Remotely Created Checks and ACH Transactions: Analyzing the Differentiators

A Risk Management White Paper

This risk management white paper examines the uses of Remotely Created Checks (RCCs) and the distinctions that enable an informed choice between RCC and ACH transactions. The paper also identifies opportunities to make ACH transactions the payment method of choice in comparison to RCCs.

Table of Contents

Executive Summary

Remotely Created Checks (RCCs)[1] can be a useful payment device for some depositors under certain circumstances. In the current marketplace, RCCs may be used for recurring payments and collection activities authorized over the telephone, as well as contracts that necessitate same-day availability of funds. However, RCCs are also vulnerable to fraud because they do not bear a readily verifiable indication of authorization. In place of a signature, an RCC generally bears a statement that the customer authorized the check. It may also bear the customer's printed or typed name. A significant number of cases resulting from consumer and bank complaints allege fraud due to the exploitation of this vulnerability. Unfortunately, the volume of fraudulent RCCs cannot be factually quantified because of the difficulty of identifying RCCs among deposited items.

The Federal Reserve amended Regulation CC, effective July 1, 2006, to define RCCs and create transfer and presentment warranties that apply to RCCs that are transferred or presented by banks to other banks. The warranties apply only to banks and ultimately shift liability for losses attributable to an unauthorized RCC from the Paying Bank to the Depository Bank. The rights of checking account customers were not affected as they are not liable for unauthorized checks drawn on their accounts.

A newer product, a “non-check e-check,” is similar to an RCC, but is never an actual paper item. These non-check e-checks are payments authorized over the Internet, phone, or similar device that are sent through the check clearing system as an image, based solely on the payment instructions and not on any paper document. As non-check e-checks are not originally captured in paper, they cause a greater risk from both a risk management and legal standpoint. The legal framework for non-check e-checks is unclear. The Federal Reserve revised Operating Circular 3 on July 15, 2008 to specifically state, “Data sent to a Reserve Bank in the form of an electronic item is not an “electronic item” unless the data was captured from a check. By definition, the check from which the data was captured must be paper.”

To reduce the impact of both fraudulent intent and deceptive marketing messages, this paper introduces important factors for financial institutions to consider when dealing with RCC depositors. Institutions should also bear these factors in mind for customers that may switch from originating ACH debits to RCCs. Although many entities using RCCs operate without fraudulent intent, those that perpetrate fraud create significant harm to the payments system. Some entities market RCC services with outdated information, unknowingly or knowingly citing liabilities as they existed prior to the amendments to Regulation CC as a competitive advantage over ACH transactions. In addition, this paper includes a list of straightforward practices that, if followed by a financial institution, will help to mitigate the risk of fraudulent RCCs. These practices address the entire lifecycle of transactions from on-boarding to off-boarding RCC depositors, and for monitoring transactions and returns.

This risk management white paper cites current characteristics specific to the payment type that enable an informed choice between RCC and ACH transactions. It also identifies near-term opportunities to make ACH transactions the payment method of choice over RCCs (e.g., same-day settlement for specific ACH transactions, a change in the regulatory basis for a telephone authorization of recurring ACH debits, notice equals authorization for NSF fees). NACHA’s Risk Management Advisory Group (RMAG) concludes that: (1) ACH transactions offer a payment choice where the safeguards to Receivers outweigh the conveniences that RCCs currently offer to Payees and (2) with changes to the *NACHA Operating Rules,* the ACH Network can offer greater convenience with less risk for a range of payment applications.

[1] An RCC is defined in Regulation CC (Availability of Funds and Collection of Checks; 12 CFR Part 229.2 (fff) Definitions, Remotely Created Check) as a check that is not created by the Paying Bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn.

Participant Overview

Check Participants

Depository Bank

This financial institution is where the RCC is deposited or transferred. This institution is also known as the Bank of First Deposit. Transfer and presentment warranties for RCCs are held by the Depository Bank. This is equivalent to an ODFI of an ACH debit.

Paying Bank

This financial institution is where the RCC is payable. The Paying Bank is the financial institution whose routing number appears on the RCC and to which the RCC is sent for payment. This is equivalent to an RDFI of an ACH debit.

Payer

This is the person who owes the debt (i.e., the check writer). This is equivalent to the Receiver of an ACH debit.

Payee

A person to whom a check is made payable. This is equivalent to the Originator of an ACH debit.

ACH Participants

Originator

This is any individual or organization that initiates ACH debit or credit entries in accordance with an authorization from a Receiver. The Originator is usually a company directing a transfer of funds to or from a consumer's or other company's account.

