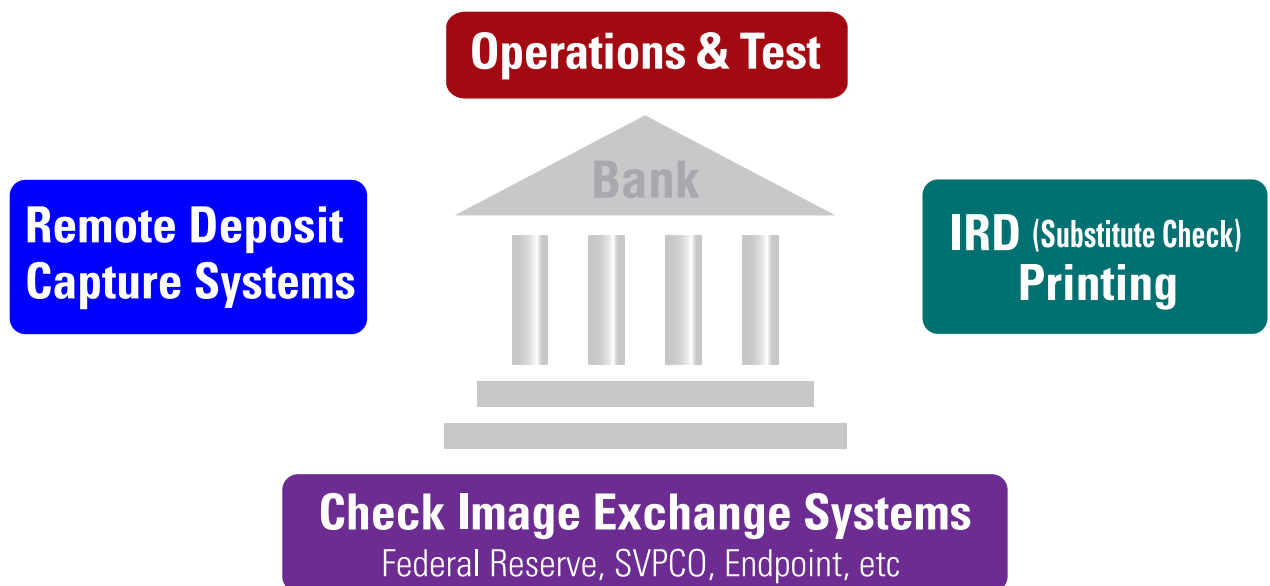




# ***Ramifications of MICR Mismatch in Check Image Exchange***

*By Ray Higgins*

**Solving Interoperability & Data Integrity Issues**



## Contents

Executive Summary	3
Privacy and Operational Risks Within Check Image Exchange	5
Data Quality Issues are Creating Privacy and Operational Risks	6
Data Errors that are Creating Privacy and Operational Risks	7
IRD MICR Line Must Match the Original Check	8
MICR Data from X9.37 ICL Files and Legacy Database Applications Do Not Retain the Original MICR Line Format	9
Why is This a Problem Now and Not Before?	10
MICR Verification Processing to Minimize Privacy and Operational Risks Within Check Image Exchange	11
MICR Verify Technology from All My Papers	13
X9 QUALIFIER Overview	15
Conclusion	16

*Third Edition January 2008*

*Copyright © 2008 All My Papers*

*All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information retrieval system, without permission in writing from All My Papers.*

## Executive Summary

Data errors made during the check truncation and exchange process are creating privacy and operational risks to the financial institutions involved in Check 21 check clearing.

With a one year 320% growth rate in the volume of checks exchanged electronically, the incidence of these data errors has also grown astronomically.

The financial institutions are now feeling the pain of these issues.

### Multiple Problems in Check Image Exchange

- Banks' customers researching their check deposits are seeing images of other customers' checks
- Banks cannot determine where to return a check that has a wrong image
- Checks are posted to wrong accounts or without a corresponding image
- Checks are routed to the wrong banks
- Unusable check images are clearing on IRD or via Image Exchange
- Banks are needing to manually repair account numbers that are missing or have errors

The root causes of many of these problems are the errors in the MICR data at the time of original check scanning.

