

Meeting The Check 21 and RDC Error and Fraud Threats

A Case Study

In 2005, Southern Commercial Bank in St. Louis was looking into the future. They are an aggressive ten location community bank in the St. Louis and adjoining Jefferson County areas, with a major business lending portfolio and a strong retail presence. They planned to actively promote remote deposit capture. They were looking at any other technology based on Check 21 that would help them maintain and increase their market share, and reduce costs.

As they worked through the implications of the widespread adoption of Check 21 and remote deposit capture, they saw both major opportunities and serious new threats. The greatly increased likelihood of both mistakes and fraud loomed as a serious problem.

Before Check 21, checks either wound up back with their maker, or in the possession of a bank. With IRD creation now widely available, and remote deposit capture leaving untold millions of checks in the hands of the public, the opportunity for checks to be presented more than once was a new threat that would have to be handled.

Southern Commercial was in the process of implementing image presentment and acceptance, branch capture, CAR/LAR, and remote deposit capture using software provided by MICR Automation.

It became apparent that their existing software would not be adequate to catch

the errors and potential fraud they saw on the horizon. A new system dedicated to meeting this threat would be needed. After searching the marketplace, it was decided that their needs could best be met by creating an entirely new system.

Art Kniffen and Rick Bampton, both Senior Vice Presidents at Southern Commercial, created a series of threat scenarios to guide them in the definition of the new fraud detection software.

Defining the Threat Scenarios

The first and most obvious scenario was simply human mistake. With checks in the hands of the businesses receiving them, the chances for one or more to be scanned in, and then either scanned again or deposited with a teller, are always present. The new system had to catch not only duplicate electronic RDC items, but had to find any RDC item coming through again as a paper item.

Additional scenarios involved the ways criminals could take advantage of the new Check 21 environment.

With criminal involvement, checks deposited via RDC can easily be taken from their original payee and deposited again by a different business through a different bank.

The presence of millions of checks in public hands also invites criminals to use high quality scans of actual checks and edit them, creating new fraudulent

checks. These new checks have perfect signatures and perfect backgrounds, and can be made payable to any payee for any amount. Large numbers of apparently perfect under \$100 check images, created by criminals and designed to not overdraw typical accounts, are possible. Files of high quality images of actual checks are likely to become articles of commerce among criminal elements in the Internet world, like stolen credit card numbers are today.

Since all RDC systems allow the MICR information to be edited, changed check numbers and/or amounts could allow the same check to be deposited multiple times without being caught as a duplicate. Southern Commercial uses CAR/LAR to test the RDC items submitted by its customers, and to check its image inclearings. RDC presentments of checks through other banks may have information changed or omitted.

Three Categories of Solutions – Implementation of Testing Rules

To address these threats, approaches in three areas were implemented. The first utilizes a profile of daily activity for each account, and compares the current activity against it. The second involves a series of tests of the data in incoming items and deposits. The third gets the customer involved by automatically emailing customers a short summary of account activity each day.

For maximum flexibility, all the tests in the first two areas were implemented as Rules. Rules may be applied globally, or to specific accounts or classes of accounts. White lists allow specific

accounts to be excluded from a rule. Multiple instances of the same rule allow different parameters to be applied to specific accounts or groups.

Activity Statistical Analysis Rule:

Activity Statistical Analysis matches individual account daily activity against the same period in previous months. The rule allows setting the number of days to attempt to fit the pattern before and after the current day, and allows setting a History Check Period to create and maintain the daily statistics. By setting the tolerance the rule can be tailored to all types of accounts. As with all the rules, several different iterations can be implemented and applied to different groups of accounts.

Duplicated On-Us Debits Rule:

The Duplicates Rule finds both duplicate check numbers and duplicate entire checks. Outright duplicates of the same item are one of the most likely situations arising out of the widespread use of Remote Deposit Capture.

The rule includes an option called “Determine Duplicated Check Books”. When enabled it prevents false positives by determining that a duplicate check book is in use after seeing more than five in the last twenty numbers duplicated for the same account. When this condition exists, duplicates are not reported for this account.