Originating Depository Financial Institution (ODFI)

A participating financial institution that receives ACH files from Originators and delivers ACH entries to an ACH Operator.

ACH Operator

This is the entity that accepts files from ODFIs (or other ACH Operators), to sort and distribute ACH files to RDFIs (or other ACH Operators), and to effect settlement between the financial institutions that are parties to the transactions.

Receiving Depository Financial Institution (RDFI)

This is the financial institution that receives ACH entries from the ACH Operator and posts the ACH entries to Receivers.

Receiver

An individual, corporation, or other entity that has authorized an Originator to initiate a credit or debit entry to a transaction account held at an RDFI.

Figure A – The Forward Collection Flow for a Remotely Created Check

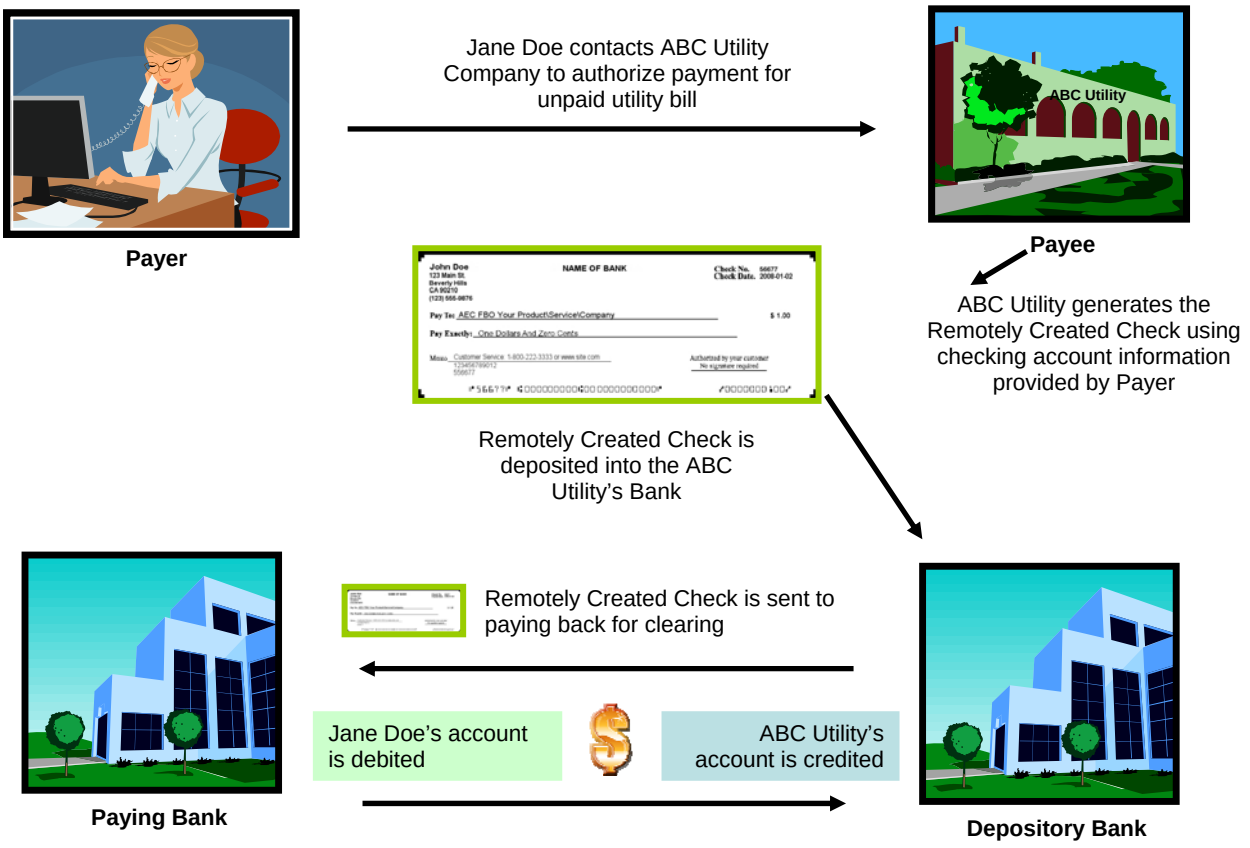
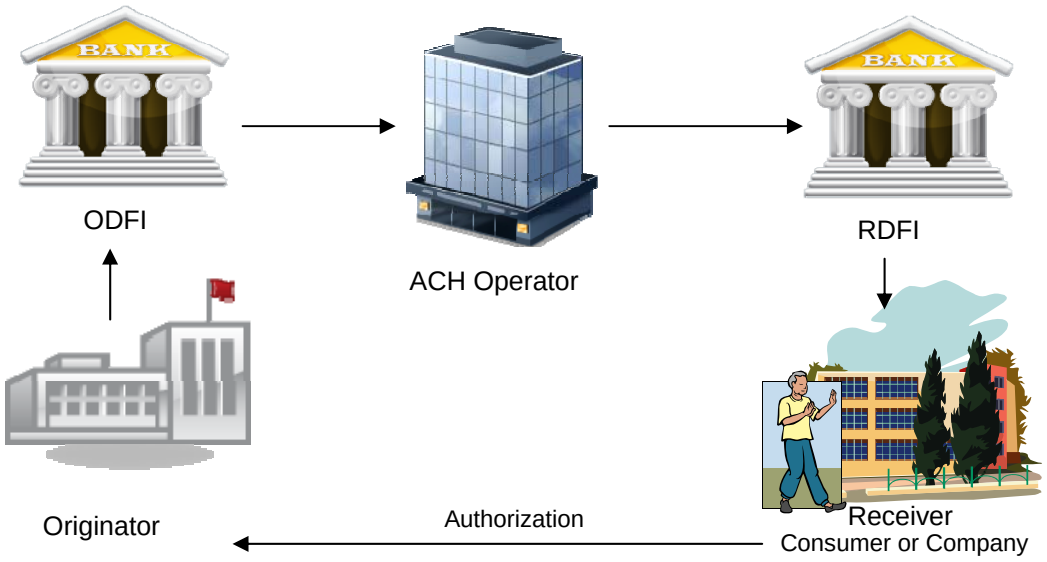


