



IMAGE INDUSTRY BEST PRACTICES DOCUMENT

IMAGE INTEGRITY ANALYSIS: FROM PERCEIVED VALUE TO INDUSTRY STANDARD

**VERSION 1.0
APRIL 2010**

**FOR MORE INFORMATION:
VISIT WWW.I3GGROUP.COM**

i3G: Image Industry Best Practices Document

IMAGE INTEGRITY
ANALYSIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

HOW ARE CHECKS PROCESSED? 3

PROPOSAL FOR INDUSTRY STANDARD 5

CONCLUSION 6

ABOUT I3G 6

CONTACT INFO 7

EXECUTIVE SUMMARY

Image Integrity Analysis

Since the advent of Check 21, the law that enables the expanded use of captured check images, image exchange has been widely adopted as an economical and reliable way to perform forward check collection. In anticipation of the most obvious potential problem, the industry first debated and set standards for, image quality and usability – in other words how the paying bank and its customers viewed the suitability of the image being presented for collection. But as with many new processes, some of the more subtle growing pains associated with this type of breakthrough technology become more apparent only later, as the process became more widely adopted.

One major problem overlooked is the fact that measuring either quality or usability is irrelevant if front and back check images become disassociated with their respective MICR codeline data as it is the codeline data that is commonly used to perform the actual customer posting of items. This problem – commonly referred to as “codeline data mismatch” - and the inherent issues that may arise from it, is now clear and must have industry-level attention and resolution.

HOW ARE CHECKS PROCESSED?

Historically, checks were run through a sorter which would read only the MICR line. The obtained data was then used to form the actual cash letters which were used for settlement. While complex in its own right, the process relied on purpose-built equipment with over 50 years of engineering to perform these tasks.

With the advent of image exchange, a scanner was added to these machines to obtain images of the front and back of the checks being processed. Typically, the images created by these scanners were moved to a staging area for later processing. Farther down the processing stream, new applications were developed to take the MICR data and marry it back up with both front and back images to form an X9.37 file. Those files were then submitted to an image exchange.

What Can Go Wrong in Processing?

The historical method of processing checks was subject to mismatches between paper and cash letter codeline data, but as it was simply a paper listing error due to the physical nature of the medium, negative effects were quite limited. But the introduction of scanners to check processing has introduced several hardware, software, and network dependencies to the check processing workflow.

Within each of these dependencies exists the potential for codeline data and check images to become disassociated. For most financial institutions there are no safeguards later within the processing stream to recognize and/or correct the problem before the data goes out the door. As it is considered to be too computationally expensive for the paying bank to interrogate images in order to compare the information within them to the paired MICR data, paying banks more often than not simply trust that the data they receive is coherent. This situation is creating problems for both the collecting and paying banks.

Even More Complexity

Further compounding this problem, in recent years these back-office environments have begun to evolve into more distributed customer-based capture orientations, creating new tools such as remote deposit capture that has allowed consumers and businesses alike to create check images for the purpose of deposit. Consider that roughly within the last five years, the industry has moved check processing from back-office, to external businesses with dedicated hardware and trained staff, to consumers with commodity PCs and scanners and minimal training. And now the industry is on the cusp of enabling check imaging and deposits via cell phone.

It is important to note that the move away from the back-office is eliminating the efficacy of the MICR line, namely its magnetic characteristics which have formed the backbone of check processing for decades. Even worse, the introduction of image acquisition/check conversion at a consumer level is threatening what little contractual controls could be negotiated with businesses. While the clear intent of these moves is convenience, permitting this critical task outside of financial institution's "controlled" environments adds a new dimension to the risks of disassociated front/back images along with the potential of losing codeline integrity. In addition, image quality is also significant may suffer due to the large number of image capturing devices associated with the process itself.

What do Mistakes Mean?

There are three primary negative outcomes that can arise with a disassociation event: warranty problems, privacy breaches, and institutional abandonment, customer dissatisfaction with their financial institution. These problems can affect both collecting and paying banks.

- Warranty Issues

The collecting bank is considered to be liable, and for all intents and purposes creates warranty issues with the effect of the disassociated items. Potentially, they are nullifying any items associated with the actual mismatch, bringing cause to dispute the collectability of these items.

- Privacy Breaches

The disassociation may not be noticed by either the collecting or the paying institution until it has been recognized and reported by the paying bank's customer(s), for example, by viewing in an online banking application. Once exposed to the wrong party, this information clearly introduces risk. And note that the personal information represented on the check may not even belong to the customer of the paying / displaying institution.

The privacy protections in the Gramm-Leach-Bliley Act were written with the full intent of ensuring financial service providers protect and secure the identity of depository customers, and in certain circumstances, the personal information of all consumers (16 CFR Part 314, Section C states "...protecting information about consumers may be a part of providing reasonable safeguards to 'customer information' where the two types of information cannot be segregated reliably."). Knowing that it's a possibility that images and their associated data can get out of sequence, GLBA arguably requires the collecting bank to address the potential of sending disassociated data out the door (6801(b)(2)). And the paying bank, who will more

often than not display the check images to their customers, would be under the same requirement. Further, depending on the number of disassociated items sent or received various state data breach notification laws may come into play as well.