Check Number Out of Range Rule:

The Check Number Out of Range Rule catches checks which may be fraudulent or whose MICR line information may have been modified. This rule

complements the Duplicate Rule by catching image submittals whose check numbers have been changed, or whose check numbers didn't scan and were manually entered incorrectly. Changed or fraudulent numbers should trigger either the duplicate test, or the out of range test.

Repetitive Amounts Rule:

The Repetitive Amounts Rule traps duplicate presentments of the same item, but which were presented with different check numbers. It also catches duplicated items whose check number is left out of the presentment record.

Duplicate Deposited Items Rule:

The Duplicate Deposited Items Rule protects against items being deposited as images via remote deposit capture, and then also as physical items. It searches the entire bank database, and is not limited to the items from any single depositor.

Other Rules:

In addition to Rules unique to testing for duplicate presentments and fraudulent checks, the system includes optional tests for conditions which have traditionally been tested in core processing systems. They are included to provide for a convenient single location for watching account activity. The ability of the Fraud Detection software to apply rules to individual accounts, or groups of accounts, and to remove specific accounts from certain rules by placing them on White Lists, increases the flexibility of these standard tests.

Large Amount Testing:

Large amount testing is similar to the test in most DDA systems, but is included to allow different cut-off amounts to be easily applied to different groups of accounts or to specific individual accounts.

Block Ranges of Check Numbers:

The range rule allows items in a series of check numbers reported missing, or already used, to be caught if presented again.

Stolen Checkbook:

The Stolen Book Rule provides a convenient way to catch all the checks in a stolen or lost checkbook.

Managing the Rules

The system allows authorized users to create new versions of rules, and to manage the accounts associated with specific iterations of rules and any related white lists. The system design places almost all management of the system into the user's hands.

New Rules

New rules are added easily as new ways to look for problems are defined. A new rule checks daily deposits against the average balance.

Another checks for matches with fields in known fraudulent checks. Several other ideas are being studied.

Automatic Daily Emails

Daily emails with a summary of activity bring the customer into the fraud detection process. It also provides an excellent way to put advertising messages where they will be seen.

The emails can be sent to all authorized parties. Accounts can be combined, with emails containing both business and personal items, and the accounts of children and elderly parents.

If customers see something they don't recognize, they can log onto the bank website and check it out. Fraudulent items can be identified and returned immediately.

Commercial Accounts Get All Check Images

Commercial customers can have images of all their checks, images of items in deposits, and reconciliation files automatically emailed to them daily in an encrypted email attachment. A program on the customer PC automatically decrypts and stores them in its integrated database.

Southern Commercial believes that today's customers not only want to be informed and to participate in protecting themselves, but that it is an excellent way to protect the bank. Customers experience a high level of service, and the computer does all the work.

The screenshot shows an email window titled "Daily Activity" with a menu bar (File, Edit, View, Tools, Message, Help) and a toolbar (Reply, Reply All, Forward, Print, Delete, Previous, Next, Addresses). The email content includes:

From: [Redacted]
Date: [Redacted]
To: [Redacted]
Subject: Daily Activity

Looking for a Home Loan? Let us show you what we can do.

03/16/2006 5:20 PM
Bank of Shady Valley
Group Name John & Mary Doe

156.23	Check
255.40	Deposit
38.00	Debit Card
266.72	ACH Debit

Logon to our website to see transaction images and details. Always use the bank website name provided when you set up your Internet account with us. We will never provide a link in an email or ask you to verify your logon information or password or PIN. If you receive an email with such a link, or an email asking you to verify this information, it did not come from us.

The callouts provide the following explanations:

- "The daily advertising message goes here:" points to the promotional header.
- "Multiple accounts may be grouped together and handled with one email. A customer selected name is assigned different from the actual account name." points to the group name.
- "No account numbers or identifying information is shown, just a short summary of the day's activity, or the statement 'No Activity' on days when nothing happened." points to the transaction list.
- "A warning about phony emails asking customers to verify their passwords and PIN's, and a warning about emails with links to bogus Phish websites, helps protect customers from fraud." points to the security notice at the bottom.