Additional problems are caused by creation of IRDs from the transaction database. Frequently this database has an incorrect or incomplete record of the original MICR line data. An IRD of a check must have an exact copy of the original check MICR line.

Probably the worst error occurs when the process associates the wrong check image with the MICR data. These problems result in serious privacy issues and operational risks.

This white paper will help the users of the check payment system understand these problems, how they occur, and what can be done to minimize the risks of them happening.

### MICR Verification

MICR verification is a process that can detect and potentially correct errors when the MICR data in the ICL file or legacy database does not match the image data. This technology compares the MICR data captured to the MICR code line on the image using MICR OCR recognition technology.

It must be more than just a MICR OCR process that has a high read rate and a low substitution rate. MICR data on the check image has to correspond directly to the MICR data in the various Image Cash Letter formats and internal databases. Business rules must be applied to account for missing symbols, missing leading zeros, check sum digits, etc.

## **Executive Summary (cont.)**

MICR verification processing can and should occur at different stages of processing to detect errors before they create privacy issues or operational risks.

### **Suspect Ratio**

A major cost in dealing with MICR mismatches is the manual review of suspects. A practical MICR verification process must generate a low Suspect Ratio – the ratio of suspects that need to be reviewed to the number of actual mismatches.

### **Enable High Quality Data Capture at Capture Time**

MICR verification should be used at capture time for magnetic read correction for high read rate and low substitution rate.

### **Detect MICR Mismatches at Exchange Time**

For X9.37 ICL MICR data and image match verification, MICR verification needs to match X9.37 fields to parsed MICR line captured from the image. A low suspect ratio is essential.

### **Ensure Encoding of Accurate MICR Code Line at IRD Print Time**

MICR verification needs to ensure accurate IRD code line generation using image and X9.37 field data. Auto correction rules must deal with data errors and missing symbols.

### **Detect MICR Mismatches at Archive Time**

For database MICR data and image match verification, MICR verification needs to match Database field data to parsed MICR line captured from image. A low suspect ratio is essential.

### **MICR Verify Technology from All My Papers**

All My Papers is the maker of MICR Verify technology that achieves better than 97% accurate read performance with less than 0.1% substitution errors.

Combined with its MICR verification rules-based engine that detects and corrects for mismatches, the MICR Verify technology system minimizes the number of suspects that would otherwise need to be manually reviewed by the financial institution, thus reducing costs.

MICR Verify technology from All My Papers is available as a tool kit and in our X9 QUALIFIER application.

## Privacy and Operational Risks Within Check Image Exchange

The number of checks exchanged electronically by images and by substitute checks has grown 320% in the last year, with 30.3<sup>1</sup> million check items per day now being truncated (check stops moving as a paper item). Users of the check payment system are just starting to feel the pain over many issues related to data errors made during the check electrification process.

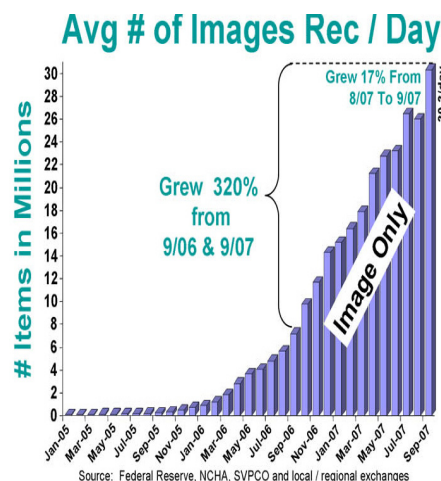
Banks' customers researching their check deposits are seeing images of other customers' checks instead of their own. This is a serious breach of privacy laws and can have negative repercussions for the bank.

Banks performing return processing on Image Replacement Documents (IRDs) are discovering the image on the IRD is not the image of the check that the MICR data was captured from. As a result, they are unable to determine who the original bank of first deposit (BOFD) is, to return the item.

