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

June 3, 2011

Via E-MAIL

Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, D.C. 20551

RE: Docket No. R-1409 – Regulation CC

Dear Ms. Johnson:

NACHA—The Electronic Payments Association[1] respectfully submits this response to the Federal Reserve Board ("Board") on proposed amendments to Regulation CC ("Proposed Rule") to facilitate the transition to fully-electronic check clearing, including provisions that would:

- Condition a depositary bank's[2] right of expeditious return on its agreement to accept returned checks in electronic form;
- Amend the funds availability schedules and related model forms to reflect that there are no longer non-local checks; and
- Define a new form of transaction ("electronically-created item" or "E-CI"), with related warranty and liability provisions, to address a payments practice where an image of a "check" is created, but the check never existed in paper form (therefore being fully electronic and not a "check" for legal purposes).

NACHA's specific comments are limited to those provisions in the Board's proposal with potential impact to the ACH Network, and to the legal interpretation of fully electronic

[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.

[2] The term "bank" throughout reflects its regulatory definition and includes thrifts and credit unions.

authorizations. However, we also note our broad support for both the Board's approach in the Proposed Rule supporting a complete transition to fully-electronic interbank clearing, and for other financial services industry comments we are familiar with[3] that do not directly conflict with any NACHA comments.

NACHA Comments

§ 229.2(b) – Automated clearinghouse (ACH) credit transfer. The Proposed Rule would replace the defined term "automated clearinghouse" with "automated clearinghouse credit transfer." This term is also referenced in Regulation CC's definition of "electronic payment" at § 229.2(t)[4] and in the commentary to § 229.10(b) which requires a bank to make funds received for deposit by an electronic payment available for withdrawal the next day. We describe below a request that the Board use its authority under the Expedited Funds Availability Act (EFA Act) to extend the application of exception holds under the Final Rule to ACH credit transfers. We are making this request to permit RDFIs to impose an exception hold on ACH credit transfers if they have reason to doubt the authorization for the transaction and thereby reduce the potential for losses due to fraud. In making this request, we note that amending Regulation CC in this way would be consistent with the Board's prior inclusion of ACH credit transfers, along with statutorily-specified wire transfers, in the current definition of "Electronic Payments" for Regulation CC's general availability purposes.

We call out our request regarding exception holds here because of the relevance in how the Proposed Rule defines and applies the terms "ACH credit transfer" and "electronic payment."

§ 229.2(r) – Depositary bank. We agree with the clarification in the Proposed Rule that a bank that rejects a deposit should not be viewed as a "depositary bank." Further, we support other industry commenters in seeking examples in the final rule of different circumstances in which an item purporting to be a "check" could be received and subsequently rejected for deposit by a bank of first deposit. Consistent with our comments below regarding proposed § 229.34(e) and "Electronically-Created Items," we further believe that the type of transaction the Board contemplates in its proposed definition of this term be considered among the specific examples of what a bank might reject and thereby avoid being deemed a "depositary bank" with respect to that deposit for the purposes of Regulation CC.

§ 229.13(e) Reasonable Cause To Doubt Collectability. NACHA is using this opportunity to ask the Board to include in Section 229.13(e), an exception to the availability requirements for instances in which a paying bank (the Receiving Depository Financial Institution ("RDFI") in

---

[3] Including joint industry comments submitted by the Electronic Check Clearing House Organization ("ECCHO"), the Clearing House ("TCH"), the Independent Community Bankers of America ("ICBA"), and BITS.

[4] In the Proposed Rule, the revised commentary to§ 229.2(t), T. 229.2(t) Electronic Payment, states:

> 1. Electronic payment is defined to mean a wire transfer as defined in §229.2(bbb) or an ACH credit transfer as defined in § 229.2(b). The EFA Act requires that funds deposited by wire transfer be made available for withdrawal on the business day following deposit but expressly leaves the definition of the term wire transfer to the regulation. Because ACH credit transfers pose little risk of return to the depositary bank, the regulation requires that funds deposited by ACH credit transfers be available for withdrawal on the business day following deposit.

ACH parlance) has reasonable cause to believe that an ACH credit was not authorized by the accountholder at the Originating Depository Financial Institution ("ODFI"). When Regulation CC was drafted, the concept of an unauthorized ACH credit was a remote one. But today, an unauthorized ACH credit may be initiated as the result of Corporate Account Takeover. Corporate Account Takeover is a type of identity theft in which cyber-thieves steal the valid online banking credentials of a business, enabling the cyber-thief to steal funds from the business account by initiating transfers out of that account. According to some reports, the occurrence of Corporate Account Takeover is on the rise, imposing significant losses on its victims.[5] In some instances the funds stolen through Corporate Account Takeover are never recovered, and the loss is absorbed by the business whose account has been wrongfully accessed. Depending on the facts and circumstances, a bank may be willing to reimburse its customer for all or a portion of such losses, but this merely shifts the cost of criminal activity and does nothing to prevent that activity or mitigate its effect. Moreover, each such intrusion damages the reputation and integrity of the financial institutions and the ACH Network even though such fraudulent activity generally originates from flaws in corporate security and internal control systems rather than in the ACH Network itself.

Currently, the *NACHA Operating Rules* prescribe that the RDFI make the amount of each ACH credit transfer received from its ACH Operator available to the Receiver for withdrawal no later than the settlement date of the entry, subject to its right to return the transaction.[6] NACHA has proposed, in a Request for Comment (attached hereto), an exception to NACHA's day of settlement availability requirement for certain ACH credit transfers. If an RDFI reasonably suspects that the transaction is unauthorized, the *Rules* change would allow the RDFI additional time to investigate the suspicious entry, but in any event, it would have to make the funds available in the time required by applicable law. To the extent that Regulation CC's next-day availability terms would apply, this exception would give the RDFI hours – not even an additional full day – to determine whether the funds were fraudulently originated. While helpful, this is not enough time for a bank to complete a thorough investigation of a suspicious entry.

Therefore, we ask the Board to extend Regulation CC's reasonable cause exception hold for check deposits to ACH credit transfers received.

