

BITS

FINANCIAL SERVICES
R O U N D T A B L E

REMOTE DEPOSIT IMAGE CAPTURE: THE PROCESSES, RISKS AND STRATEGIES USED TO MITIGATE THEM

A PUBLICATION OF THE
BITS FRAUD REDUCTION STEERING COMMITTEE
SEPTEMBER 2006

BITS
1001 PENNSYLVANIA AVENUE NW
SUITE 500 SOUTH
WASHINGTON DC 20004
(202) 289-4322
WWW.BITSINFO.ORG

REMOTE DEPOSIT IMAGE CAPTURE: THE PROCESSES, RISKS AND STRATEGIES USED TO MITIGATE THEM

EXECUTIVE SUMMARY

This document is a tool for financial institutions' use in assessing and mitigating risks associated with implementation of Remote Deposit Image Capture (RDIC).

This paper provides successful strategies that financial institutions (FIs) have employed for managing the risks with RDIC. It does not imply that all of these strategies are necessary for a successful program. This paper also does not address the specific technologies used to implement the RDIC process and/or mitigate the risk, as technology used will often be determined by other factors such as the compatibility of the clients' and FIs' equipment. This paper identifies potential risks as they pertain to product distribution, equipment and software, information system security, images and image quality, and processes.

There are many benefits to offering the RDIC product to clients; however the attendant risks must be mitigated.

With the proper understanding of both the benefits and risks associated with RDIC, this product could increase client satisfaction while simultaneously reducing some expenses for financial institutions.

BACKGROUND

In September 2005, the BITS Electronification Working Group began drafting a briefing paper in response to a request from the BITS Fraud Reduction Steering Committee (FRSC) to assess the risk implications of financial institutions (FIs) offering Remote Deposit Image Capture (RDIC) services to their qualifying commercial clients. This briefing paper focuses on fraud and operational issues as they relate to RDIC. For those who would like more information on legal and regulatory issues that pertain to RDIC, we suggest that you review the NetDeposit paper available at <http://www.netdeposit.com/rdc/documents/NDRemoteDepositCaptureWhitePaperRV2.pdf>.

DEFINITION AND SCOPE

For the purposes of this briefing paper, Remote Deposit Image Capture is defined as “the process that enables clients to scan check deposits at their location (such as an office or retail store/branch) and transmit electronic check images and related deposit information to the financial institution (FIs) for processing and presentment/clearing in a secure environment.”

This paper will focus on the product sold to clients for on-site processing. While FIs and clients may outsource image capture and/or item processing to third parties, the risks associated with these processors are not fully addressed in this paper.

This paper also does not address specific technologies used to implement the RDIC process and/or mitigate the risk, as technology used will often be determined by other factors such as the compatibility of the clients’ and FIs’ equipment.

BENEFITS STATEMENT

RDIC is flexible enough to be tailored to merchants with high volume/low dollar checks or low volume/high dollar checks and, if used as intended and afforded reasonable protections by the client and FI, it offers great rewards to both. RDIC can enhance customer service and safety by:

- Reducing expenses for floats and courier services;
- Allowing clients to choose a processing alternative;
- Decreasing the number of checks to be physically deposited (less chance for theft, robbery, loss of information); and
- Allowing companies to collect high-dollar checks quickly.

Industry experts expect that the next two years will see tremendous growth in remote deposit service offerings. While larger firms may appreciate the ability to credit deposits quicker, smaller merchants will appreciate the convenience of the service. For remote deposit participants, later deadlines and improved funds availability on their deposits are other expected benefits of the service. Merchants’ ability to reduce employee travel time, consolidate deposits from several retail locations into one account, and increase funds availability will generate a growing demand for this product.

RISKS AND MITIGATION STRATEGIES¹

As stated above, there are many benefits to offering this product to clients. However, as with any new technology and/or process, there are risks that FIs should consider and take steps to mitigate. For this paper, the BITS Electronification Working Group identified RDIC-related risks and mitigation strategies as they pertain to:

- Product distribution;
- Equipment and software;
- Information system security;
- Images and image quality; and
- Processes.