Banks are being presented with items of mismatched image and MICR data. The image and the MICR data originated from entirely different checks. How does this happen?

Being presented with a mismatched MICR item is actually a presentment of two different checks in one transaction.

One check item is invalid as it does not have a corresponding image. This will likely be posted to an account, with the risk of the error being detected later by the customer. The image is a valid check item according to rules of presentment. This will not be posted until the error is discovered, if ever. In both cases the bank is at risk, as return deadlines have likely passed before the errors are discovered. ECCHO rules will be defining a MICR mismatch as a "Breach of Warranty," shifting liabilities to the institution that truncated the item.



These examples represent some of the more significant issues related to data capture errors in check truncation processing.

Other serious problems include:

- Posting checks to wrong accounts
- Routing truncated check data to the wrong banks
- Clearing unusable check images on IRDs or via image exchange

These issues have previously been tolerated because the number of incidences was low. Now that the truncated volume is almost ten times that of a year ago (and hence the volume of incidents ten times greater), the increased risk exposure and drastically increased operational costs have become intolerable. Banks' operational costs are also increasing due to unnecessary correction of account and serial numbers that were either missed or captured with errors during the truncation process.

<sup>1</sup> [www.eccho.org](http://www.eccho.org)

## **Data Quality Issues are Creating Privacy and Operational Risks**

The root causes of many of these problems are errors made at the time the original check is scanned for the image and MICR data. Other problems arise when IRDs are created from the MICR and image data captured from the truncated check.

These errors also occurred in the legacy paper check clearing system, but the paper check was recaptured multiple times in the clearing process. In effect, the MICR data was verified at every stage in the process, and errors captured and corrected early.

In check image exchange processing, the data is captured only once, and typically not verified again throughout the entire process. Now, errors are detected through customer complaints, and posting clearing exceptions. These problems result in serious privacy issues and operational risks.

This white paper will help users of the check payment system understand these problems, how they occur, and what can be done to minimize the risks of them happening.

### **Issues for the Check Truncation Check Clearing System**

The adoption rate of Check 21 processing continues to increase rapidly. In April 2007, over 667<sup>2</sup> million items were either cleared electronically or by substitute check. This represents more than 23% of the monthly volume of checks cleared between banks.

Initially, the financial institutions' focus had been on the operational processes to create and process electronic truncated check data. Checks are truncated by scanning the image and MICR data and exchanging via substitute checks or image exchange using X9.37 Image Cash Letter Files. Inclearing processes have also been updated to receive and process the X9.37 Image Cash Letter Files.

The impact of errors made in the truncation process was not felt immediately, as volume was low with a negligible number of occurrences. Now that volume has grown almost tenfold from a year ago, problems are more frequent, with the impact being felt throughout the check clearing process and systems.

An institution that had 100 exceptions a day a year ago created by truncated data errors, might today have nearly 1,000 exception incidents and can expect that number to continue to increase rapidly.

These problems have the potential to compromise customer privacy and to expose a bank to liability lawsuits. Customer satisfaction is also at risk, and that has intangible costs associated with it.

The frequency of incidents is growing exponentially, so it is now becoming necessary to reduce the risks of these incidents affecting banks.

<sup>2</sup> [www.eccho.org](http://www.eccho.org)

## Data Errors that are Creating Privacy and Operational Risks

There are two primary types of errors that are occurring in Check 21 processing.

### “This is Not My Check Image!”

Many of the check processing errors occur at the time the check is truncated (stops moving as a paper item). This is when the check is scanned for the MICR and image data. Quality problems in the scanning process create mistakes that cause issues later in downstream processing.

The most prevalent problem is errors captured in the MICR data. The hardware scanner is unable to read one or more of the fields from the check, or worse, reads them incorrectly. Checks are now being truncated at teller stations, in businesses, and even homes, using low speed check scanners. It is known that these scanners create more errors than the traditional high speed equipment used in banks' operational centers. It is common that incorrect information is captured from the check. These errors result in an increase in operational costs to manually correct the errors. Undetected errors result in the check being misrouted or posted to the wrong account.