We believe the Board has the authority under § 609(a) and § 609(c) of the EFA Act to extend the application of exception holds under the Final Rule to ACH credit transfers. This change to Regulation CC, together with the *NACHA Operating Rules* change described above, would permit RDFIs to impose an exception hold period on an ACH credit transfer for up to 4 days if they have reason to doubt the authorization for the transaction. This, in turn, would provide RDFIs the necessary additional time to prevent or reduce losses associated with unauthorized

---

[5] The incidences of Corporate Account Takeover "are rising in numbers because cybercriminals have found them rather easy to perpetrate—especially when it comes to [small and midsize businesses] that don't have a dedicated IT security staff…The rewards are great – often surpassing hundreds of thousands of dollars – and the risk is low." Time Wilson, *FBI Warns of 'Corporate Account Takeover' Scams* , Oct. 21, 2010 (available at http://www.darkreading.com/smb-security/security/perimeter/showArticle.jhtml?articleID=227900529) (referring to the *Fraud Advisory for Businesses: Corporate Account Take Over*, released on Oct. 20, 2010 through a Joint effort of the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) and available at http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf).

[6] NACHA Operating Rules, Article Three, Subsection 3.3.1.1 General Rule for Availability of Credits.

ACH credit transfers. Further, amending the Rule in this way would be consistent with the Board's prior inclusion of ACH credit transfers, along with statutorily-specified wire transfers, in the current definition of "Electronic Payments" for Regulation CC general availability purposes.

§ 229.13(h) – Availability of deposits subject to exceptions. NACHA is supportive of other industry commenters with respect to the maximum period allowable for exception holds. Specifically, we would support additional time for the safe harbor for non-on-us items, beyond the additional two days set forth in the proposed rule. Based on the industry's review of the Proposed Rule's four (4) business days maximum hold period, we understand that depositary banks may be exposed to substantial monetary risk from the reduction of the safe harbor period to any period under a total of five (5) business days (2 days plus 3 additional days).[7] This reflects the industry's assessment that there are situations where it will take longer than four business days to collect an item, even using electronic collection methods. This may occur, for example, where the item has been fraudulently altered to delay its collection and return (e.g., the item bears a fictitious or non-matching routing number and account) or where there is another problem with the electronic collection or return and manual intervention is required. Second there will remain a small subset of items that are not eligible for image exchange. If items subject to a deposit hold exception are collected and returned in paper process, the time period for forward and return exchange may extend beyond four business days.

§ 229.16(c)(2)(i) – Notice at time of case-by-case delay. The Proposed Rule requested comment on whether banks found the case-by-case hold option still useful and our understanding is that they do. Therefore, banks should retain the ability to impose case-by-case holds on deposited items (potentially including ACH credit transfers as we describe above).

§ 229.30(e) – Notice in lieu of return – Commentary. This section provides that a bank may send a notice in lieu of return only where neither the check itself nor an image of and information related to the check sufficient to create a substitute check is available. The Proposed Rule requested comment on whether the notice in lieu of return should be maintained or deleted, and whether the ACH Network should be supported as a means to convey such notices. As with other industry commenters, we support maintaining the option for a paying bank to send a notice in lieu of return since the need for the notice has not gone away with image exchange and return. There may still be situations where the notice is the only option for the paying bank. We would also support including the MICR line information from the original check (and the depositary bank sequence number of the item, if available) in the notice of lieu of return where that information is available to the paying bank. This information is typically helpful to the depositary bank identifying the item to which the notice relates.

With respect to using the ACH Network for routing notices in lieu of return, in the future this application might represent a viable option. That said, initial consultations with the industry suggest there is insufficient support for this option, at this time, to begin a rulemaking initiative to implement such a capability. The primary concern expressed to NACHA in this regard is that many banks' check and ACH systems remain separate, and that such routing comes with the risk that appropriate bank staff and systems will not recognize or be in a position to process the notice.

---

[7] See, e.g., the comments of ECCHO and The Clearing House.

§ 229.34(e) – Electronic image and information transferred as an electronic collection item or electronic return. In this proposed new section the Board acknowledges a new form of transaction now in the marketplace that is being deposited and collected as an image of a "check," but no check ever existed in paper form. The Proposed Rule refers to these types of transactions as "electronically-created items." Other industry terms include "paperless items," "virtual checks," "electronic payment orders," "fully-electronic checks," and "non-check RCCs." NACHA will rely on the Board's proposed terminology and refer to these transactions by their acronym – "E-CIs" (not to be confused with another new term in this Proposed Rule – "electronic collection items"). For the reasons described more fully below, we are generally supportive of the proposed application of the warranties under § 229.34 to E-CIs, but do not support extending Subpart C coverage to E-CIs as "checks" at this time pending a more thorough review of the appropriate legal foundation for these particular types of transactions.

The Board notes two forms of E-CIs. The first form involves a payee (e.g., a merchant or biller) producing E-CIs that resemble imaged remotely created checks ("RCCs"). A common process for doing this involves the drawer completing the elements of a check online at the payee's website (or that of its agent) and "authorizing" the transaction electronically (as a substitute for an actual handwritten signature). The second form of E-CI involves the paying bank supplying a smart phone application through which its customer is able to execute a "handwritten" signature on the screen, which is then attached to an electronic "check" sent as an image via the Internet to the payee for the payee's subsequent deposit with its bank. In neither case is an original physical check involved, and therefore it cannot be used to create a substitute check that meets the requirements of the Check21 Act and Regulation CC. Further, for both forms of E-CI the authorization and transaction initiation process is entirely electronic.

As described more fully below, the Proposed Rule (1) would extend to E-CIs the warranty scheme in place for RCCs to protect banks downstream from the first bank receiving an E-CI that process these transactions without knowledge that they are anything but images of legitimate "checks," and (2) requests comment on whether an E-CI should in future be subject to subpart C of Regulation CC as if it were a "check."

1. Proposed E-CI warranty scheme. Since E-CIs are virtually indistinguishable from images of checks and RCCs, a bank (including the depositary bank) receiving an E-CI may transfer that image as if it were an electronic collection item or electronic return, or produce a paper item that is indistinguishable from a valid substitute check. To protect a bank that receives an E-CI from another bank from potential liability, the Board is proposing that any bank transferring an E-CI make any warranty that the bank would make if the E-CI were in fact a valid electronic collection item or electronic return.