¹ These risks and mitigations strategies are included in a matrix located in Appendix A

A matrix contained in Appendix A of this document provides a high-level overview of the risks and mitigation strategies associated with the aforementioned issues and may be used as a checklist for those implementing RDIC into their product line.

PRODUCT DISTRIBUTION

The line of business most likely to offer this service to qualified clients is the institution's Treasury Management department. Those representatives selling the product must receive comprehensive and ongoing training that addresses both the benefits and the associated risks of offering this product to customers.

It must be noted that the client, in performing the role as processor, becomes an extension of the FI. Once the sales staff signs-off as having acknowledged the risks of RDIC to a client, the next critical step is to ensure that the sales staff and/or FI knows their customer and has performed a risk assessment to determine that the client is a viable candidate for use of this product. Initially, the product should be offered only to existing and established customers who have a good credit rating with the institution. It can later be offered to those outside of the institution's footprint, provided that a risk assessment and due diligence are performed on the business and its principals. In addition, since the client (by virtue of their processing of the checks) places the liability for the checks on themselves and their FIs through the clearing process, FIs must have a full understanding of the client and financial institution liabilities. While strict terms and conditions can help limit liability to the FI, it is important that FIs maintain ongoing dialogue with and monitoring of the client to ensure that the product is being used correctly.

The risks and mitigation strategies identified for product distribution are as follows:

Risk: Inadequate knowledge of product by sales staff which causes product to be marketed to unqualified clients

Potential Strategies:

- Provide initial and ongoing training to individuals responsible for sales and service of product
- Provide technology overview of product and process flow to individuals responsible for sales and service of product
- Require those individuals responsible for sale of product to sign-off acknowledging risk
- Limit product to Treasury Management departments of established small businesses, and middle market and large corporate customers
- Implement a risk assessment process to determine if client is a viable candidate for use of product
- Adhere to internal KYC programs
- Perform enhanced due diligence on prospective clients (underwriting processes, background checks on business and principals, qualification process)
- Require clients to provide collateral with a dollar amount determined from a sliding scale relative to the risk exposure from the total deposits
- Tie sale of product to loan risk rating

Risk: Improper or incorrect use of product by client

Potential Strategies:

- Re-certify clients at least annually to ensure an acceptable risk level (similar to wire certification)
- Require periodic on-site inspections and review the file information received

- Perform ongoing enhanced due diligence (underwriting processes, background checks on business and principles, qualification process)

EQUIPMENT AND SOFTWARE

FIs must consider the variances in the type of equipment needed to process RDIC and strive to ensure that the software is compatible. While the hardware used for this service is relatively standard, there could be issues with the interoperability of the software used between the client and FI. The industry is assessing the variances in the appearance of images from different capture systems. It is believed that a calibration process should be used to set up the capture equipment to perform to acceptable minimum industry standards.

FIs must also determine who owns the equipment and software and define the terms and conditions for its use. The terms and conditions should acknowledge the risk(s) of transitioning software from one FI to another. Clients must be made aware of and adhere to the minimum standards of use, regardless of whether the equipment was issued or purchased. Contracts should include information concerning how the software and hardware are provided (i.e., buy vs. lease) inspected, maintained, and upgraded and also the specifics of who is responsible for servicing the equipment, providing back-up during down-times, and acting as the point of contact for customer service issues. Due diligence is also needed on behalf of both the FI and client to ensure that the standards of computer security (such as regularly updating patches, etc.) are met.