Testing Rule Settings

A test mode allows users to test settings against the history before they are put into live operation. This avoids large numbers of false positives, and allows creation of settings to catch known problems.

Creating the New System

Once the needs were defined, MICR Automation Inc. wrote and implemented the new software. St. Louis based MICR Automation has provided check processing software and hardware to Southern Commercial for over fifteen years.

Vladimir Vassiliev, Vice President for Software at MICR Automation, designed the system and both wrote and directed the writing of the new software. Dr. Vassiliev has a PhD in Computer Science, and years of experience in financial software and database design. Before immigrating to the United States, he wrote the entire core processing system for one of the first commercial banks established in Russia after the fall of communism.

The fraud detection system is built around its own integrated relational database. Open source software was used wherever practical, and the system was designed to run in a Microsoft environment.

Testing of the new software was carried out using the historical data and images in the Southern Commercial archive. Programming work started in June 2005, with live testing starting in November. While enhancements are still being

added, the basic system was in full operation by June 2006.

Addressing other Check 21 Issues

Elements in the MICR Automation System protect against other Check 21 problems and mistakes.

These elements are designed to be easily implemented as stand-alone processes, allowing their use by banks with other check processing systems already installed.

CAR/LAR on incoming presentments and RDC batches

This process allows viewing and correction of items whose actual MICR line images don't match the data contained in the presentment file fields.

Testing of outgoing image presentment files for duplicates

This process tests outgoing electronic letters for either duplication of the entire letter or duplication of any items in it with items in earlier letters. It stops mistakes before they become problems.

Retention and access of intact incoming presentment files

Incoming image presentment files are indexed and kept in their original form. A specialized viewer allows them to be searched and viewed in their original configuration, and provides a description of each field based on the Federal Reserve Documentation as the file fields are viewed. The retention period is set by the user.

Remote Deposit Capture – Remote Lockbox

Southern Commercial Bank expects remote deposit scanners to become as common as fax machines.

The system supports Panini and Unisys Source One scanners directly, removing the need to pay annual interface license fees. It supports all other scanners via the Ranger Silver Bullet interface.

The system also provides for use of regular fax/scanner/copier/printers to be used to capture check images. This provides banks the ability to install their low volume users at almost no cost. The software may be downloaded from a website after obtaining a login and password, so no visit is required.

Almost all printers sold in recent years provide the scanner/copier functionality.

In the scanner/copier version, the customer scans the front and back of each check, enters the amount, and transmits the images via a secure FTP Internet link. At the bank, CAR/LAR fills in the MICR line information and double checks the amount.

Pre-Authorized Draft creation for selected customers is provided as part of the RDC function. It supports one time or automated monthly draft creation, with optional automatic email notification to account holders when pre-authorized drafts are submitted

In addition to the standard RDC functions, the MICR Automation RDC System provides Remote Lockbox. Return payment tickets may be scanned and their amounts read by the CAR/LAR

process, along with the checks. The check images are sent securely to the bank for clearing, and the data from the return payment tickets is formatted for input into the accounts receivable system. A local relational database allows lookup and viewing based on any field.

Crawford Electric, serviced by Bank of Sullivan in Sullivan Missouri, uses the remote lockbox to handle all their incoming monthly payments.

RDC Support

MICR Automation supports all RDC users directly from St. Louis, via secure Internet connections initiated by the user. This removes any technical burden on the bank.

Source Code Provided

MICR Automation is unique in providing all source code for all programs under a simple non-disclosure agreement.

In over twenty years of operation, no MICR Automation user has ever needed to seek support from any other source, but they could if they desired. This policy also allows maximum auditability, and provides a level of user independence not available in any other way.

Southern Commercial Bank can be reached at 314-481-6800.

MICR Automation can be reached at 314-323-2650 or 314-406-1654.