Figure B – The Transaction Flow for an ACH Debit Entry



Introduction

RCCs can be useful payment devices for some depositors under certain circumstances. In the current marketplace, RCCs are often used for recurring payments authorized over the telephone and collection activities because merchants and billers do not have good alternatives on other payment systems.

RCCs are particularly vulnerable to fraud because a fraudster can create an RCC solely based on having a bank account number and routing number. This vulnerability was the primary reason cited by the Canadian Payments Authority (CPA) to disallow RCCs (or "tele-cheques") as of January 27, 2004. A policy statement issued by the CPA Board of Directors in 2003 explained the board's reasoning:

> "The key risk associated with a tele-cheque is fraud (i.e., risk of unauthorized payment). This particular type of payment does not contain the signature of the Payor nor is it supported by any other form of signed authorization. Given this, it is impossible for the Payor financial institution to verify that the Payor has in fact authorized the Payee to act as a signatory for the specific payment. Furthermore, the risk of unauthorized payments is elevated since a Payee could issue a tele-cheque against a Payor's account simply after obtaining the necessary account details. In this regard, to permit tele-cheque entry into the clearing system would increase the risk that unauthorized parties would use this vehicle to gain access to deposit accounts fraudulently.
>
> In studying the tele-cheque issue, the CPA considered whether procedures could be put in place to sufficiently mitigate the risks associated with this payment instrument. In its assessment, the CPA consulted broadly with financial institutions and payment system service providers and users. There was a generally held view that tele-cheques represent an unacceptable level of risk, since the key to mitigating the risk of unauthorized transactions is the ability to verify authorization."[2]

The CPA acted because they believed RCCs represented an "unacceptable level of risk." At the time of their decision to eliminate RCCs in June 2003, the CPA was not aware of any fraudulent use of these items in Canada. Their action was a proactive measure to address heightened risk.

The National Association of Attorneys General also articulated concerns about fraud in a letter to the Federal Reserve Board in May 2005. This letter, in response to a proposed amendment to Regulation CC for RCCs, stated its position at the time related to RCCs:

> "In brief, the Attorneys General take the position that demand drafts are frequently used to perpetrate fraud on consumers; that such drafts should be eliminated in favor of electronic funds transfers that can serve the same payment function; that if demand drafts are to continue to be used, the proposed originating bank warranty of authorization should augment, not supplant, the existing receiving bank warranty; that demand drafts should be mandatorily marked as such; and that serious consideration should be given to extending the midnight deadline for returning unauthorized items to 60 days, as long as the ACH system is not adversely affected."[3]

Non-check e-checks are similar to RCCs but have a key difference. An actual paper item never exists. These non-check e-checks are payments that start as electronic payment instructions obtained over the Internet, phone or similar device that are then converted to an image for clearing through the check clearing system. Non-check e-checks that are not originally captured via a paper document cause greater risk than RCCs because they are even more difficult to identify and monitor and because their legal framework is not clearly defined.