The risks and mitigation strategies identified for equipment are as follows:

Risk: Hardware/software will not interoperate with FI or industry or meet minimum industry capture and processing requirements

Potential Strategies:

- Ensure that minimum standards are defined
- Define ownership and deployment of equipment and software as part of the terms and conditions and establish equipment replacement procedures
- Determine if imaging equipment and software is proprietary or commercially available
- Ensure imaging equipment and software is compatible with FI software and equipment
- Ensure that all equipment/software (purchased/not purchased through the FI) is evaluated and certified to meet minimum requirements
- Implement quality control process to ensure images are of good quality and are in expected formats

Risk: Equipment not functioning as intended

Potential Strategies:

- Ensure that there is oversight and a quality control process in place
- Perform calibration to ensure that system set-up and maintenance procedures are properly performed
- Monitor and check equipment on a regular basis to ensure it is functioning properly
- Review volume and bandwidth capabilities
- Educate client on the importance of performing regular equipment maintenance

INFORMATION SYSTEM SECURITY

Current paper processes in place today allow clients to control access to account information or activity for an account by segregating accounts and/or duties. The RDIC process should allow the client to provide the same segregation to ensure continued customer privacy. Additionally, images of all deposited checks, as well as the original checks, will be housed at the customer site creating an additional data security concern. This concern should be addressed in the terms and conditions/contract that the client signs.

It is possible that a foreign entity could edit files after capture before receipt by the FI. In thick client based software, the file could be edited on the PC prior to transmission. In thick and thin client software, the file could be hijacked and edited en-route. Additionally, an unauthorized user could attempt to transmit a fraudulent file created either with or without the software.

With RDIC, the most common method of file transmission will be via the Internet. While some larger corporate clients may utilize dedicated communications lines, most traffic will be across public lines. As a result, RDIC files will be open to all the same attacks that on-line banking or on-line commerce face. Files could be intercepted on the Internet and either be edited for fraudulent submission or data mined for fraud and identity theft.

The risks and mitigation strategies identified for information security are as follows:

Risk: Unauthorized access to and/or use of the imaged information

Potential Strategies:

- Ensure software has user authentication capabilities, with acceptable user administration functionality at the client site
- Ensure the software has audit trail capabilities
- Ensure software and process provides data security
- Assign user(s) credentials that are password-protected

Risk: Edited or unauthorized files are submitted for clearing

Potential Strategies:

- Secure transmission mechanism according to FI's best practices
- Software should only accept transmissions from validated sources by authentication
- Restrict and control installation of software at client site
- Ensure that software has the ability to validate the sources of the file and validate that the file has not been compromised

Risk: Loss of data

Potential Strategies:

- Identify and resolve communication issues that impact transmission of data between FI and client
- Establish authentication process to validate source and allow authentication at both client and FI site
- Ensure that equipment and software have the ability to encrypt files to ensure data security and integrity if files are compromised

IMAGES AND IMAGE QUALITY²

An image quality assurance strategy is a key component of a RDIC risk mitigation strategy to assure payment chain reliability (fee defense, risk management, and dispute resolution). Banks incur liability risk because they must ensure that an image is of adequate quality to support electronic clearing requirements and meet customer needs.³

As part of the overall RDIC strategy, clients and FIs should perform automated image defect and/or usability assessment (IDA/IUA) according to common industry practice as well as MICR codeline evaluation at the point of capture and before settlement. This can be achieved through a batch review before transmission or real time as each item is scanned. The first line of defense against poor image quality would be solutions that allow the person performing the scanning of checks to see the image as it is captured – eliminating for example, mismatched, piggyback or skewed images before completing and closing out a deposit transaction or transmission.

Automated software analyses should supplement manual review and should be deployed before substitute checks are created or files are exchanged. Consolidating this process into batch mode will enable images to be automatically assessed and allow for more consistent human review of suspects for decisioning. Deposits can be adjusted for items that fail the image quality review and the customer can be contacted soon enough to retrieve the original check for representment or other exception processes. Meanwhile, settlement occurs with the remaining items in the deposit that have passed image inspection routines.