If implemented, the result of this warranty scheme would be that a bank receiving a warranty claim on an electronic collection item, electronic return or non-conforming substitute check could pass back its liability for the item to the bank from which it received the E-CI. Therefore, the chain of warranties could be traced back to the first bank in the collection chain. Although this bank may not always know whether an image it received from a customer came from a paper item, the Board bases its proposed warranty scheme on the assumption that this bank is in the best position to know and protect itself contractually against the risk that it did not.

2. Making E-CIs "Checks" in Regulation CC. The Board seeks comment on whether it should consider making an E-CI subject to subpart C of Regulation CC as if it were a check. Such a change would result, for example, in the paying bank to which the E-CI is presented being subject to Regulation CC's expeditious return requirement.

The Board also seeks comment on return rates for E-CIs (to the extent they can be distinguished from other returns), and whether there are valid reasons for E-CIs as a payment means as opposed to ACH debit transactions or other means.

The proposed application to E-CIs of the warranty scheme applicable since 2006 to remotely-created checks ("RCCs") makes practical sense considering that the paying bank (or its agent) is not the bank that "authorized" the initiation of the E-CI by a business or consumer. By way of comparison, the manner in which E-CIs are initiated is similar in all functional aspects to telephone-initiated entries ("TEL") and internet-initiated entries ("WEB") in the ACH Network (i.e., a verbal or electronic consent of a customer providing approval for a transaction to debit their DDA without a paper item or written approval). It follows that the warranty scheme should be comparable to the approach taken through the *NACHA Operating Rules* whereby the ODFI warrants that an entry (including WEB and TEL entries) is properly authorized.[8]

In the case of a merchant or biller using and depositing virtual checks with a financial institution for collection in the consumer environment, NACHA believes that in many cases an ACH or other EFT transaction would suffice as an alternative. In fact, we have noted in recent years online pitches by payment processors for the technology and services behind these virtual check creators that clearly are intended to skirt ACH Network and other EFT system risk management controls and consumer protections. This is not to say that all parties initiating E-CIs today are seeking to evade responsibility, and banks are hampered in their ability to even recognize such transactions, but given the clear and transparent legal foundation accorded to all parties to an ACH transaction under the law and the *NACHA Operating Rules*, we believe a more appropriate mechanism for conveying these types of transactions, generally, is the ACH Network.

Looking forward as payment channels continue to converge at the point of payment initiation, adding paying bank protective warranties through Regulation CC addresses an immediate practical need, but stops short of the larger issue – i.e., the need for clarification of the legal underpinnings of the types of transactions the Proposed Rule's warranties seek to address. For this reason, we do not support at this time going beyond the proposed warranty scheme and subjecting E-CIs to the provisions of Subpart C as if they were checks. Instead, and we know other commenters may reply differently, we believe the underlying legal foundation of these transactions, and the appropriate regulatory regimen that should apply, is an area requiring further study by the Board and the industry.

---

[8] Extending Regulation CC's warranty scheme for RCCs to E-CIs, and their consideration for coverage under Subpart C, is also suggestive of ACH transactions having, in a like way, the flexibility to potentially clear through check collection systems with Regulation CC coverage. The attendant operational, risk management provisions and legal foundation issues would require thoughtful consideration before NACHA could support such a course of action, even though such structure would give ACH transactions risk management and consumer protection provisions similar to checks.

Appendix C, Model Availability Disclosures – C-1 through C-4B.

As the Board notes, § 229.10 (b) requires next-day availability for electronic payments (as defined in § 229.2(t) and including ACH credit transfers). However, the model availability policy disclosures in Appendix C of the Proposed Rule include clauses stating that funds from "electronic direct deposits" are available on the day the bank receives the funds. As indicated in paragraph B(1)(b) of the commentary to the appendix, this is because "U.S. Treasury regulations and ACH association rules [i.e., the *NACHA Operating Rules*] require that preauthorized credits, such as direct deposits, be made available on the day the bank receives the funds."

The Board is proposing that model funds availability disclosures C-1 through C-3B, which are designed for banks that generally make deposits available by the next day, be modified to indicate that funds from cash deposits and electronic direct deposits will be available for withdrawal on the same business day that the bank receives the funds. The proposed commentary states that a bank basing its disclosure on one of these models should modify its disclosure to indicate that funds will be available the next day if that reflects the bank's practice.

In contrast, proposed models C-4A and C-4B, which are designed for banks that hold funds from deposits to the statutory limits, indicate that funds from cash deposits and electronic direct deposits will be available on the business day following receipt. The proposed commentary states that a bank that bases its disclosures on one of these models, but that makes the funds available the same day they are received – i.e., a bank that places holds to statutory limits only on check deposits, should modify its disclosures accordingly.

As we have discussed previously, it is possible for an ODFI to discover a problem with the authorization of an ACH transaction and inform the RDFI on or about the day the transaction is received. We believe that no changes should be made to the model funds availability disclosures to state same-day availability for electronic payments (referred to as "electronic direct deposits" in the model forms), which are given next-day availability under the Rule. For banks that make the proceeds of ACH credit transfers available on the day received,[9] the model disclosures provide necessary flexibility when a bank might need to hold funds availability over to the next day if there is reason to doubt a transaction's authorization. Since such occurrences represent an exception to the bank's general availability policies (and its compliance with the *NACHA Operating Rules* and 31 CFR Part 210), asking all banks to make different disclosures for exceptions only adds cost to the bank and potentially confusion for the customer. Also, if the Board extends Regulation CC's exception hold provisions to electronic payments (as defined in the Proposed Rule) as NACHA has requested in this letter, we would recommend the following edits be considered to the proposed language in model disclosure C-2 addressing exception holds (using the Board's same convention for editorial changes – i.e., "►**NEW LANGUAGE**◄", and "[~~deleted language~~]"):

> **Longer Delays May Apply**
>
> Funds you deposit by check ►**or electronic direct deposit**◄ may be delayed for a longer period under the following circumstances:
>
> - We believe a check you deposit will not be paid.

[9] In accordance with the *NACHA Operating Rules* and 31 CFR part 210 for Federal government payments.

- ▶**We believe an electronic direct deposit may not have been authorized by the payor**◀
- You deposit checks totaling more than $5,000 on any one day.
- You redeposit a check that has been returned unpaid.
- You have overdrawn your account repeatedly in the last six months.
- There is an emergency, such as failure of computer or communications equipment.