### MICR Mismatch Errors

There are even more serious errors occurring in the capture process. Image and MICR data are often scanned at different times in the capture process, and sometimes the image data gets associated with the MICR data from a different check. The result is that a user or bank operations employee doing image research on the check is presented with the wrong check image. The real check image was assigned to another item and is probably now non-locatable. Even high speed check reader-sorters have been known to make these types of errors, but low speed devices under the control of applications with inferior document handling and recovery procedures have exacerbated these problems.

Being electronically presented with an item with mismatched MICR and image data also causes risk to the paying bank. The electronic item actually now consists of two items that are being presented. The MICR data is for one item and is invalid as there is no corresponding image. The image is of another item and is actually valid according to the rules of presentment. New ECCHO rules coming into effect will transfer liability for a MICR mismatch to the institution that truncated the item.

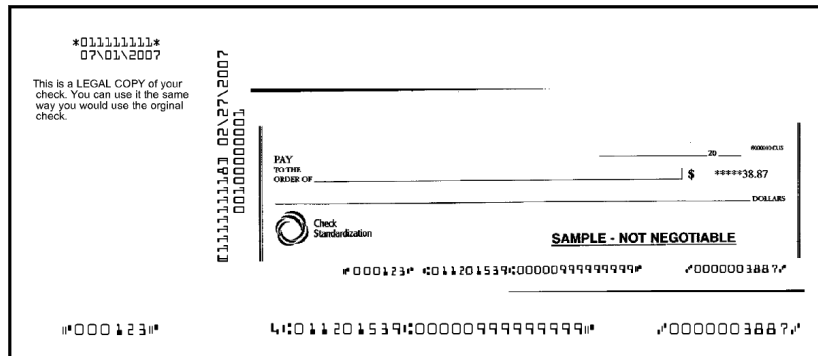
The problem for the bank is that this error is not likely to be detected through current payment clearing processes. The probability is that the check item represented by the MICR line will be posted to the customer's account and would only be discovered by the customer doing account research later on. The item represented by the image would not be posted unless discovered later. As the image represents a legal presentment, it can be posted, but if the item cannot be paid the bank would most likely assume the loss because the return deadline would have passed.

Not capturing a usable image of the check is another quality problem. Checks scanned backwards, upside down, or scanned with excessive skew are too common. Captured images that have poor contrast, noise, or incorrect image dimensions are also frequent.

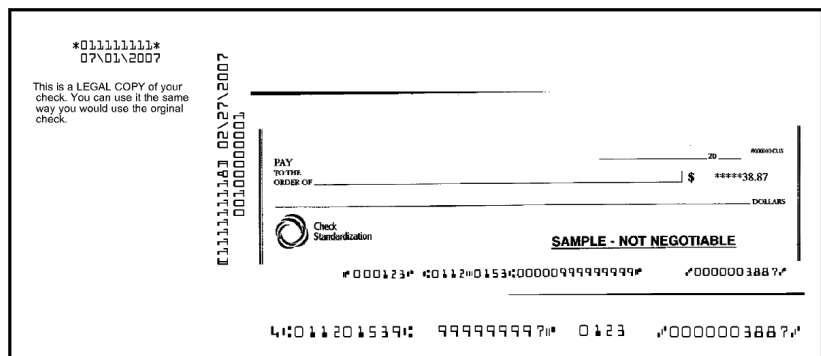
## IRD MICR Line Must Match the Original Check

Regulations require the IRD MICR line to be identical to the original check MICR line. The MICR line data, as it is applied to substitute checks (IRDs) during printing operations, regularly has errors and does not match the MICR line of the original check.

This wrongly printed data exposes the creating financial institution of the IRD to risk of financial loss if the item cannot be paid.



Properly Formatted IRD



IRD Printed with MICR Errors

The sources of errors in the IRD MICR line are multifold.