The risks and mitigation strategies identified for images/image quality are as follows:

Risk: Poor Image Quality

- Inability to validate amount (CARLAR)
- Inability to distinguish image survivable security features
- Inability to recognize and detect information in fields
- Inability to check that the image captured meets depositor and/or check-writer expectations for usability
- Inability to reproduce the check once it has been cleared
- Check image is not usable for purpose intended

Potential Strategies:

- Establish an ongoing process to ensure good quality images
- Identify and ensure clients comply with existing image quality standards
- Ensure images comply with current ANSI standards
- Deploy image inspection tools, at the point of capture, downstream, and RDIC to ACH, exchange or IRD printing
- Implement image defect and image usability assessment tools along with image quality usability (IQU) and image quality analysis (IQA) engines for defect analysis/assessment and to ensure that the image is usable
- Inspect images visually or using image usability assessment software to ensure key fields (MICR, amount, maker, etc.) are readable for clearing
- Retain document long enough to ensure a usable image
- Ensure ability to retrieve original source documents or image, as applicable

² Remote deposit images should have the same standards and responsibilities as imaged checks².

³ Please see Appendix B for more information regarding image quality assurance strategies.

- Implement a quality review process to oversee CARLAR accuracy rates
- Perform quality check at client location and processor location

Risk: Inability to settle item

Potential Strategies:

- Determine document settlement process (i.e. ACH, substitute check, image exchanges, etc.)
- Establish and document a process for recourse to converting bank and ensure that converting FI has recourse to client
- Develop timeframes in which an item may be resubmitted
- Establish an agreement with the client to share the risk regarding re-presentments and warranties for substitute checks

Risk: Point of capture difficulties (i.e.; mis-matched, piggyback, or skewed images.)

Potential Strategies:

- Ensure high-level image defect analysis (IDA) and MICR code lines are done at the point of capture
- Allow the person performing the scanning of checks to see the image as it is captured
- Ensure that the image is reviewed at capture
- Ensure that batch mode processing is being used as this will enable images to be automatically assessed while allowing for more consistent human review

Risk: Duplicate images entering payment stream

Potential Strategies:

- Incorporate quality controls to search for duplicate items at client and FI processing stage
- Ensure that client has a process to secure items after imaging to prevent their re-entry

PROCESSES

To best serve the clients, as well as protect the financial institution, there must be an understanding of what the client’s processing volume is and what kind of equipment is and/or should be provided. However, it is important to note that these and many of the issues regarding RDIC can be addressed through enhanced contract language that distinctly outlines the responsibilities and liabilities for both the FI and the client. Contracts should include tight terms and conditions for all risks and outline what should and should not be included in the process.

The retention period for the original checks used as “source documents” for substitute checks or image replacement documents is not regulated nor is there yet a standard industry practice. Without a standard for retention, individual institutions must determine their own retention timeframe by balancing the time an item should be retained to insure that a good image has been produced against the risk of the items reentering the payment stream as duplicates because the item was not destroyed in a timely manner. If, during the settlement process, a check image is determined to be unusable, the RDIC customer may need access to a “better” version. In situations such as this, the image may need to be rescanned and it will be important to have access to the original items.

Clearing strategies now allow a single deposit transmission containing electronically captured items to be settled through ACH, Substitute Check or Image Exchange clearing channels. The choice for final settlement is at the discretion of the FI. Agreements and practices constructed with the RDIC

customer should insure that the customer is aware of and able to manage NACHA-related customer opt-out or exclusion rules and notifications, if applicable to the FI's product offering. The FI's internal engines should apply business rules based on the items in the file, type of check (consumer versus business), amount of check, check image defects present and the lowest cost route for clearing. Poor image quality items can be converted to ACH transactions provided the MICR information is accurate since the check image is not required for clearing. From a RDIC customer point of view, this reduces customer deposit adjustments and exceptions processing.

There are believed to be risks related to the clearing process and these risks are dependent on the channel through which they are cleared. However, the legal issues with changing channels within check presentment have not yet been determined. For example, clearings that are classified as ACH SEC codes POP and ARC are covered by Regulation E, images and image exchange are covered by check law, and substitute checks are covered by Check21. There are many possible combinations of cross channels but it is not yet clear which combinations might be covered by Regulation E. It is important for financial institutions to be aware of the clearing channels that they are using and the legalities surrounding those clearing channels.