We will notify you if we delay your ability to withdraw funds for any of these reasons, and we will tell you when the funds will be available. They will generally be available no later than the (number) business day after the day of your deposit.

Special Rules for New Accounts

If you are a new customer, the following special rules will apply during the first 30 days your account is open.

[~~Funds from electronic direct deposits to your account will be available on the day we receive the deposit.~~] Funds from deposits of cash, ▶**electronic direct deposits,**◀ wire transfers, and the first $5,000 of a day's total deposits of cashier's, certified, teller's, traveler's, and federal, state and local government checks will be available on the first business day after the day of your deposit if the deposit meets certain conditions. For example, the checks must be payable to you (and you may have to use a special deposit slip). The excess over $5,000 will be available on the ninth business day after the day of your deposit. If your deposit of these checks (other than a U.S. Treasury check) is not made in person to one of our employees, the first $5,000 will not be available until the second business day after the day of your deposit.

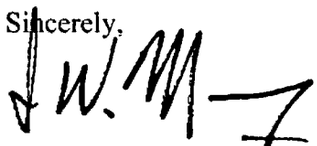
Funds from all other check deposits will be available on the (number) business day after the day of your deposit.

We recommend comparable changes to model disclosures C1 (removing the reference to same-day availability for "electronic direct deposits" and including these among the examples for next-business day availability), C-3 and C-4.

* * *

Again, NACHA appreciates the opportunity to provide comments on the Board's Proposed Rule. If you have any questions regarding our comments, please do not hesitate to call me at (703) 561-3929.

Sincerely,



Ian W. Macoy, AAP
Managing Director

Attachments:

1. *NACHA Operating Rules* Proposal and Request For Comment
2. White paper: *The Hold Rules Proposed By NACHA Are Consistent In Practice And Policy With The Expedited Funds Availability Act And Regulation CC*

cc: David E. Teitelbaum, Esq., Sidley Austin LLP

NACHA
The Electronic Payments Association®

Corporate Account Takeover

Request for Comment

Executive Summary and Rules Description
April 29, 2011

REQUEST FOR COMMENT – RESPONSES DUE BY FRIDAY, JUNE 10, 2011
NACHA requests comment on a proposal to amend the *NACHA Operating Rules (Rules)* to address Corporate Account Takeover. Comments are due by Friday, June 10, 2011.

NACHA STAFF CONTACTS

Return comments to:
Maribel Bondoc, Manager, Network Rules
Fax: (703) 787-0996
email: mbondoc@nacha.org

Questions:
Deborah Shaw
Managing Director, Network Enforcement & Risk Management
Phone: (703) 561-3919
email: dshaw@nacha.org

Michael Herd, Managing Director, ACH Network Rules
Phone: (703) 561-3924
email: mherd@nacha.org

Part I: Proposal Brief

This proposal would amend the *Rules* by adding two new provisions - the "Sound Practices Rule" and the "Availability Exception Rule" - each of which is designed to protect and strengthen the reputation, security and integrity of the ACH Network by providing participants with tools to address Corporate Account Takeover. The proposed rules are part of a more comprehensive effort that NACHA is undertaking to reduce the incidence and impact of Corporate Account Takeover on ACH Network participants. In addition to the proposed rules, the NACHA Board of Directors adopted a Policy Statement on October 21, 2010 on the Importance of Sound Practices to Mitigate Corporate Account Takeover. This policy announced NACHA's intent to communicate sound practices that should be implemented by ODFIs and other ACH participants, such as Originators and Third-Party Senders, to minimize the risk of, and protect against, Corporate Account Takeover.

The "Sound Practices Rule" proposal is intended to keep non-consumer Originators and Third-Party Senders informed about current industry sound practices to prevent the origination of

unauthorized credit Entries, including unauthorized transactions that result from Corporate Account Takeover. Specifically, the Sound Practices Rules would:

- Require an ODFI to provide, on an annual basis, its Originators and Third-Party Senders with current industry sound practices to prevent unauthorized credit Entries from being initiated from non-Consumer Accounts (Subsection 2.11.1); and

- Require a Third-Party Sender to provide, on an annual basis, its Originators with current industry sound practices to prevent unauthorized credit Entries from being initiated from non-Consumer Accounts (Section 2.14.6).

In each case, the sound practices should relate to the nature of the relationship between the parties.

The "Availability Exception Rule" proposal is designed to allow RDFIs additional time to investigate suspicious credit Entries prior to making funds available to a Receiver. The Availability Exception Rule is expected to reduce losses associated with unauthorized credit Entries. Specifically, the Availability Exception Rules would:

- Provide an RDFI that reasonably suspects that a credit Entry is unauthorized with an exception to the *Rules* provisions requiring the RDFI to make certain credit Entries available to customers more quickly than required to under Regulation CC; and

- Require the RDFI promptly to notify the ODFI if the RDFI makes use of this exception to the funds availability requirements of the *Rules*.

Part II: Background

Risks to payment networks are ever-changing. Cyber-thieves are becoming increasingly sophisticated at exploiting vulnerabilities in all types of corporate and banking systems in order to commit fraud. Corporate Account Takeover is a type of corporate identity theft in which cyber-thieves steal a business' valid online banking credentials and subsequently utilize those credentials in fraudulent banking activity. Corporate Account Takeover represents a risk to ACH Network participants even though the roots of this criminal activity generally are not in banking systems themselves.

Corporate Account Takeover is particularly pernicious because once a cyber-thief obtains a company's valid online banking credentials, the thief can use those credentials in a variety of ways. The thief may initiate funds transfers out of the compromised business' account by ACH or wire transfer to the bank account of associates within the U.S. or directly overseas (with wire). In some cases, the perpetrator also may be able to gain access to and review the business' account details, such as account balances, activities and patterns, enabling the perpetrator to mimic the legitimate users and initiate transactions undetected.

Cyber-thieves employ various methods to obtain access to banking credentials from legitimate businesses, including mimicking a legitimate institution's website, using malware and viruses to compromise the legitimate business' system, or even using social engineering to defraud

employees into revealing security credentials or other sensitive data. For example, corporate systems may be compromised by (1) an infected document attached to an email, (2) a link within an email that connects to an infected website, (3) employees visiting legitimate websites – especially social networking sites – and accessing the infected documents, videos or photos posted there, or (4) an employee using a flash drive that was infected by another computer. In each case, the infected system is then exploited to obtain legitimate security credentials that can be used to access a company's corporate accounts.

