from someone they do not know from another financial institution. As time is of the essence, financial institutions need a way to communicate with each other quickly in the event of a problem, whether to request freezing stolen funds or releasing them if an issue is resolved.

Proposed Amendment No. 5

NCLC supports proposed amendment No. 5, which expands the types of transactions an RDFI may exempt from funds availability to include credit entries it believes originated as part of a fraud scheme or event. The ability to freeze funds from questionable transactions immediately is crucial. As previously mentioned, funds received due to a fraudulent scheme are often quickly withdrawn from an account, and the impacted victim is unable to recover those funds. Proposed amendment No. 5 therefore advances the Risk Framework objective to improve the recovery of funds by allowing an RDFI more time to investigate a claim of fraud and determine whether their customer is entitled to the funds.

Proposed Amendment No. 6

NCLC also supports proposed amendment No. 6, which establishes two new standard descriptions: (1) PAYROLL for PPD Credits for payment of wages and the like and (2) PURCHASE for e-commerce purchases. The more specificity an RDFI has about the purpose of a transaction, the easier it will be for the RDFI to detect fraud. As a result, proposed amendment six will advance the Risk Framework objective to reduce the incidence of fraud and more generally to improve ACH transaction quality.

Proposed Amendment No. 7

NCLC generally supports proposed amendment No. 7, which would standardize the formatting for the Individual Name field for consumer names. Standardization can help identify fraudulent actors.

However, NCLC believes that RDFIs should be required to perform name matching when handling received ACH Entries. RDFIs should verify that the name of the recipient matches the name on the account. Payments should not be processed if the recipient identified by the sender does not match the name on the account. This additional requirement truly will help prevent fraud and advance the Risk Framework objective to reduce the incidence of fraud.

Proposed Amendments No. 8 and No. 9

NCLC supports proposed amendments No. 8 and No. 9. Proposed amendment No. 8 allows for a written statement of unauthorized debit (WSUD) to be submitted before the unauthorized

payment has posted to the account. Proposed amendment No. 9 requires the RDFI to promptly return an unauthorized debit upon receipt of a completed WSUD.

Because time is of the essence in recovering lost funds, the sooner an accountholder can report an unauthorized transaction, the sooner an RDFI must return the unauthorized debit, and therefore, the greater the likelihood of preventing the loss of funds. As a result, proposed amendments Nos. 8 and 9 improve the process and experience when debits are claimed to be unauthorized and advance the Risk Framework objective to reduce the incidence of fraud.

Concluding remarks regarding money mule accounts

We support the proposed amendments as important steps towards preventing and mitigating fraud. However, we ultimately believe that more measures are needed to ensure consumers are reimbursed for fraudulently induced payments, even if the funds are gone by the time the ODFI sends a reversal or request for return. If the ODFI's customer is a fraudster, the ODFI should bear the liability. If the accountholder that received the funds is a money mule[3] intermediary who was also a fraud victim and transferred funds to the fraud actor's account at a third institution, the liability should be passed down the chain. While in some cases the money mule may have transferred the funds to the fraud actor through a method other than and ACH (cash withdrawals, gift card purchases, etc.), making it impossible to reach the ultimate scammer, imposing liability on the receiving institution will create the incentive to set up systems that detect and ideally prevent suspicious transactions, such as large and unusual ACH transfers immediately followed by large cash withdrawals. For example, in the UK, financial institutions are working to implement the Mules Insights Tactical Solution (MITS), a new technology that helps to track suspicious payments and identify money mule accounts.[4]

Thank you for the opportunity to provide comments on these proposed amendments. Please contact me at csanchezadams@nclc.org with any questions.

Yours very truly,

Carla Sánchez-Adams
Senior Attorney
National Consumer Law Center
(on behalf of its low-income clients)

[3] *See* Lisa Weintraub Schifferle, Federal Trade Comm'n, "What's a money mule scam?" (Mar. 4, 2020).
[4] *See* UK Finance. "Fraud - The Facts 2021: The Definitive Overview of Payment Industry Fraud," (2021) at 55.