RDIC solutions must weigh potential customer experience impacts (such as overall processing time including exception handling) for point of capture image quality review versus the impact of potential adjustments to customer deposits and exception processing by the bank after receipt of the transmission. In addition, it is important that financial institutions determine if items processed through the RDIC channel are filtered through existing or new fraud prevention and detection solutions. Many financial institutions are able to process items captured as a RDIC transaction through their existing solutions. Other financial institutions have additional tools within the RDIC software that they have employed. To insure that risks are being managed, it is important that the financial institutions know what tools they are using for fraud prevention.

The risks and mitigation strategies identified for processes are as follows:

Risk: Multiple presentment of same item

Potential Strategies:

- Check for duplicate items
- Check for duplicate batches
- Establish a process control to identify duplicate items across entry points within RDIC software
- Develop a business process to cross reference multiple points of presentment for duplicate items (payment database of record)

Risk: Fraud and returned items

Potential Strategies:

- Ensure clients have established security procedures and are stated in terms and conditions
- Ensure checks deposited through RDIC are fed through fraud detection systems
- Define loss mitigation and develop a plan, including the fraud tools used
- Establish an escalation process for fraud suspects
- Monitor incoming transactions for unusual activity
- Place liability on the party best able to prevent losses
- Preclude client from depositing items drawn on their own accounts through RDIC
- Identify clearing channel and ultimately regulations that guide returned item process

Risk: Operational-related risk

Potential Strategies:

- Check for valid routing and transit (R&T)
- Use CARLAR to detect amount keyed vs. check image
- Use operational control features within the RDIC software to detect process errors
- Check for foreign items and bonds
- Place endorsements on scanned items
- Identify and limit the fields that customers can edit (i.e.; dollar amount only)
- Review items manually keyed
- Review availability schedules (immediate credits, holds, routing of positive pay)
- Provide confirmation of receipt of file

Risk: Errors committed by client

Potential Strategies:

- Identify processes that customers can/cannot perform
- Include specific wording that states the customer must have effective controls in place or assume liability for failure in process
- Identify and limit the fields that customers can edit (i.e.; dollar amount only)
- Use one account to one merchant control (cannot image into multiple accounts)
- Implement a dual-control, role based process
- Identify a business process for reconcilements

CONCLUSION

As previously stated, there are many benefits to offering the RDIC product to clients. Implementing a RDIC solution can reduce expenses for the client and increase income and customer retention for the FI. However, while there are significant benefits, there are also risks associated with this product that both FIs and their clients need to be aware of and take steps to mitigate.

This paper identifies potential risks as they pertain to product distribution, equipment and software, information system security, images and image quality; and processes. It also provides FIs and their clients with recommended mitigation strategies to possible risks associated with RDIC. Not all of these strategies will work for all FIs. Rather, each FI must conduct its own risk assessment of its RDIC process and determine which strategies will fit their individual needs. FIs must take into consideration that RDIC is an ongoing practice where new standards are continually being developed. Flexibility is needed to take necessary steps in adjusting a FI's processes to meet these new developments. Most importantly, FIs must maintain an open dialogue with their clients and provide ongoing monitoring of their RDIC program following the initial implementation of the product.

With the proper understanding of both the benefits and risks of RDIC and with explicit terms and conditions that provide an understanding of the FI's and client's responsibilities, this product should increase client satisfaction and relations by providing an efficient and convenient method of banking.