Part III: Justification for the Proposal and *Rules* Framework

As further described below, this *Rules* proposal is designed to strengthen the reputation, integrity and security of the ACH Network by (1) keeping ACH Network participants informed about the sound practices available in the industry to help prevent and mitigate the risk of Corporate Account Takeover; and (2) provide RDFIs with greater flexibility to prevent and/or reduce losses associated with unauthorized credit Entries.

The Sound Practices Rule

Originators, particularly small businesses that have the ability to initiate funds transfers online but may not have focused on fraud detection and prevention, are vulnerable to the constantly evolving methods by which cyber-thieves perpetrate Corporate Account Takeover. ODFIs and the Third-Party Senders each have the ability to educate their customers about the prevention, detection, and reporting measures that their customers can take to help prevent unauthorized transfers, including Corporate Account Takeover. The centralized roles of ODFIs and third Party-Senders position these parties to more efficiently deliver this education than other participants in the ACH Network. The Sound Practices Rule is designed to strengthen the integrity and security of the ACH Network by educating potentially vulnerable Originators on how they can protect themselves against unauthorized Entries, including Corporate Account Takeover.

The Sound Practices Rule adds the following two new provisions to Article Two of the *Rules*:

- Require an ODFI to provide, on an annual basis, its Originators and Third-Party Senders with current industry sound practices to prevent unauthorized credit Entries from being initiated from non-Consumer Accounts; and

- Require a Third-Party Sender to provide, on an annual basis, its Originators with current industry sound practices to prevent unauthorized credit Entries from being initiated from non-Consumer Accounts.

Because Third-Party Senders may provide services that involve accounts at multiple institutions, the *Rules* would require Third-Party Senders to address sound practices only to the extent applicable to the relationship between the Third-Party Sender and the Originator, and would not require the Third-Party Senders to address other aspects of an Originator's relationship with its financial institution.

The Sound Practices Rule is intended to educate Originators, which are often targeted by cyber-thieves and fraudsters, how to protect themselves against the origination of unauthorized credit Entries. Small business Originators are susceptible to Corporate Account Takeover as well, and accordingly, the obligations imposed by the Sound Practices Rule apply to small business Originators. Samples of sound practices for financial institutions, Originators and Third Party Senders are available at:
http://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm.

NACHA specifically requests comment on whether the requirement to annually distribute sound business practices to Originators should be limited to Originators of credit Entries only or should include Originators of credit or debit Entries.

The Availability Exception Rule

To comply with the current *Rules*, RDFIs are required to make funds from a credit Entry available to the Receiver within certain *Rules*-specified time limits, subject to the RDFI's right to return the Entry. Generally, the *Rules* require RDFIs to make funds from credit Entries available on the Settlement Date, i.e. by close of business on that date. The funds availability requirement for PPD credits (that often represent payroll) is by opening of business on the Settlement Date if the Entry is made available to the RDFI by its ACH Operator by 5 p.m. (RDFI's local time) on the Banking Day prior to Settlement Date. These requirements are faster than those mandated in the ordinary course by Regulation CC, which provides that funds from electronic credits must be made available "not later than the business day after the banking day on which the bank received the electronic payment."[1]

ODFIs may, from time to time, request an RDFI investigate or return funds related to a credit Entry that the ODFI reasonably suspects was originated without authorization. RDFIs also may have their own reason to suspect that a credit Entry received was originated without authorization. In cases of unauthorized ACH credits, some RDFIs believe that they are not able to cooperate with an ODFI's request to recover the funds or their own desire to investigate potential fraud because they are required by the *Rules* to make funds available.[2] The Availability Exception Rule would permit the RDFI additional time to respond to such request before having to make the funds available to the Receiver, thereby increasing the likelihood that the funds will be recovered by the ODFI for its customer. Of course RDFIs must still comply with Regulation CC availability requirements unless an exception to the Legal Requirement applies.

The goal of this Rules proposal is to provide an exception to the funds availability requirements contained within the *Rules* if the RDFI has a reasonable suspicion that the Entry was not properly authorized. The Availability Exception Rule would give the RDFI additional time under the *Rules* to investigate such suspicions, including in response to requests from ODFIs before having to make funds available in accordance with Legal Requirements. An RDFI also could avail itself of this exception to respond to a request from an ODFI to investigate or return the funds related

[1] Under Regulation CC Section 229.10(b)(2), an electronic payment is received when the bank has received payment in actually and finally collected funds. Funds availability for ACH credit payments under Regulation CC is the opening of business the business day after the Settlement Date, which is the later of 9:00 a.m. (RDFI's local time) or the time when the ATM or tellers are available. *See* 12 C.F.R. § 229.19(b).
[2] The existing *Rules* do provide that an ODFI can request an RDFI to return an Entry.

to a credit Entry if the ODFI reasonably suspects that the Entry was originated without authorization, up to the time the RDFI is legally obligated to make the funds available under applicable law.

This exception does not allow the RDFI to delay availability because of an RDFI's errors in processing an Entry. Accordingly, existing rules related to the availability of credit Entries (Subsection 3.3.1.1 (General Rule for Availability of Credits) and Subsection 3.3.1.2 (Availability for Certain Credit PPD Entries)) would be modified to provide only a limited exception to the RDFI's obligation to make credit Entries available within the time frames specified by the Rules if it suspects that the Entry is unauthorized. If the RDFI makes use of this exception, the RDFI would be required to promptly notify the ODFI of any delay in availability. (Subsection 3.3.1.1 and 3.3.1.2)

NACHA specifically requests comment on whether the requirement to promptly notify the ODFI of any delay in availability is necessary given that the RDFI must make the funds available the day after settlement as required by Regulation CC if the funds haven't been otherwise returned by that time.

Part IV: Impact of the Proposed Rule

Benefits of the Proposed Rule

The Sound Practices Rule and the Availability Exception Rule are designed to protect and strengthen the reputation, security, and integrity of the ACH Network, and all participants in the ACH Network are expected to generally benefit from such improvements. Direct benefits to specific ACH Network participants are set forth below.