IRDs are usually printed from the contents of X9.37 Image Cash Letter (ICL) files. The X9.37 MICR field formats do not retain the formatting from the original check. Special symbols including dashes may be suppressed. Often, leading zeros in fields are also not retained.

This makes it challenging to know how to recreate the original MICR line. This is compounded by potential errors in the original MICR data caused in the capture process as described earlier - substitution errors where the “7” is read as a “4” or a “3” as an “8”.



## **MICR Data from X9.37 ICL Files and Legacy Database Applications Do Not Retain the Original MICR Line Format**

IRDs may also be created from the data in a legacy database application where none of the original MICR formatting is likely to be retained.

The legacy database may contain the account number and check serial number from the check On-Us fields, but it will not be known how this information was originally formatted on the check. There is no standard for formatting the On-Us field data. Each financial institution may, and often does, format it uniquely for their internal purposes.

It is also not known if there are leading zeros present, or if and where special account symbols are used. The routing number will also be in the database but likely stored as an 8 digit value. On the original check, the routing number is most probably a 9 digit version with a check digit verification character, but it also could have been printed as 8 characters with a dash between the 4th and 5th characters ("1234-5678" format).

Check Payment Details	
Amount: \$99.99	Payor Bank Routing Number 11111111
Account Number: 45678	Check Serial Number: 123

```

⑈00123⑈ ⑆111111118⑆ 45678⑈ ⑈0000009999⑈
⑆111111118⑆ ⑈45678⑈0123⑈
⑆111111118⑆ 045678⑈ 0123
⑆111111111⑆ 123⑈45678⑈ ⑈0000009999⑈
  
```

### Examples of Valid MICR Code Lines

Many institutions also employ account mappings, where the account number on the check is mapped to a different account number used in the bank system.

This is the result of bank mergers and accounting system changes, with the bank not wanting to migrate customers' checks to the actual account number used. In this case, the database account number is entirely different than what is on the original check image.

## Why is This a Problem Now and Not Before?

## These errors were occurring in legacy paper check clearing. Why is it an issue now?

MICR Read errors have always been happening in the legacy paper check clearing processes, albeit not as badly since high speed reader-sorters were typically used. The paper check would be recaptured at every point of the clearing process:



Traditional Check Clearing Process

For every pass through a reader-sorter, the captured MICR data would be verified and reconciled with previous control totals. If an item rejected, it would be out-sorted and corrected with a MICR correction strip.

In effect, a MICR verification operation was being performed at multiple processing points in the clearing process. This detected and corrected for errors early on in the process, which reduced the number of incidents of undetected errors.



Check 21 Clearing Process Example

The check is only captured once in the image exchange clearing process. The data captured is assumed to be correct and is not verified in the clearing process. Now errors are only being detected at posting times or by customer complaints.

The cost of these errors is now a magnitude larger than what it would have been if detected earlier.

## **MICR Verification Processing to Minimize Privacy and Operational Risks Within Check Image Exchange**

Using an effective MICR verification process will detect and reduce all types of errors described in the previous section. In MICR verification, the captured MICR information from the magnetic read is compared to the results of an OCR process on the image of the item. Using MICR Verify from All My Papers, it is possible to:

- Detect and correct many of the errors attributed to the magnetic-reading hardware capture device during the check image capture process of reading the magnetic-encoded information
- Detect items whose image data came from a different source document than the MICR data was captured from
- Ensure the usability of the MICR line on the check image. Knowing that an item has a usable MICR image ensures the check has been captured with the correct orientation, and without excessive skew. It also raises the confidence that the entire image is usable, as the essential fields for clearing the check are legible. It does not ensure legibility of other important fields on the check required for authentication processes (signature, payee, payer, date, and amount information)
- Ensure the MICR line applied to the IRD matches the MICR line on the original image. The OCR process will be able to determine the formats with use of dashes and special symbols, and generate a MICR line identical to the original. The verification process will even detect and correct for errors in the captured MICR data.
- Detect and autocorrect items with errors in the MICR field data of the received ICL files. This reduces the manual effort to correct these items that would normally be rejected during the posting process.