- Institutional Abandonment Customer Dissatisfaction

The final risk: reputational harm leading to institutional abandonment/ customer dissatisfaction, is clearly conceivable yet one of the hardest to quantify. This risk is assumed every time the paying bank posts an item from an exchange partner without scrutinizing the content. In assuming this risk, organizations jeopardize a relationship should a misposting cause embarrassment and/or introduce “opportunity” for someone to exploit the information banks have provided to them through the introduction of the error. How anyone chooses to spend their money via check (or otherwise) is often very personal, and a violation of that trust through an error caused or allowed by financial services providers through the image process could easily lead to the end of the relationship. A customer’s financial service provider may have not directly caused the error, in the customer’s eyes it would not matter – their exposure stemmed directly from that relationship and in turn would be held liable if damages should result from this error.

The above considerations make it clear that both collecting as well as paying institutions have a vested interest in addressing the problem. And the fact that many institutions have, or are in the process of, pushing the ability to generate check images outside of their walls makes the matter more urgent.

PROPOSAL FOR INDUSTRY STANDARD

As mentioned earlier, it is computationally expensive to interrogate check images in an efficient and timely manner. Nonetheless, in the interest of customer privacy as well as quality product delivery to customers, should not financial organizations agree that a standard that incorporates a universally acceptable level of integrity assurance be adopted? The overarching answer is yes; however, all the aforementioned challenges will most likely mean a significant group effort amongst industry peers, as well as proving to each bank’s internal groups of its worthiness. Unfortunately, this type of process could be deemed an “insurance policy” of sorts that may never prove its financial gain until the potential damage becomes reality.

Two-Pronged Approach

When considering a solution to a perceived problem of this magnitude, there are two logical approaches to resolving – either positioning this type of prevention/detection on the outgoing side or the incoming – or potentially on both. There are clear benefits to both approaches:

Outgoing – Positioning an image/data integrity process on the outgoing cash letter send side will ensure that all data records are indeed accurate prior to presenting to a paying institution. By doing so, the collecting bank or institution is ensuring warranty for collection. However, this particular approach will not ensure that once the image cash letter reaches the paying institution that some disassociation may not have occurred through the series of network handoffs and subsequent processing necessary to reach the settlement point.

Incoming – Placing an integrity checking process on the incoming side of image exchange is favorable in a number of ways, including the ultimate insurance that a paying institution will never have disassociated data visible to its customers. This will

not only protect the paying bank from one of its customers potentially misusing data that is erroneously made available to them, but also the check issuer from righteously charging anyone in the payment cycle with a breach of warranty claim should sensitive data be used to defraud or cause financial harm.

Ultimately, placing this sort of assurance on both the incoming and outgoing functions of image exchange is ideal, but due to operational and technical constraints, this seems unreasonable. And when logically addressed, the industry would have to be engineered in the same fashion or at a very high level the industry would inherently defeat the purpose of the integrity process as a whole – meaning every image exchange participant would have to be equipped to detect anomalies either on the incoming or the outgoing and not a mixture of both.

Resolution of Occurrences –

When data mismatches are discovered, notifications must be made to all institutions in the collection stream to insure that items are suppressed from archives and customer views to prevent and mitigate privacy breaches.

It is recommended that standardized adjustment codes and resolution timeframes be developed for identification of mismatches to allow for expedited handling by impacted institutions.

A standardized notification processes similar to the [Duplicate Notification Process](#) recently announced by the Federal Reserve should be developed expedite notification to impacted institutions.

CONCLUSION

Every day, financial institutions strive for flawless quality in their customer deliveries – be they through online or traditional products that customers have relied on for decades. While check usage may be declining, check writing remains a large, fundamental component of these basic product offerings and most likely will be for years to come. Meanwhile, the financial industry has improved check collection processes but hasn't quite yet achieved perfection in customer safety and soundness. Adopting an industry standard process for image integrity analysis will be a huge leap in that direction.

Image quality aside, allowing banking customers to perform such fundamental tasks as deposit construction and creation dictates that the industry makes every attempt to promote check image integrity. While the industry has developed strict parameters around the remote deposit capture processes, banks are no less liable for the images and MICR codeline creation that comes to them. Regardless of the nature by which an image and its associated codeline data is created, ultimately every financial institution warrants that forward collection items are valid and reasonably usable by the paying bank's customers.

ABOUT i3G

The Image Industry Interoperability Group, i3G, is a US financial services industry collaborative formed in 2008 by a small and diverse set of bank organizations with the mission to quickly solve for lingering exceptions and interoperability issues impeding check payment processing efficiencies. The group's goal is to eliminate a large percentage of industry processing exceptions with a few changes to industry operational practices and procedures. i3G members include Bank of America, The Federal Reserve Bank, Frost Bank, JP Morgan Chase & Co,

Independent Community Bankers Association (represented by Midwest Independent Bank), Southwest Corporate Federal Credit Union, Sterling Savings, US Bank, and Wells Fargo. More information can be found about i3G and proposed industry solutions by visiting www.i3ggroup.com and [i3G's linkedin group page](#).

Other i3G best practices documents and industry efforts can be found on www.i3ggroup.com include:

- “Dealing with Duplicates” – An industry wide duplicate file notification system
- Bank of First Deposit Electronic Endorsements
- TIFF Tags
- MICR: Interrogating to populate X9.27 Record 25
- Best Practices for Incoming Returns
- Best Practices for Image Defects

CONTACT INFO

Contact the group by emailing info@i3ggroup.com.