ACKNOWLEDGEMENTS

BITS would like to acknowledge BITS Electronification Working Group Co-Chairs Lisa Zarzycki, Comerica Incorporated, and Rick Pickens, Bank of America Corporation, for their leadership in developing this paper. In addition, we would like to acknowledge the following individuals who drafted various sections of this paper:

Austin McCormick, Citigroup
Christian Tomooka, City National Corporation
Dexter Holt, Federal Reserve Bank of Boston
Stan Sienkiewicz, Federal Reserve Bank of Philadelphia
Tom Haller, Marshall & Ilsley Corporation
Darlene Moore, Wells Fargo & Company

The following institutions are represented by participants in the BITS Electronification Working Group and may have provided input into the development and/or review of this paper:

American Bankers Association	HSBC North America Holdings, Inc.
American Express Company	Huntington Bancshares Incorporated
American General Financial Services, Inc.	JPMorgan Chase & Co.
AmSouth Bancorporation	KeyCorp
Bank of America Corporation	M&T Bank Corporation
Bank of Hawaii Corporation	Marshall & Ilsley Corporation
The Bank of New York Company, Inc.	Mellon Financial Corporation
BB&T Corporation	NACHA
Capital One Financial Corporation	National City Corporation
Check Payment Systems Association	NetBank, Inc.
Citigroup Inc.	Northern Trust Corporation
Citizens Financial Group, Inc.	The PNC Financial Services Group, Inc.
City National Corporation	Regions Financial Corporation
Comerica Incorporated	Sky Financial Group, Inc.
Commerce Bancshares, Inc.	Sovereign Bancorp, Inc.
Compass Bancshares, Inc.	State Farm Insurance Companies
Countrywide Financial Corporation	SunTrust Banks, Inc.
CUNA/GHS Federal Credit Union	TD Banknorth, Inc.
CUNA/Valley Credit Union	U.S. Bancorp
Custom Direct, Inc.	UnionBanCal Corporation
Deluxe	USAA
Federal Reserve Bank of Boston	Wachovia Corporation
Federal Reserve Bank of Philadelphia	Washington Mutual, Inc.
Federal Reserve Board	Wells Fargo & Company
First Horizon National Corporation	Zions Bancorporation
FSTC	
General Electric Company	

ABOUT THE BITS FRAUD REDUCTION STEERING COMMITTEE AND PROGRAM

The BITS Fraud Reduction Steering Committee was created to:

- Reduce payment-related fraud losses.
- Secure a critical mass of financial institutions to participate in a shared account database and standardized data collection process.
- Identify successful strategies for reducing check fraud and make those strategies available to the industry.
- Assess fraud risk exposure to electronification and develop strategies to minimize losses.

Working Groups under the BITS Fraud Reduction Program include:

- Debit Card/ATM Fraud
- Electronification
- Emerging Fraud Risks
- Identity Theft
- Internet Fraud
- Prevention of the Exploitation of the Elderly and Vulnerable
- Shared Databases

About BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Advisory Board and BITS Advisory Council. For more information, go to www.bitsinfo.org.

BITS

1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
WWW.BITSINFO.ORG
(202) 289-4322

APPENDIX A: Risk and Mitigation Strategy Matrix

Topic	Risk	Potential Strategies
Product Distribution	Risk: Inadequate knowledge of product by sales staff which causes product to be marketed to unqualified clients	<ul style="list-style-type: none"> • Provide initial and ongoing training to individuals responsible for sales and service of product • Provide technology overview of product and process flow to individuals responsible for sales and service of product • Require those individuals responsible for sale of product to sign-off acknowledging risk • Limit product to Treasury Management departments of established small businesses, and middle market and large corporate customers • Implement a risk assessment process to determine if client is a viable candidate for use of product • Adhere to internal KYC programs • Perform enhanced due diligence on prospective clients (underwriting processes, background checks on business and principles, qualification process) • Require clients to provide collateral with a dollar amount determined from a sliding scale relative to risk exposure from the total deposits • Tie sale of product to loan risk rating
	Risk: Improper or incorrect use of product by client	<ul style="list-style-type: none"> • Re-certify clients at least annually to ensure an acceptable risk level (similar to wire certification) • Require periodic on-site inspections and review the file information received • Perform ongoing enhanced due diligence (underwriting processes, background checks on business and principles, qualification process)
Equipment/ Software	Risk: Hardware/software will not interoperate with FI or industry or meet minimum industry capture and processing requirements	<ul style="list-style-type: none"> • Ensure that minimum standards are defined • Define ownership and deployment of equipment and software as part of the terms and conditions and establish equipment replacement procedures • Determine if imaging equipment and software is proprietary or commercially available • Ensure imaging equipment and software is compatible with FI software and equipment • Ensure that all equipment/software (purchased/not purchased through the FI) is evaluated and certified to meet minimum requirements • Implement quality control process to ensure images are of good quality and are in expected formats

