

Remote Deposit Capture

A White Paper Addressing Regulatory, Operational and Risk Issues

By: **Paul A. Carrubba**

Special Counsel
Adams and Reese LLP

Mary Hockridge

Executive Vice President
NetDeposit, Inc.

Michael K. Harris

Consultant
Executive Project Support

The Check Clearing for the 21st Century Act (Check 21) and the substitute check created new opportunities for financial institutions and their customers. But, the Act also created new operational and risk issues for financial institutions that take advantage of the opportunities and offer remote deposit capture to their customers giving them the convenience of electronically depositing checks. With remote deposit capture, instead of physically transporting checks to a banking facility, customers are able to scan checks on image scanners maintained in their own offices and transmit the images to the financial institution via the internet or dedicated lines. This paper will address and provide suggestions for best practices to manage and mitigate risk in the following areas: regulations, laws, contracts, fraud detection, operations and software capability.

Regulatory Issues

The unexpected consequences of making a deposit via electronic means versus delivering the paper checks introduce some interesting questions and the need for legal interpretation of the laws that have governed banking for many years. It is important to understand the impacts in the following areas:

- Bank Branch Law
- Assignment of Funds Availability
- Return Item Timeframes–Local Item DeterminationNon-public customer information includes, but is not limited to, the following:

Remote Capture Locations and Bank Branch Law

While Regulation CC (Reg CC) establishes where a deposit is made if the check is deposited at a physical location of the bank, it is silent as to where a deposit is made when the deposit is delivered via a transmission of an image of the original check. However, there is no question that a deposit is made when the customer sends a transmission of images of checks to the bank. Under the McFadden Act, 12 U.S.C. Section 36, a "branch" is a location established by a national bank at which deposits are received, checks paid, or money lent.

So the question that is raised is, must the bank make a branch application to take remotely captured checks from customers? This question was recently answered by the Comptroller of the Currency in Interpretive Letter #1036, August 2005. According to the Letter, the customer's place of business is not a branch, even though the bank is taking a deposit, because this activity is excluded from the definition of branch. The definition of a branch excludes Automated Teller Machines (ATM), Automated Loan Machines (ALM) and Remote Service Units (RSU). An RSU is defined as; "An automated facility, operated by a customer of a bank that conducts banking functions, such as receiving deposits. An RSU includes an ATM, ALM, and an automated device for receiving deposits. An RSU is not a 'branch' and is not subject to state geographic or operational restrictions or licensing laws." The scanning device operated by the customer meets the definition of an RSU and is not a branch whether the scanner is owned by the bank or the customer. While this Interpretive Letter applies only to national banks, it is likely that the FDIC and the Federal Reserve Board will follow the OCC's Interpretive Letter.

Requirements for Funds Availability

The next regulatory issue pertains to when the financial institution must make the funds available to the customer under Federal Reserve Board Reg CC. While many banks give customers next day availability, the question of availability becomes an issue when a bank invokes a case-by-case hold or invokes an exception hold. The hold period is based on whether the item that is deposited is a local or non-local item. If the depository bank and the drawee bank are located in the same Federal Reserve processing region, the item is a local item. If the depository bank and the drawee bank are located in different Federal Reserve processing regions, the item is considered a non-local item.

With the customer scanning a check for deposit, the problem is determining the definition of where the deposit is being made. Section 229.19 of Reg CC establishes when deposits are received by a bank. Under that section the determination as to when the deposit is received is based on the location of the staffed facility, ATM, or contractual branch at which the funds are deposited. In the case of a remote deposit, the funds are not deposited at any of the locations described in the Regulation. Therefore, according to an unofficial interpretation by a Federal Reserve Board staff attorney, since the funds are not deposited at a location specified in Reg CC, the images of the remotely captured checks are not subject to the availability requirements of Reg CC. The issue of availability and the period of time for which funds may be held must be resolved by agreement between the parties.