### **Applying MICR Verification Processes in A Check Truncation System**

#### **“Correct errors early in the truncation process!”**

The ideal time for error prevention is at time of capture. This is when MICR verification technology can be used to correct errors made by the hardware capture device reading the magnetic information encoded on the check. Ensuring MICR codeline usability at this point also raises the confidence that a good image has been captured for the item.

MICR verification can be used for X9.37 ICL quality assurance, whether it is for outgoing or incoming, or used internal to the institution. The MICR verification will detect and correct for MICR data errors, ensure MICR codeline usability in the image, and ensure the MICR and Image data originated from the same check.

Using MICR verification before inserting check item data into an image archive will ensure that when a customer retrieves a check image, it is the image of the correct check and does not belong to someone else.

The technology needs to be accurate and provide a low ratio of suspects to the number of actual mismatches. An engine that produces 200:1 suspects would require the inspection of 20,000 items per million inserted into an archive, assuming one MICR mismatch per 10,000 items. A technology that produces 2:1 suspect ratio would be considered very good.

## **MICR Verification Processing to Minimize Privacy and Operational Risks Within Check Image Exchange (cont.)**

MICR verification technology can also be used for the generation of X9.37 ICL files from check data stored in a database application. The X9.37 needs properly formatted “On-Us” and “Aux On-Us” fields. This formatting is likely not available from the legacy database. MICR verification should use the database data and be able to determine the format of the On-Us MICR data from the image of the check. MICR Verification should return a properly formatted MICR line that enables the application to extract “On-Us” and “Aux On-Us” fields compliant to the requirements of the X9.37 specification. For example, the database may have a check serial number of “123”, and account number of “56789”. MICR Verification should determine that the check image actually had an Aux On-Us of “00123”, and an On-Us field of “ /0056789.. (“/” - On-Us special symbol).

In IRD production, MICR verification technology is required to ensure that the MICR line that is to be applied to the IRD is a match of the original MICR line contained on the check image. This process will ensure the formats are matching and add missing special symbols and missing leading zeros while still correcting for errors in the captured data.

### **MICR Verification Operational Costs**

The primary implementation cost will not be the software or servers. It will be the manpower cost of reviewing and correcting suspects. To implement an affordable MICR verification operation requires an investment in high performance technology. Recognition performance of classic MICR line OCR reading technology has been published<sup>3</sup> to have 15% reject rates with 1% substitution errors. This performance level is not good enough to make a MICR verification operation cost effective. A practical operation requires MICR verification recognition performance less than 3% with a 0.1% substitution rate. If not, the resultant number of suspects that need to be reviewed will create an unacceptably high manpower cost.

There are many high-speed MICR verification products. They also tend to generate high suspect ratios with many false positives per each actual mismatch. Because the suspect ratio is so high, a manual review is required to correct or return the items. However, with a high quality, low suspect ratio product, suspects can be returned without manual review, providing a huge savings both in review cost and downstream correction costs.

The All My Papers AmpLIB Software Development Kit (SDK) contains the technology to perform all the MICR verification processes described in this white paper. This SDK contains two main functional areas for processing MICR information from the electronically captured financial items:

- 1) MICR OCR functions are used to read the MICR image from check images.
- 2) MICR Verify technology is used to detect and correct for errors in hardware captured MICR data. MICR Verify can be used to detect data whose image data came from a different item than the captured MICR data.

The functionality of the AmpLIB SDK is also incorporated in the All My Papers X9 QUALIFIER application, which will scan an X9 ICL file and detect MICR mismatches and other errors in the MICR field data. All My Papers AmpLIB runtimes support both single and multiprocessor/multicore environments. The multiprocessor version is both thread safe and multithread enabled with the capabilities to perform MICR verification processing on over 10 million items per shift on a single MS Windows server (quad processor, dual core).