Topic	Risk	Potential Strategies
Equipment/ Software (cont.)	Risk: Equipment not functioning as intended.	<ul style="list-style-type: none"> • Ensure that there is oversight and a quality control process in place • Perform calibration to ensure that system set-up and maintenance procedures are properly performed • Monitor and check equipment on a regular basis to ensure it is functioning properly • Review volume and bandwidth capabilities • Educate client on the importance of performing regular equipment maintenance
Information System Security	Risk: Unauthorized access to and/or use of the imaged information	<ul style="list-style-type: none"> • Ensure software has user authentication capabilities, with acceptable user administration functionality at the client site • Ensure the software has audit trail capabilities • Ensure software and process provides data security • Assign user(s) credentials that are password-protected
	Risk: Edited or unauthorized files are submitted for clearing	<ul style="list-style-type: none"> • Secure transmission mechanism according to FI's best practices • Software should only accept transmissions from validated sources by authentication • Restrict and control installation of software at client site • Ensure that software has the ability to validate the sources of the file and validate that the file has not been compromised
	Risk: Loss of data	<ul style="list-style-type: none"> • Identify and resolve communication issues that impact transmission of data between FI and client • Establish authentication process to validate source and allow authentication at both client and FI site • Ensure that equipment and software have the ability to encrypt files to ensure data security and integrity if files are compromised

Topic	Risk	Potential Strategies
Images/ Image Quality	Risk: Poor Image Quality <ul style="list-style-type: none"> • Inability to validate amount (CARLAR) • Inability to distinguish image survivable security features • Inability to recognize and detect information in fields • Inability to check that the image captured meets depositor and/or check-writer expectations for usability • Inability to reproduce the check once it has been cleared • Check image is not usable for purpose intended 	<ul style="list-style-type: none"> • Establish an ongoing process to ensure good quality images • Identify and ensure clients comply with existing image quality standards • Ensure image formats comply with current ANSI standards • Deploy image inspection tools, at the point of capture, downstream, and RDIC to ACH, exchange or IRD printing • Implement image defect and image usability assessment tools along with image quality usability (IQU) and image quality analysis (IQA) engines for defect analysis/assessment and to ensure that the image is usable • Inspect images visually or using image usability assessment software to ensure key fields (MICR, amount, maker, etc.) are readable for clearing • Retain document long enough to ensure a usable image • Ensure ability to effectively retrieve original source documents or captured images, as applicable • Implement a quality review process to oversee CARLAR accuracy rates • Perform quality check at client location and processor location
	Risk: Inability to settle item	<ul style="list-style-type: none"> • Determine document settlement process (i.e. ACH, substitute check, image exchanges, etc.) • Establish and document a process for recourse to converting bank and ensure that converting FI has recourse to client • Develop timeframes in which an item may be resubmitted • Establish an agreement with the client to share the risk regarding representations and warranties for substitute checks
	Risk: Point of capture difficulties (i.e.; mis-matched, piggyback, or skewed images.)	<ul style="list-style-type: none"> • Ensure high-level image defect analysis (IDA) and MICR code lines are done at the point of capture • Allow the person performing the scanning of checks to see the image as it is captured • Ensure that the image is reviewed at capture • Ensure that batch mode processing is being used as this will enable images to be automatically assessed while allowing for more consistent human review