---

[2] "Prohibition of Tele-cheques in the Clearing and Settlement System - Policy Statement," Canadian Payments Association. (June 1, 2003) http://www.cdnpay.ca/news/tele.asp

[3] Comment to FRB Docket No. R-1226 (Proposed Amendment to Regulation CC/Remotely Created Checks), May 3, 2005, National Association of Attorneys General http://www.federalreserve.gov/SECRS/2005/May/20050512/R-1226/R-1226_264_1.pdf

Although many entities using RCCs operate without fraudulent intent, those who perpetrate fraud create significant adverse impact to the payments system. This risk management white paper explains characteristics that enable an informed choice between RCC, non-check e-check, and ACH transactions. It also identifies near-term opportunities that could make ACH transactions a payment method of choice over RCCs and non-check e-checks for all parties to a transaction in qualifying payment situations.

Legal Issues

The following paragraphs describe the authorization requirements, as well as the warranties and liabilities of the various parties for each of the payment instruments.

RCCs - Transfer and Presentment Warranties & Authorization Requirements

The Depository Bank has a different liability for RCCs than it does for other checks or images. The different liability is the result of warranties defined in Regulation CC, stating that "a bank that transfers or presents a RCC, and receives settlement or other consideration warrants to the transferee bank, any subsequent collecting bank, and the paying bank that the person on whose account the RCC is drawn, authorized the issuance of the check in the amount stated on the check and to the payee stated on the check."[4] This warranty has the effect of shifting the traditional check liability from the Paying Bank to the Depository Bank. For these reasons, a Depository Bank should have a process to identify and review RCCs. Because they are often included in bulk deposits and are not easily distinguishable from other checks, Depository Banks most often find that a manual process is required to identify RCCs.

The Uniform Commercial Code addresses the authorization of an RCC. Authorization of an RCC may be by writing or by telephone, subject to compliance with applicable state law, if any.[5] "If a person acting … as a representative signs an instrument … the represented person is bound by the signature to the same extent the represented person would be bound if the signature were on a simple contract." The signature can be via use of a word, mark, or symbol.[6]

Non-Check E-Checks – Unclear Legal Framework

There is no defined legal framework for non-check e-checks as these payments created from payment instructions received over the Internet, phone, or other similar device never exist in paper form. The Federal Reserve's Operating Circular 3 states these payments are not eligible for collection through the Federal Reserve's check image services, and the Federal Reserve has no liability for them.

ACH – ODFI Warranties & Authorization Requirements

The *Rules* provide that an ODFI warrants that each entry transmitted by the ODFI is in accordance with proper authorization provided by the Originator and the Receiver.[7] Each ACH Standard Entry Class (SEC) Code has authorization requirements that are aligned with how the account information for the ACH transaction is provided. Some ACH debits to consumer accounts are authorized in writing, some are authorized orally, and some by receipt of a notice. For instance, Internet-Initiated Entries (WEB) transactions are authorized in writing that is similarly authenticated by the consumer over the Internet. The authorization must be readily identifiable as an authorization and its terms must be clearly and readily understandable. The authorization process must evidence both the consumer's identify and his assent to the authorization.[8] Authorization of Telephone Initiated Entries (TEL) transactions are authorized orally where the Originator must either: (1) record the oral authorization, or (2) provide the Receiver with written

[4] Regulation CC – Availability of Funds and Collection of Checks; 12 CFR Part 229.34 (d)(1) Transfer and presentment warranties with respect to a Remotely Created Check
[5] Uniform Commercial Code, Section 1-103
[6] Uniform Commercial Code, Sections 3-401 – 3-402
[7] *NACHA Operating Rules*, Section 2.2.1.1, Authorization by Originator and Receiver
[8] *NACHA Operating Rules*, Subsection 2.1.2, Receiver Authorization and Agreement

notice confirming the oral authorization prior to the settlement date of the entry.[9] TEL transactions are limited to single-entry payments. The authorization requirements for Accounts Receivable Entries (ARC) and Back Office Conversion (BOC) Entries are authorized by notice where the authorization is accomplished through the consumer's receipt of a notice followed by the Originator's receipt of the consumer's source document (check).