<sup>3</sup> Digital Document Processing -- Major Directions and Recent Advances by Bidyut B. Chaudhuri (Springer, 2007)

## MICR Verification Technology from All My Papers

### AmpLIB SDK Overview

The AmpLIB SDK contains five basic functions required for fast and accurate processing of the MICR data from check images:

1) OCR Functions – Incorporates three different OCR engines. Its very fast engine is able to process easy-to-read items and will provide high throughput rates in Verify operations. The additional engines provide high accuracy on the more difficult to read items.

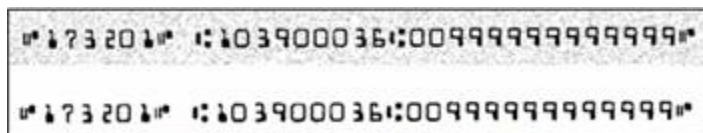


Image Repair Improves MICR OCR Accuracy

2) Image Enhancement and Repair – Contains functions that will correct for image quality problems, resulting in improved OCR accuracy. These functions will de-skew, de-border, rotate, remove noise, remove lines, and even enhance character shapes. The enhanced and repaired image can be saved or just used to increase the OCR read rate.

3) Voting Technology – Combines the results of multiple OCR processes and hardware MICR data to produce highly accurate MICR data for the check item.

4) MICR Line Parsing – Separates the MICR line into the individual field components required for X9.37 Image Cash Letter Files or for validating against captured data.

5) Processing Rules Engine – Contains the rule sets required for the different processing functions. The rules determine what OCR engines to use and when, what image repair processing is required, and invoke parsing and voting as required for the particular function being performed.

Additionally, the AmpLIB SDK contains functions for general OCR and barcode recognition from document images.

### AmpLIB Main Functions

**MICR OCR** – Finds and reads the MICR line data from a check image (or other financial document). This function uses multiple OCR engines and voting technology to produce an accurate result. MICR OCR produces best and secondary read choices, with confidence levels. Application developers have options to invoke image repair functions. Additional functions are provided to pre-process the image before OCR recognition to correct for skew and image border effects.

**MICR Verify** – Reads the MICR from a check image, using previously captured MICR data to assist in the process. There are several applications that can use MICR Verify technology, so this consists of a family of functions, each using a different set of inputs, outputs and processing rules.

All MICR Verify functions use the fast OCR engine to verify the easy-to-read items that usually represent the majority of the cases. Image repair, the other two engines, and OCR retry operations are used on the harder-to-read items as required

## **MICR Verification Technology from All My Papers (cont.)**

to verify the most difficult-to-read items. The combined result is higher throughput with higher accuracy.

### **MICR Verify Functions**

#### **MICR Verify – Check**

This is used in capture systems to detect and correct for errors in hardware captured MICR data. It uses the hardware-captured MICR data with the image to detect and correct for rejects, substitutions, and missed data. This technology is used by Unisys and 7-Eleven for check image capture applications.

The success rate of reading MICR code lines accurately has been measured at 99.7% on customers' check image databases.

#### **MICR Verify – IRD**

Regulatory policy requires that the MICR line applied to an IRD must match the MICR line of the original item. This function will input the MICR field data from a X9.37 Image Cash Letter File with the check image to produce an accurate MICR line that can be applied to the IRD. Often the X9.37 MICR field data is missing dashes, special symbols, and contains errors requiring a verification OCR process to produce accurate IRDs. This same function can be used to detect and correct for errors in X9.37 MICR field data.

#### **MICR Verify – Error Detection**

This function can be used to detect images whose source document is different than the associated captured MICR data. It will input the check image and the MICR field data associated to the check image, and return results that can be used to validate whether the MICR and image came from the same source document. The function will return the parsed OCR field data read from the image with a match confidence level. Two different versions of this function are provided to accommodate MICR field data from an X9.37 file (RT, Aux On-Ups, On-Ups, Amount) or from a database/capture file (RT, Account Number, Serial Number, Amount). Verification accuracy is very high as the function will ignore dashes, special symbols, and leading zeros in the OCR processing.

Customer database testing has shown suspect rates below 0.3%, reducing operational costs.