Topic	Risk	Potential Strategies
	Risk: Duplicate images entering payment stream	<ul style="list-style-type: none"> • Incorporate quality controls to search for duplicate items at client and FI processing stage • Ensure that client has a process to secure items after imaging to prevent their re-entry
Processes	Risk: Multiple presentment of same item	<ul style="list-style-type: none"> • Check for duplicate items • Check for duplicate batches • Establish a process control to identify duplicate items across entry points within RDIC software • Develop a business process to cross reference multiple points of presentment for duplicate items (payment database of record)
	Risk: Fraud and returned items	<ul style="list-style-type: none"> • Ensure clients have established security procedures and are stated in terms and conditions • Ensure checks deposited through RDIC are fed through fraud detection systems • Define loss mitigation and develop a plan, including the fraud tools used • Establish an escalation process for fraud suspects • Monitor incoming transactions for unusual activity • Place liability on the party best able to prevent losses • Preclude client from depositing items drawn on their own accounts through RDIC • Identify clearing channel and ultimately regulations that guide returned item process
	Risk: Operational-related risk	<ul style="list-style-type: none"> • Check for valid routing and transit (R&T) • Use CAR/LAR to detect amount keyed vs. check image • Use operational control features within the RDIC software to detect process errors • Check for foreign items and bonds • Place endorsements on scanned items • Identify and limit the fields that customers can edit (i.e.; dollar amount only) • Review items manually keyed • Review availability schedules (immediate credits, holds, routing of positive pay) • Provide confirmation of receipt of file

Topic	Risk	Potential Strategies
	Risk: Errors committed by client	<ul style="list-style-type: none"> • Identify processes that customers can/cannot perform • Include specific wording that states the customer must have effective controls in place or assume liability for failure in process • Identify and limit the fields that customers can edit (i.e.; dollar amount only) • Use one account to one merchant control (cannot image into multiple accounts) • Implement a dual-control, role based process • Identify a business process for reconcilements

APPENDIX B: Image Quality Assurance Strategies

Image Quality Assurance Strategies:

Presently, there are no widely accepted industry-level image quality standards. The industry has settled on an operating point that uses black and white images having a minimum resolution of 200 dots per inch (DPI). Within these fundamental operating parameters there can be substantial variations on how image-processing systems retain faint information and how they react to certain types of check background colors and patterns. Even image processing solutions from the same solution provider can exhibit variations between devices.

Image quality assessment processes are emerging that will enable benchmarking baseline capture system performance and this process is described in the segment on image capture and processing systems. Even with proper system set-up and maintenance, some checks will not image well. These situations are caused by the characteristics of the source document including the use of check stock that does not comply with current industry standards. The governing standard for image-friendly check stock is called “Bank Check Background and Convenience Amount Field Specification” (ANS X9.7-2006). The industry has learned much about the printing factors that influence image processing systems and that standard is being substantially revised. All paying banks should encourage their customers to use standards compliant check stock and advise them of the implications of choosing not to use that type of stock.

Current automated image quality tests fall into two classes: image defect tests and image usability tests. Defects tests look at conditions on the entire image and usability tests focus on specific data fields that are judged to be important to check clearing needs. Until recently, these tests have been defined by the solution provider. The industry has now defined a common set of defect test metrics that will provide uniform results across platforms and is trying to extend that thinking into uniform outputs from image usability assessment tools.

The Image Defect Assessment (IDA) characterizes the metrics used to examine the entire image in an automated fashion and the thresholds for suspect processing (typically via manual review of check image which must be factored into an institutions daily production. The most important defect conditions appear to be images that are too light or too dark.

The Image Usability Assessment (IUA) refers to field level analysis on the check image. The following pre-printed or written fields influence judgments made on the suitability of the image for presentation to customers, for operational risk management processes and for clearing of the items. The fields considered most important for usability assessment are: convenience and or legal amount, payee names, maker of check, signature, and MICR code line data

Field level image quality tools are not in common use and usually embody assessment techniques that are unique to each solution. Financial institutions may want to assess incorporating these into their test programs to minimize the risk of unusable images as defined above, but need to recognize that their specific criteria may not align with other institutions criteria until the industry has completed further study in this area. It is felt that there are not likely to be standard usability metrics until 2007 at the earliest.