The Electronic Funds Transfer Act (EFTA), 15 U.S.C. 1601 note, and Regulation E permits preauthorized electronic funds transfers from a consumer's account if the transactions are authorized in a writing that is signed or similarly authenticated by the consumer. "Preauthorized electronic fund transfers from a consumer's account may be authorized only by a writing signed or similarly authenticated by the consumer."[10]

It is important to note that Regulation E has evolved over the last few years, acknowledging the important role that technology can play in the capture of valid authorizations. Until 2007, the Official Staff Commentary to Regulation E specifically precluded the use of a recorded telephone conversation in order to satisfy the requirement for written authorization. In 2007, the Board of Governors of the Federal Reserve System amended the Official Staff Commentary to eliminate the commentary that prohibited oral authorization for preauthorized debits, but did not provide guidance on how oral authorizations can be properly obtained. Regulation E permits preauthorized transfers from a consumer account as long as the form of the preauthorization satisfies the requirement of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7001 et seq. (E-Sign Act) for treatment of an electronic communication as the equivalent of a writing.

The Official Staff Commentary to Regulation E refers to the E-Sign Act:

> "The similarly authenticated standard permits signed, written authorizations to be provided electronically. The writing and signature requirements of this section are satisfied by complying with the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7001 et seq., which defines electronic records and electronic signatures. Examples of electronic signatures include, but are not limited to, digital signatures and security codes. A security code need not originate with the account-holding institution. The authorization process should evidence the consumer's identity and assent to the authorization. The person that obtains the authorization must provide a copy of the terms of the authorization to the consumer either electronically or in paper form. Only the consumer may authorize the transfer and not, for example, a third-party merchant on behalf of the consumer."[11]

Therefore, the *Rul*es prohibition on telephone authorization for recurring payments is more restrictive than the current requirements of Regulation E.

Appendix A of this paper summarizes the legal framework supporting RCCs, ACH Transactions, and non-check e-checks.

RCC Characteristics and Differentiators

While abuses of RCCs grab attention and make headlines, several legitimate uses exist. The examples below do not form an exhaustive list of all possible legitimate uses of RCCs, but they may represent the majority of such uses. They describe a few common scenarios in which one or both parties to a transaction choose to create an RCC because of its characteristics and the lack of alternatives.

[9] *NACHA Operating Rules*, Section 2.1.8, Authorization for Telephone-Initiated Entries
[10] Regulation E – Electronic Fund Transfers; 12 CFR Part 205.10 (b) Preauthorized Transfers
[11] Regulation E – Electronic Fund Transfers; 12 CFR Part 205, Supplement I to Part 205 - Official Staff Interpretations, Section 205.10, Paragraph 10(b)5

- **Same-Day Availability**

  When a consumer negotiates a contract such as an insurance policy over the telephone, he or she may authorize either an ACH TEL entry or an RCC to pay the initial premium. However, if the consumer wishes to make the policy effective on the day of the conversation, the insurance provider will likely ask the consumer to authorize an RCC. The insurance company can deposit the RCC and receive same-day availability of the funds; whereas if a TEL debit is used, the insurance company is credited on the effective date of the TEL debit to the consumer, thereby delaying the date on which the policy takes effect by a day or two.

- **Recurring Telephone-Initiated Debits**

  Merchants, insurance companies, and debt collectors all need the ability to accept recurring payments over the telephone. For example, some merchants who offer payment plans find it convenient to set up recurring debits over the phone. When they set up the plan with their customer, they obtain a single authorization for a series of recurring debits. The *Rules* do not allow the TEL application to be used for recurring debits based on a single authorization obtained over the telephone. Similarly, insurance companies also want to be able to set up recurring payments to collect monthly insurance premiums. For a collection agency to use the TEL application, a collector would have to make a call for each payment, greatly reducing the efficiency of the collection process. As with recurring debits for bills or purchases, agencies that conduct legitimate collection activities over the telephone often negotiate payment options with debtors. A repayment option may include a payment plan spread over weeks or months. These collectors prefer to set up a recurring date on which to deposit an RCC rather than schedule a call to get a new authorization for each subsequent ACH payment.

- **Collection of NSF Fees**

  Retailers often use RCCs to collect NSF fees on returned checks. They do this in accordance with notices posted at the point of checkout. Notices that are appropriately worded and prominently displayed satisfy notification requirements and support a legitimate use of RCCs. The *Rules* require that ACH debits to collect NSF fees be authorized in a writing that is signed or similarly authenticated. This takes valuable time at the point-of-sale where efficiency can be measured in seconds. The extra time necessary to obtain a signed authorization makes using an ACH debit less efficient for collecting NSF fees at the point-of-sale.

Potential Improvements to ACH Transactions

- **Same-Day Payments**

  Although same-day availability can lead depositors and consumers to prefer RCCs over ACH in certain payment situations, this difference between the transactions may soon disappear. In March 2009, the Federal Reserve announced a plan to develop an intraday service for certain ACH debits. The service would be restricted to consumer checks converted to ACH as well as consumer debits generated from Internet and telephone transactions. Institutions that opt-in to this service will eliminate the difference in availability their customers experience when using RCCs and ACH debits.