The Sound Practices Rule

Originators and Third-Party Senders: Originators and Third-Party Senders will benefit from the Sound Practices Rule through their receipt of current industry sound practices, which they could implement to reduce the likelihood and incidence of unauthorized credit Entries. Implementation of such tools and methods by Originators would help to reduce the losses Originators experience related to unauthorized credit Entries.

ODFIs: Annual distribution of sound practices to prevent unauthorized credit Entries is expected to increase awareness and implementation of current risk management tools by Originators and Third-Party Senders, therefore reducing losses to ODFIs and their customers from unauthorized credit Entries.

RDFIs: Annual distribution of sound practices to prevent unauthorized credit Entries is expected to increase awareness and implementation of current risk management tools by Originators and Third-Party Senders. This would reduce the frequency with which RDFIs receive unauthorized credit Entries and the expenses associated with handling such Entries.

The Availability Exception Rule

ODFIs: The Availability Exception Rule is expected to reduce losses related to unauthorized credit Entries by potentially allowing an ODFI more time to attempt to recover any funds associated with unauthorized credit Entries before the Receiver (a potential money mule) could withdraw funds from its account at the RDFI.

RDFIs: The Availability Exception Rule would allow an RDFI more time to investigate, and potentially prevent, a money mule from withdrawing funds from its account at the RDFI.

Originators: The Availability Exception Rule is expected to reduce the frequency and amount of losses experienced by Originators through the ACH Network.

Costs to Comply with the Proposal

NACHA anticipates that costs would be borne by ACH Network participants specific to implementation the Rules as follows:

The Sound Practices Rule

ODFIs: ODFIs will incur costs to research, develop and distribute then-current industry sound practices to their Originators and Third-Party Senders on an annual basis.

Third-Party Senders: Third-Party Senders will incur costs to research, develop and distribute then-current industry sound practices to their business customers on an annual basis.

The Availability Exception Rule

ODFIs: ODFIs may incur costs to implement the Availability Exception Rules. Such costs may include establishing policies and procedures for reacting once notified of a delay by an RDFI and possibly requesting a delay by an RDFI if the ODFI suspects a credit Entry is unauthorized.

RDFIs: RDFIs will incur costs to implement the Availability Exception Rules. Such costs may include costs related to the RDFI's (1) establishment of policies and procedures to voluntarily implement a delay in funds availability, either at its own discretion or at the request of an ODFI; (2) implementation of customer service procedures and training to handle inquiries related to Entries on which a delay has been placed; and (3) communications with ODFIs and customers regarding delayed availability.

Part V: Effective Date

In order to allow RDFIs to use the Availability Exception Rule as quickly as possible, the rule is proposed to become effective 30 days after approval by the NACHA voting members. The Sound Practices Rule is proposed to become effective on September 16, 2011, and initially apply to calendar year 2012 (i.e., the first sound practices must be provided in 2012).

Part VI: Technical Summary

Following is a list of sections within the 2011 *NACHA Operating Rules* that are impacted by the changes described within this Request for Comment:

- **Sound Practices Rule**
  - Section 2.11 (ODFI Rights and Obligations Regarding Unauthorized Credit Entries)
  - Subsection 2.11.1 (ODFI Must Provide Sound Practices to Originators and Third-Party Senders)
  - Subsection 2.14.6 (Third-Party Senders Must Provide Sound Practices to Originators)

- **Availability Exception Rule**
  - Subsection 3.3.1.1 (General Rule for Availability of Credits)
  - Subsection 3.3.1.2 (Availability for Certain Credit PPD Entries)

THE HOLD RULES PROPOSED BY NACHA ARE CONSISTENT IN PRACTICE AND POLICY WITH THE EXPEDITED FUNDS AVAILABILITY ACT AND REGULATION CC

I. Background

Corporate Account Takeover is a type of identity theft in which cyber-thieves steal the valid online banking credentials of a business, enabling the cyber-thief to steal funds from the business account by initiating transfers out of that account. According to some reports, the occurrence of Corporate Account Takeover is on the rise, imposing significant losses on its victims.[1] In some instances the funds stolen through Corporate Account Takeover are never recovered, and the loss is absorbed by the business whose account has been wrongfully accessed. Depending on the facts and circumstances, a financial institution may be willing to reimburse its customer for all or a portion of such losses, but this merely shifts the cost of criminal activity and does nothing to help stop that activity or mitigate its effect. Moreover, each such intrusion damages the reputation and integrity of the financial institutions, the ACH Network, the National Automated Clearing House Association ("NACHA") and the ACH Operators even though such fraudulent activity generally originates from flaws in corporate security and internal control systems rather than in the ACH Network itself.

In response to this illicit activity, several U.S. government agencies have stepped up efforts to increase awareness of and combat Corporate Account Takeover. By way of example, the Federal Deposit Insurance Corporation hosted the "Combating Commercial Payments Fraud Symposium" on May 11, 2010 to "examine the threat of commercial payments fraud posed by cyber criminals targeting small and midsize businesses."[2] In addition, various U.S. government law enforcement groups, including the Federal Bureau of Investigations and the U.S. Secret Service, and the Federal banking agencies have recently issued several security alerts cautioning financial institutions about the means by which fraudsters perpetrate Corporate Account Takeover and providing advice on how to prevent and/or reduce the incidence of Corporate Account Takeover and how to respond when it occurs.[3] One of the security alerts advises

---

[1] *Fraud Advisory for Businesses: Corporate Account Take Over*, released on Oct. 20, 2010 through a Joint effort of the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) and available at http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf).

[2] Announcement of "Combating Commercial Payments Fraud" An FDIC Symposium (May 5, 2010) available at http://www.fdic.gov/news/conferences/2010_fraud/index.html.

[3] *See, e.g.*, FDIC SA-185-2009, *Fraudulent Work-at-Home Funds Transfer Agent Schemes,* (Oct. 29, 2009) available at http://www.fdic.gov/news/news/specialalert/2009/sa09185.html; *Fraud Advisory for Businesses: Corporate Account Take Over*, released on Oct. 20, 2010 through a Joint effort of the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) and available at http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf); *Fraud Advisory for Consumers: Involvement in Criminal Activity through Work from Home Scams*, released on Oct. 20, 2010 through a Joint effort of the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) and available at http://www.fsisac.com/files/public/db/p264.pdf.

