RCC Identifier White Paper
RCC Identifier

BACKGROUND

Remotely Created Checks (RCC) has been a valid payment instrument for many years going back to at least the 1960’s. An RCC is generally created by the Payee, when a customer provides proper authorization to create the RCC; the check is unsigned by the drawer customer.

These instruments are used for some of the following purposes:
- Telephone Marketing
- Bill Payments
- Loan repayments
- Recurring insurance premiums (used to be called Preauthorized Check or PACs)
- Internet and web purchases
- Alternative in ACH Check conversion when the check cannot be converted to ACH or the ACH entry has been returned
- Others

While RCCs are believed by some to be the source of fraudulent transactions, there are significant legitimate uses for this payment instrument. According to the Federal Reserve’s 2010 Payment Study (most recent survey results), approximately 2.1% of the 24.5 billion checks are RCCs with an estimated volume of RCCs of 515 million.

PROBLEM STATEMENT

Generally most RCCs are properly authorized and flow through the check clearing system and are paid by the paying bank without issue. Banks do report significant increases in returns of RCCs as unauthorized from certain "bad actors" in the industry. These "bad actors" will deposit these unauthorized RCCs in one or more depositary financial institutions. The paying banks to which these items are drawn will see a significant raise in their return rates to these depositary banks (as high as 30%). Returns to specific depositary banks can include unauthorized RCCs and other return reasons like NSFs which may have been caused due to the unauthorized transactions. Many paying banks and depositary banks will take action once they determine a "bad actor" has entered the system. Paying banks will dishonor these unauthorized transactions and notify the depositary banks and depositary banks may discontinue doing business with these companies. These "bad actor" may move to other financial institutions. Federal supervisory guidance recommends that depositary banks monitor merchant return rates.

Unauthorized RCCs cause the following issues for financial institutions:

- **Cost**
  - Paying bank costs of handling and processing returns and/or adjustments
  - Depositary bank’s costs of receiving returns and/or adjustments
  - Customer service costs to paying bank
- **Risk**
  - Depositary bank risk that funds have left the bank
  - Risk of loss to customers, especially consumer customers
  - Financial risk to paying bank
  - Reputational risk to depositary and paying bank
Currently there is no automated manner in which to identify an RCC. Without a physical examination of the item, a bank does not know whether or not the item contains a signature.

The ability to automatically identify these transactions is needed.

### ASSUMPTIONS/DEFINITIONS

- **RCC** - “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” (Reg. CC - Section 229.2(fff)).
  - This definition does not include unsigned drafts generated by the paying bank or by a bill payment service acting on behalf of the paying bank.

- **EPC** - External Processing Code
  - The EPC field\(^1\) assists in determining how a check is processed. The EPC consists of one character, with a specific assigned digit (0-9) to identify the processing of the item. The standard organization X9\(^2\) assigns the digits.
    - X9 controls and assigns the EPC MICR identifier. The digits are limited in number and are assigned only after proof of process viability, sometimes following a pilot for trial use.

- Creator of RCCs or its depository bank would need to apply the EPC code in the MICR line of the RCC.

- Proper use and enforcement will be necessary for effectiveness.

### ENFORCEMENT/JUSTIFICATION

Depository banks through its account agreements are the only banks in the payment system that can enforce the use of the identifier.

Incentives for depositary banks to require the identifier:

- Enhances ability to track return item trends, as required by bank regulators. It allows banks to identify and act on high-risk depositors and take appropriate actions when thresholds indicate cause to scrutinize merchant activity.
- Facilitates early intervention to consumer targeted scams, obviating potential reputational or jurisdictional risk.

The use of an External Processing Code (EPC) to identify an RCC would enable processing financial institutions to:

- Identify automatically RCCs in normal processing

---

\(^1\) The EPC is defined in the governing standard as “a MICR digit that conveys special information regarding the correct handling or routing of a check or check data by financial institutions and other processors.” On larger checks, the field could encompass Positions 44 and 45, but the challenges associated with implementing a 2-digit EPC field have forestalled this use.

\(^2\) X9 is a Subcommittee of the Accredited Standards Committee X9, Inc., Financial Industry Standards. X9 deals with checks and check processing.
• Out sort RCCs for special handling, if desired
• Track RCCs volumes
• Facilitate identification of potential warranty claims for unauthorized RCCs

**PROPOSAL**

Determine if there is industry support for an EPC digit to flag RCCs initially as a pilot, with future intent for a permanent code. Socialize the concept through various industry groups and forums including, but not limited to the following:
• X9
• ECCHO
• TCH
• Viewpointe
• BAI Payments Connect
• Others

Determine if a pilot should be implemented.

Assign EPC value of "6" with the following definition - "Assigned for usage on Remotely Created Check (RCC). The code shall be placed on the RCC (draft) prior to processing through the payment system.

**PILOT JUSTIFICATION**

An EPC pilot will allow a digit to be used “on a trial basis”, and the permanent EPC assignment would follow after the related pilot is deemed successful.
• Permanent assignment would occur on the normal X9 schedule for the standard.

Proper use and enforcement will be necessary for effectiveness.

When and if a pilot is deemed successful, submit request to X9 for permanent EPC digit assignment.

Limitation of Pilot: If banks chose to participate in the pilot, it is likely they will code RCCs going to many institutions. Institutions participating in the pilot will be able to recognize the identifier and act accordingly. Institutions not participating in the pilot should ignore the new code. System issues may occur for institutions not prepared for the new code. This is assumed unlikely to occur.

**LIMITATIONS/ISSUES**

While the addition and use of an EPC digit for the identification of RCCs may prove beneficial to the industry, it is important to understand the limitations of this identification. It should not be assumed that having an identification method will necessarily identify all RCCs. These limitation/issues follow:
• Depending on the digit assigned, there is always the possibility of read errors, as with any MICR character.
• Not all institutions will chose to interrogate the field
  o Not all institutions will have the capability to read and interrogate the field
• Not all institutions will enforce the use of the field
• Since the recommendation is for one EPC digit, it will be possible for the RCC digit to be over written by an IRD digit
  o For example an RCC is created with the valid ECP digit. The item is imaged and sent through the check processing system as an image and then returned as an image. At the depositary bank, an IRD is created to provide to the depositing customer. Once that IRD is created the RCC EPC digit will be replaced with the IRD EPC digit.
    ▪ If that item is then represented banks will only know it is an RCC, if the item is physically examined or the original MICR line (read high) is read.
• Banks are going to need to ensure that this new EPC digit will not cause issues with their hardware and software systems.
• Standards are voluntary, so the use of this digit will be dependent on the depositary bank requiring its use. "Bad actors" who are trying to defraud individuals and companies will likely not use the digit.