- **Recurring TEL Transactions**

  TEL transactions were created in 2001 to allow for the oral authorization of a single ACH debit to a Receiver's account. This application was modeled after the FTC's 1995 Telemarketing Sales Rule that established a framework to allow paper drafts to be authorized over the telephone via an oral authorization that is tape-recorded. At that time, the Official Staff Commentary on Regulation E explicitly prohibited the oral authorization of preauthorized debits. In 2007, the Federal Reserve Board

amended the Official Staff Commentary on Regulation E and removed the prohibition related to capturing a tape recording, thereby creating an opportunity to expand TEL transactions to include recurring transactions.

The *Rules* have not yet been changed to reflect the changes to Regulation E. This limitation within the *Rules* precludes the use of TEL transactions in situations in which depositors prefer to rely on a telephone authorization for recurring payments. This limitation helps make the RCC better qualified to serve payees' needs in these situations, and a change to the *Rules* could give depositors another option for recurring debit transactions based on an authorization obtained over the telephone. NACHA is currently using its rulemaking process to consider whether to allow for recurring debits to be authorized by telephone.

- **Notice Equals Authorization**

  The *Rules* require that NSF fees that are collected via the ACH Network be authorized by a writing that is signed or similarly authenticated. This requirement is inefficient for merchants that would prefer to have the authorization to transmit an NSF fee without the additional time at check-out to obtain a signed authorization, or the follow-up needed to obtain authorization after a check bounces or an ACH debit is returned. NSF fees can be collected via RCCs with notice at the point of checkout. Regulation E does not require a written authorization for a single payment to collect service fees. NACHA is currently using its rulemaking process to consider allowing notice equals authorization for service fees.

- **Identifying Transactions: Monitoring Returns and Noticing Problems**

  The ability to identify transactions also differentiates ACH from RCCs. RCCs are indistinguishable from signed checks when included in bulk deposits of paper items that are processed by automated means. This makes hard data on RCCs difficult to obtain. Since financial institutions cannot conclusively identify all RCCs in forward collection, return rates are difficult to calculate. As a result, the preponderance of evidence related to RCCs is anecdotal and tends to focus on exceptions and negative experiences.

  Conversely, financial institutions have the ability to identify both forward and return ACH activity. ACH entries can be counted with ease. The ability to track ACH activity by Standard Entry Class (SEC) Code and by Return Reason Code enables identification of problem Originators. This ability provides a critical risk mitigation tool to financial institutions that originate ACH transactions. Consequently, a problem with RCC returns is more difficult to detect than a problem with ACH returns.

- **Due Diligence**

  An ODFI on-boarding a new ACH Originator takes several steps to complete its due diligence for that Originator before transmitting ACH transactions. The ODFI must establish the credit worthiness of the Originator and sign an agreement that outlines obligations and liabilities for ACH transactions. The *Rules* currently requires the ODFI to establish and monitor the Originator's exposure limits. As of June 2010, the *Rules* specifically incorporate due diligence provisions related to the ODFI's relationship with its Originator. This includes the ODFI having to have formed a reasonable belief that the Originator has the capacity to perform its obligation under the *Rules,* assessing the nature of the Originator's activity, and enforcing restrictions on the types of ACH transactions that are originated. A bank that establishes a relationship with a depositor of RCCs is not required to do any of these due diligence steps.

Factors to Consider – RCCs versus ACH Transactions

Financial institutions and the industry have certain factors to consider when determining whether to continue use of RCCs. A financial institution should consider its own set of questions, as outlined below, when determining whether or not to accept RCC deposits from its customers. Additionally, in light of risks

associated with RCC abuse, challenges in monitoring this type of transaction, and possibly unnecessary restrictions on ACH transactions, the payments industry should consider how it might best utilize available payment mechanisms, and modify rules and regulations to meet legitimate payment needs while minimizing risk.

Financial Institutions

- Do Originators and depositors receive appropriate due diligence during on-boarding?
    - Will your institution require depositors to disclose their intent to deposit RCCs?
    - Will your institution utilize the same pre-approval and underwriting processes for RCCs that are used for ACH?
    - Will your institution provide depositors with guidelines on expectations and prohibited activity?
- Can transaction and account monitoring enable quick identification of problem ACH Originators and RCC depositors?
    - Will special attention be paid to unauthorized returns and adjustment entries?
    - Will red flag thresholds be set?
    - Will an escalation process be defined to enable action to be taken to confront a depositor about questionable practices, and to off-board a depositor if necessary?
- Does the Depository Bank understand that the warranties it is making for an RCC are different than for images or other checks?