#### **MICR Verify – MICR Codeline Usability**

This function is similar to the "Error Detection" verification function except it can also be used to determine usability issues of the MICR codeline on the image. This function will generate a very low rate of suspects (<0.3%) but be accurate to detect items with serious image quality problems such as:

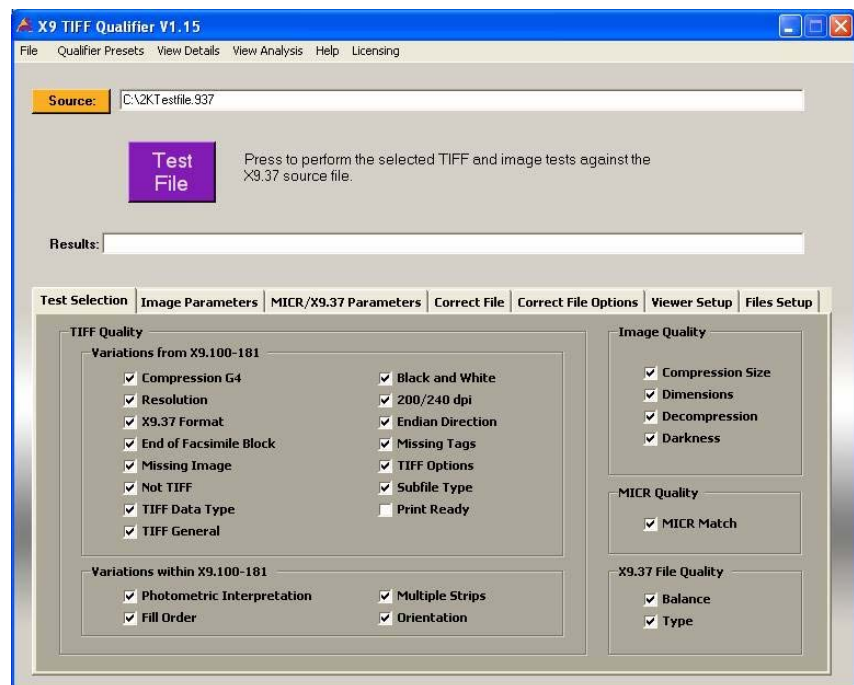
- Wrong orientation (upside down, backwards)
- Excessive skew
- Poor contrast
- Excessive noise
- Wrong document image



## X9 QUALIFIER Overview

All My Papers has incorporated MICR Verify functionality into a standalone application, X9 QUALIFIER, a Windows .NET application built using AMP SDKs.

- Tests the data integrity of X9.37 Image Cash Letter files to ensure their interoperability in check image exchange,
- Tests the data contained in ICL files to ensure their accuracy, quality, and conformance to industry standards.
- Performs a MICR verification of the MICR data contained in the ICL file against the MICR data in the image.
- Flags items that have mismatched MICR data and other MICR data errors.
- Tests the TIFF image formats, image quality, and the X9 ICL format for conformance to exchange standards and rules.



X9 QUALIFIER will generate reports of the nonconforming items. Lists are also generated that can be used for exception processing of the nonconforming items.

## **Conclusion**

MICR Mismatch errors are creating privacy and operational risks with image exchange, and it is only going to get worse with the current adoption rates.

Implementing MICR Verify in the early processing stages of your check imaging systems will reduce these risks while minimizing the cost impact on your institution.

We hope you have found this white paper informative, and now understand the issues at hand as you take the next steps toward your own implementation.

We would like to hear from you if you have any questions or comments related to this white paper or about any of the All My Papers ICL processing products.

Please contact us at:

**All My Papers  
13750 Serra Oaks  
Saratoga, CA 95070**

**Phone: (408) 366-6400  
Fax: (408) 366-6406**

**Email us: [sales@allmypapers.com](mailto:sales@allmypapers.com)  
[www.AllMyPapers.com](http://www.AllMyPapers.com)**

We hope you will choose All My Papers technology for your implementation.

We believe you will appreciate how easy our tools and applications are to use, to help you rapidly implement an efficient image exchange system with reduced risks for privacy and operational issues caused by MICR mismatches.