"financial institutions [to] act promptly when they believe fraudulent or improper activities have occurred .... Appropriate actions may include, but are not limited to, filing a Suspicious Activity Report and/or closing the deposit account in accordance with existing, board-approved account closure policies and procedures."

Consistent with these government efforts, NACHA is considering implementing new *NACHA Operating Rules(Rules)* as part of a comprehensive effort aimed at preventing Corporate Account Takeover and mitigating its risks. Specifically, the proposed rules would, in part, amend the *Rules* by adding the "Hold Rules" – which are designed to protect and strengthen the reputation, security and integrity of the ACH Network by providing depository financial institutions new tools to combat Corporate Account Takeover. As explained below, among other things, the proposed *Rules* would allow financial institutions to recapture stolen funds that have been credited to a Receiver's account by placing a hold against otherwise available funds before they are irretrievably removed by the gangs and others perpetrating these crimes. As a result, the Hold Rules are expected to strengthen the integrity of and protect the reputations of the ACH Network and its participants. The Hold Rules, if implemented, also are expected to reduce losses experienced by small to mid-size businesses, which are not protected by the consumer protections in the Electronic Funds Transfer Act and Regulation E, and their financial institutions. Moreover, these benefits will be accomplished without harm to individual consumers.

This white paper explains why the implementation of the Hold Rules would be consistent with the Expedited Funds Availability Act ("EFAA")[4] and its implementing regulations promulgated by the Board of Governors of the Federal Reserve System (the "Board") set forth in Regulation CC ("Reg. CC").[5]

II. The Proposed Hold Rules Summarized

NACHA's "Hold Rules" proposal is designed to allow Originating Depository Financial Institutions ("ODFIs") and Receiving Depository Financial Institutions ("RDFIs") a short period of time to investigate suspicious ACH credit Entries when suspicious activity is identified after funds have been credited to a Receiver's account, but before a Receiver has had the opportunity to remove funds from that account. Specifically, the Hold Rules would, among other things:

- Permit ODFIs to request that an RDFI hold for up to 2 Banking Days (and require that the RDFI honor such request) funds posted to a Receiver's account representing the proceeds of a credit Entry that the ODFI reasonably suspects was originated without authorization;
- Permit an RDFI that reasonably suspects that a credit Entry is unauthorized to hold the otherwise available funds related to such Entry for up to 2 Banking Days; and

---

[4] 12 U.S.C. §§ 4001 *et seq.*

[5] 12 C.F.R. Part 229.

- Require the ODFI to cooperate with an RDFI's investigation of a credit Entry on which the RDFI has placed a hold, including by providing any information required for the RDFI to complete any required regulatory filings.

NACHA expects the Hold Rules to reduce damages associated with unauthorized ACH credit Entries by enabling the recapture of funds that presently may slip through the banking system while institutions investigate probable fraud. By facilitating quick action to freeze the proceeds of criminal activity, the Hold Rules will mitigate losses to ODFIs and their Originators. These steps to staunch the flow of illicitly gained funds through the ACH Network also will thereby increase the security, stability and integrity of the ACH Network by making the fraudulent use of banking credentials to initiate ACH transactions more difficult and a less profitable proposition for criminal actors. We believe that these steps are completely consistent with the EFAA and Reg. CC, and that Congress never intended the EFAA to bar depository institutions from acting to prevent fraudulent transfers where there is a reasonable suspicion of a specific unauthorized transaction.

III. The EFAA and Reg. CC Do Not Prohibit the Hold Rules

Among other things, the EFAA generally requires that funds received by a depository institution by wire transfer for deposit to an account shall be made available for withdrawal no later than the business day after the business day on which such funds are received for deposit.[6] Through Reg. CC, the Board has extended these requirements to ACH credit transfers.[7] It is important to recognize, however, that the EFAA states only a financial institution's obligation to make funds initially available from various types of credits to an account. The EFAA says nothing about the ability of a financial institution to take action against funds previously made available in an account based on later arising circumstances and the rights or obligations of the depository arising under other laws. In short, once funds have been made available in an account, the EFAA and Reg. CC do not prohibit financial institutions from placing holds on those otherwise available funds for valid reasons, such as freezing the proceeds of a potentially fraudulent transfer. To the contrary, the provision of the EFAA that addresses post-availability holds in order to prevent evasion of the statute provides a clear implication that *holds for reasons other than later deposit of an additional check are not prohibited.*

Specifically, Section 607(d) of the EFAA provides as follows:

> In any case in which a check is deposited in an account at a depository institution and the funds represented by such check are not yet available for withdrawal pursuant to this chapter, the depository institution may not freeze any other funds in such account (which are otherwise available for withdrawal pursuant to

[6] 12 U.S.C. § 4002(a)(1)(B).

[7] *See* 12. C.F.R. § 229.2(p) and Comment P1 (Electronic Payment).

> this chapter) *solely* because the funds so deposited are not yet available for withdrawal.[8]

The word "solely" is critical here; by prohibiting reliance on subsequent deposit of additional checks as the "sole" reason for a future hold on other funds, Congress clearly implies that there may be other legitimate reasons for freezing funds that have been made available.[9] If Congress had intended that once made available funds could no longer become subject to hold, regardless of the reason, this limitation on freezing of funds would have been much more broadly worded. Instead, Congress focused very narrowly on the question whether subsequent freezes could be used to evade the statute. As the Board's own Commentary states, "This provision of the [EFAA] is designed to prevent evasion of the [EFAA's] availability requirements."[10] It is not designed to prevent action against funds in an account when a reasonable suspicion arises that those funds derive from illegal or unauthorized activity in the sender's account.

The Hold Rule, which is narrowly tailored to prevent the release of the proceeds of unauthorized transactions and to do so only when either the ODFI or RDFI has a reasonable belief that the ACH credit was unauthorized, in no way enables evasion of the statute. Indeed, in most cases the RDFI will be acting in response to notice from the ODFI that the original credit appears to have been unauthorized. It could hardly be said in such circumstances that the RDFI is attempting to evade the EFAA by responding in good faith to the ODFI's request.