Industry

- Should the *Rules* be modified to allow recurring debits based on an oral telephone authorization?
- Should the *Rules* be modified to allow for notice equals authorization for the collection of NSF fees?
- Should same-day availability for specific ACH transactions exist as a matter of course, without an opt-in requirement?
- Can RCCs be monitored reliably and consistently by financial institutions of varying capability?
- Can non-check e-checks be monitored reliably and consistently by financial institutions?

Practices to Mitigate the Risk of Fraudulent RCCs

RCCs present a unique set of risks for consumers and for financial institutions that accept RCC deposits. A depository financial institution can mitigate the risk of fraudulent RCCs by following a few straightforward practices:

- Require disclosure by depositors of intent to deposit RCCs. Include this requirement in commercial deposit agreements.
- Bring RCC depositors on board like ACH Originators, including appropriate pre-approval and underwriting.
- Tell RCC depositors what they can and cannot do by providing a set of guidelines that describe expectations and prohibited activity.
- Monitor return rates, with special attention to unauthorized returns and adjustment requests.
- Establish red flag thresholds.
- Define an escalation process that enables the institution to act decisively to confront a depositor about questionable practices.
- Define an off-boarding process for bad actors that preserves the financial institution's rights and limits its exposure.

Some of these practices are more difficult to put in place than others, but together they form an integrated approach to managing RCC risks. They also echo requirements stated in OCC Bulletin 2008-12, *Risk Management Guidance on Payment Processors,* which describe the risks associated with depositors who may abuse RCCs. The guidance states: "Banks have two distinct areas of responsibility to control these risks. The first is due diligence and underwriting, and the second is monitoring these high-risk accounts for high levels of unauthorized returns and for suspicious or unusual patterns of activity."

Conclusion

It is incumbent upon a financial institution that enables RCCs, non-check e-checks, or ACH payment activity to understand the underlying business activity of its customers in order to steer their customers toward appropriate use of the transaction type that best serves their legitimate needs. It is also incumbent for that financial institution to confront those customers who do not appropriately utilize either the check or ACH payment systems.

NACHA's Risk Management Advisory Group concludes that ACH debit transactions, such as TEL transactions, offer a payment choice where the safeguards to Receivers outweigh the conveniences that RCCs currently offer to Payees. This conclusion is based on the following factors: (1) the heightened risk profile of RCC transactions that bear no evidence of authorization, (2) the fact that ACH transactions can be identified and monitored with relative ease, and (3) the fact that the *Rules* include clear and explicit authorization requirements for capturing evidence of a consumer's authorization of a transaction.

The Risk Management Advisory Group concludes further that NACHA and ACH Network participants should consider the benefits of same-day settlement for specific ACH transactions, allowing recurring TEL transactions, and allowing notice equals authorization for NSF fees. These changes would enable the ACH Network to offer greater convenience with lower risk for a range of payment applications.

Appendix A – Legal Framework
RCCs, ACH Transactions, and non-check e-checks

	RCC	ACH	non-check e-checks
Regulations	Regulation CC UCC FTC	*NACHA Operating Rules* Regulation E FTC	Undefined
Authorization Requirements	Authorization may be by writing or by telephone, subject to compliance with applicable state law, if any. (UCC § 1-103) "If a person acting… as a representative signs an instrument… the represented person is bound by the signature to the same extent the represented person would be bound if the signature were on a simple contract." The signature can be via use of a word, mark, or symbol. (UCC §§ 3-401 – 3-402) Subject to compliance with applicable state law, NSF or UCF Fees can be collected by notice at point of checkout or by other means evidencing an authorization. The FTC's Telemarketing Sales Rule (68 Fed. Reg. 4669, January 23, 2003) requires that an authorization be written or oral. The written authorization must be signed by the customer. The signature may be an electronic or digital form. The oral authorization must be tape recorded.	Each ACH Standard Entry Class (SEC) Code has authorization requirements that are aligned with how the account information for the ACH transaction is provided. Some ACH debits to consumer accounts are authorized in writing, some are authorized orally, and some by receipt of a notice. WEB: The written authorization is similarly authenticated by the consumer over the Internet, must be readily identifiable as an authorization, and its terms must be clearly and readily understandable. The authorization process must evidence both the consumer's identity and his assent to the authorization. An electronic authorization must be able to be displayed on a computer screen or other visual display that enables the consumer to read the communication. The writing and signature requirements are satisfied by compliance with the Electronic Signatures in Global and National Commerce Act. (*NACHA Operating Rules* § 2.1.2) TEL: The Originator must obtain an oral authorization from the consumer and either (1) tape record the oral authorization, or (2) provide the Receiver with written notice confirming the oral authorization prior to the settlement date of the entry. (*NACHA Operating Rules* § 2.1.8) ARC/BOC: The authorization is accomplished through the consumer's receipt of a notice followed by the Originator's receipt of the consumer's source document. (*NACHA Operating Rules* § 2.1.2)	Undefined

	RCC	ACH	non-check e-checks
Return Timeframes and Warranty Claims	Paying bank has up to midnight of the banking day following the banking day of presentment to return the RCC for any reason. (UCC §§ 4-301 and 4-302) The clearing houses have adopted Rule 8 allowing a warranty claim for an unauthorized RCC through the return check process for 60 days from statement. The Federal Reserve Banks allow a warranty claim for an unauthorized RCC through an adjustment process within 90 days of the cash letter. Neither clearing house rules nor the Federal Reserve Banks prohibit a warranty claim for an unauthorized RCC within one year, if those claims are outside the check collection system.	ACH debit transactions can be returned for NSF or UCF within two days of the settlement date of the original entry. (*NACHA Operating Rules* § 6.1.2) Regulation E provides for dispute resolution rights and provisional recredit for an unauthorized transaction for 60 days from statement. (Regulation E §§ 205.6 and 205.11) Regulation E does not provide for the RDFI returning the transaction to the ODFI; however, the *NACHA Operating Rule* allow consumer debit transactions to be returned by the RDFI on behalf of the Receiver if the transaction was unauthorized and the Receiver signs a WSUPP for 60 days from settlement date. (*NACHA Operating Rules* § 8.6.1*)*	Undefined

Warranties	A bank that transfers or presents an RCC, and receives settlement or other consideration warrants to the transferee bank, any subsequent collecting bank, and the paying bank that the person on whose account the remotely created check is drawn authorized the issuance of the check in the amount stated on the check and to the payee stated on the check. (Regulation CC § 229.34(d)(1))	The ODFI warrants the transaction was authorized. (*NACHA Operating Rules* § 2.2.1.1) The ODFI also warrants: WEB: Originator has employed commercially reasonable procedures to verify the identity of the Receiver. (*NACHA Operating Rules* § 3.9.3) Originator has used commercially reasonable procedures to verify that routing numbers are valid. (*NACHA Operating Rules* § 3.9.2) Originator has employed a commercially reasonable fraudulent transaction detection system to screen each entry. (*NACHA Operating Rules* § 3.9.1) Originator has conducted an annual audit to ensure financial information obtained from Receivers is protected by minimum security practices and procedures. (*NACHA Operating Rules* § 3.9.4) TEL: Originator has employed commercially reasonable procedures to verify the identity of the Receiver. (*NACHA Operating Rules* § 3.10.1) Originator has used commercially reasonable procedures to verify that routing numbers are valid. (*NACHA Operating Rules* § 3.10.2) BOC: Originator must employ commercially reasonable procedures to verify the identity of the Receiver. Warranties also cover the notice obligation, source documents, proper capture of the MICR information, providing a customer service phone number and securely storing payment information. *(NACHA Operating Rules* § 3.7) ARC: Warranties cover notice obligation, source documents, secure storage of payment information, and proper capture of the MICR information. *(NACHA Operating Rules* § 3.6)	Undefined

NACHA — **The Electronic Payments Association** supports the growth of the ACH Network by managing its development, administration, and governance. The ACH Network facilitates global commerce by serving as a safe, efficient, ubiquitous, and high-quality electronic payment system. More than 15,000 depository financial institutions originated and received 18.2 billion ACH payments in 2008. NACHA represents nearly 11,000 financial institutions through 18 regional payments associations and direct membership. Through its industry councils and forums, NACHA brings together payments system stakeholder organizations to encourage the efficient utilization of the ACH Network and develop new ways to use the Network to benefit its diverse set of participants. To learn more, visit www.nacha.org, www.electronicpayments.org and www.payitgreen.org.

The Risk Management Advisory Group is dedicated to establishing best practices for risk management, developing rules necessary to assure ongoing strength and stability, and improving quality in the ACH Network. This Group's achievements include significant contributions to the NACHA rules process and to Network education around the changing face of ACH payments risk. The Risk Management Advisory Group advises the NACHA Board and works with staff to guide and implement the risk management strategy. This Group plays a vital role in developing and promulgating a comprehensive approach to Network risk management, working with NACHA staff and key industry stakeholders to produce best practices and rules recommendations, and to share findings with payments professionals across payments channels.