Furthermore, the restrictions imposed by the Hold Rules would be equivalent to other holds that depositories are currently obligated or permitted to impose in connection with funds previously credited to the accounts they maintain. Examples of circumstances in which financial institutions routinely impose holds on funds include asset blocks required by the laws and regulations enforced by the Office of Foreign Assets Control, holds related to liens secured by funds held in an account and holds related to set off rights reserved by the account-holding financial institution. Indeed, in customer services questions and answers posted by the Office of the Comptroller of the Currency ("OCC"), the OCC expressly provides the following commentary: "A deposit was credited to my account by mistake. Can the bank freeze the account? Yes. The bank may freeze the account to ensure that no funds are withdrawn before the error is corrected. Or the bank may place a hold on the deposit."[11] Nothing in this OCC guidance suggests that a bank must have a court order or pursue some other legal process in order to hold funds that are reasonably suspected of being improperly credited to an account. Nor is there a suggestion that a financial institution must wait until an improper credit is definitively proven before it can take action to ensure that funds that are reasonably believed to

---

[8] 12 U.S.C. § 4006(d) (emphasis added).

[9] The Commentary also clearly notes that the statute only prohibits freezes of otherwise available funds when the sole reason is a later check deposit: "Section 607(d) of the EFA Act (12 U.S.C. 4006(d)) provides that once funds are available for withdrawal under the EFA Act, such funds shall not be frozen solely due to the subsequent deposit of additional checks that are not yet available for withdrawal." *Id.*

[10] 12 C.F.R. § 229.19(e), Comment E.1.

[11] OCC, Answers and Solutions for Customers of National Banks, Answers about Bank Errors, http://www.helpwithmybank.gov/faqs/banking_errors.html#drop08.

be improperly credited are not removed pending completion of the bank's investigation. Placing a temporary hold on funds in an account because of a reasonable belief that the funds are proceeds of an unauthorized transaction, rather than a simple error, certainly is no less justified.

Moreover, the Hold Rules also are consistent with the public policy goals articulated by Congress when adopting the EFAA. Representative John LaFalce, a co-sponsor of the legislation and member of the House Subcommittee with jurisdiction over the EFAA, in a statement made in support of the EFAA on the floor of the House of Representatives stated that:

> Providing banks with carefully circumscribed discretion to protect themselves against potential fraud also greatly benefits the consumer who otherwise would pay, either directly or indirectly, for the increased costs that widespread check kiting schemes might visit upon the banks. Moreover, several states have incorporated such good faith exceptions into their checkhold legislation, and have done so without undermining their basic thrust or engendering any consumer complaints. Indeed, one of the strongest proconsumer elements of this legislation is the provision which allows financial institutions to take reasoned steps to prevent fraud and thereby reduce costs which otherwise would be passed along to the consumer.[12]

While these comments were made to explain exceptions to the funds availability requirements in the EFAA when funds have not yet been made available, it is clear that Congress understood and supported the need for financial institutions to have flexibility in making funds available to customers to prevent fraud for the benefit of consumers.[13]

IV. Conclusion

In sum, the Hold Rules are consistent with both the language and policy rationale for the EFAA and Reg. CC, which do not restrict the ability of depository institutions to take appropriate action to freeze funds previously credited to deposit accounts in the event of suspected criminal activity. The tools provided by the Hold Rules are narrowly tailored to prevent and mitigate

---

[12] 133 Cong. Rec. H 3068 (daily ed. May 5, 1987) (statement of Rep. John LaFalce).

[13] Although Congress did not specifically identify the need to prevent fraud in the context of Corporate Account Takeover in electronic payment systems, this should not be interpreted to mean that Congress intended to afford less flexibility to financial institutions to prevent fraud in those systems. Rather, the general perception at the time the EFAA was adopted was that electronic payment systems were not vulnerable to fraud in same way that checks were. For example, in 1985, on behalf of the American Bankers Association, J. Kenneth Glass, testified in a Congressional hearing on the EFAA that "many [regularly recurring] payments ... can be received through automated clearinghouses, and others can be handled as wire transfers, Both of these electronic means of payment are secure against loss or theft and entail immediate and usually irrevocable credit to the receiver's account." *The Expedited Funds Availability Act: Hearings Before the Subcomm. on Financial Institutions Supervision, Regulation and Insurance of the House Comm. On Banking Finance and Urban Affairs on H.R. 2443*, 99th Cong. 34 (1985) (statement of J. Kenneth Glass, Executive Vice President, First Tennessee Bank, Memphis, TN, on behalf of The American Bankers Association).

risks associated with unauthorized ACH credit Entries and do not give ODFIs and RDFIs unfettered discretion to impose holds on Receiver funds. Rather the Hold Rules require the ODFI or RDFI to have a reasonable suspicion of an unauthorized transaction to impose such a hold. If they are unable to validate this belief within two business days, no longer than local checks may generally be held in the ordinary course prior to making funds available, they would be required to release the hold. Therefore, the specific, limited steps included in the Hold Rules, which are designed to thwart criminals from making off with the proceeds of Corporate Account Takeover, clearly do not fall within the limited prohibition of "evasion" of the statute through post-availability holds.

In light of the compelling policy arguments in favor of the Hold Rules and the lack of a clear bar against them, NACHA respectfully requests that the Board staff informally confirm that, consistent with the analysis above, the EFAA and Reg. CC do not prohibit an RDFI, either voluntarily or at an ODFI's request, from placing a hold on funds related to an ACH credit Entry that the RDFI previously made available to the Receiver in accordance the EFAA and Reg. CC if the RDFI or ODFI, respectively, has a reasonable suspicion that the Entry was not authorized. This confirmation will enable the banking industry to take steps to further protect their customers from losses due to fraudulent access to their accounts. If the Board were to take the position that the Hold Rules are inconsistent with the EFAA and Reg. CC, it would effectively undercut industry efforts to combat fraud without any demonstrable benefit to consumer protection, which was clearly of great importance to the authors and supporters of the legislation.

NACHA looks forward to working cooperatively with the Board staff to enable NACHA to implement *Rules* to protect the security and integrity of the ACH Network and its participants and their customers against the loss and damage caused by fraudulent ACH transfers.[14] Toward that end, NACHA also respectfully requests that the Board staff consider including a clarification regarding the foregoing in a future revision to the Reg CC Commentary.

[14] NACHA reserves for future discussion the possibility of permitting an RDFI to place a hold on funds related to an ACH credit Entry prior to making funds available to the Receiver if the ODFI requests the hold due to the ODFI's reasonable suspicion that the Entry was not authorized.