Determination of Local vs. Non-Local Status for Return Item Timeframes

Another Reg CC question that is raised by remote deposit capture is how to determine whether the item that was deposited is a local or non-local item for purposes of return item timeframes. If the image of the item is used to create a substitute check, the depository bank would be identified on the substitute check in the same manner as the depository bank of an original item. If the image of the item is presented pursuant to an image exchange agreement, the depository bank would be identified in the image file. Under either scenario, the location of the customer and the location of the place to which the image is transmitted are immaterial. The determination as to whether the item to be returned is a local or non-local item would be made based on the depository bank identified on the substitute check or in the image file.

The remote capture of deposits eliminates state boundaries in the banking industry. A bank could have one location in a state and receive image transmissions from customers in all of the other states. On the other hand, a bank could have physical locations in all states but receive image transmissions in only one state. The issue here becomes one of jurisdiction and the application of state law. As to the application of state law for the purpose of agreements and the state version of the Uniform Commercial Code, it would appear that the agreement between the bank and the customer could establish the controlling law.

The bank could likewise provide in an agreement that the customer submits to a specific jurisdiction stated in the agreement. As to whether having a customer within a state that transmits an image file to the bank would subject the bank to that state's jurisdiction is a question of local law. Jurisdiction may also hinge on who owns the equipment. It would appear that if the customer owns the equipment, the court would be less likely to apply jurisdiction than if the bank owned the equipment. The application of a state's jurisdiction is normally based on whether the person or company is doing business within that state. This is an issue that must be addressed by local counsel.

The Remote Deposit Customer Agreement

A financial institution can substantially reduce its risk of loss by drafting and executing a comprehensive agreement with its customer. Customers are not subject to the warranty and indemnification provisions of Check 21 and do not have the right to present substitute checks or images to the bank without an agreement. Without an agreement, a customer may only deposit original checks. The agreement accomplishes the following:

- Allows the customer to transmit images of checks to the bank in place of depositing the original check
- Defines the relationship between the bank and the customer
- Establishes the duties of the bank and the customer
- Establishes the procedures the customer must follow
- Defines the liabilities of the parties

Following are some of the provisions that a financial institution should consider when drafting the remote deposit capture agreement.

Hardware and Software

To perform remote deposit capture, the bank customer needs to purchase or lease check scanning hardware and license new software and/or subscribe to new services. The agreement should address these hardware and software issues. The agreement should contain an attachment that lists these requirements so that the requirements are clear. Because the quality of the image will be determined by the type of scanner that is used, the customer should not be allowed to purchase the least expensive scanner in the market place. However, this will surely occur if the customer is not given specifications or required to use specific scanning hardware certified by the solution provider. This section of the contract should also clearly identify whether the customer will be required to obtain the services of third parties, such as scanner maintenance, and whether the expenses related to those services are to be included in the fees charged by the bank.

Eligible Items

The agreement should limit the items that may be deposited to only cash items drawn on financial institutions within the United States. The original foreign items must be entered for collection in the same manner as is done today.

The bank may also consider not allowing the customer to deposit checks issued by and drawn on the customer or affiliates of the customer. The purpose for this restriction is to reduce the probability that the customer may initiate a check kiting scheme. One of the lines of defense in a check kiting scheme is the examination of the items that are being deposited. The bank may be less likely to examine images for check kiting when items are electronically transmitted to the bank.

Image Quality

The quality of the check image is extremely important for both image exchange and for the creation of substitute checks. This provision may very well be one of the most important provisions of the agreement. The provision should very clearly specify the image quality requirements. In describing the quality of the image, it is suggested that the bank review the commentary to Subpart D of Reg CC for guidance. The commentary contains a description of the elements that must be legible for a substitute check to be considered an accurate representation of the original check. The provision should require that the images also meet any standards for image quality established by ANSI, the Board of Governors of the Federal Reserve, or any other regulatory agency, clearing house or association.

Receipt of Files

The agreement should define the point at which the bank actually acknowledges receipt of a file from the customer. The fact that the customer transmits a file should not mean that the bank received the file. The bank should consider stipulating that only if it specifically acknowledges receipt of the file will the bank regard it as in-fact received. However, acknowledging receipt of the file should not mean that the bank acknowledges that the file contains no errors or that it is responsible for the information in the file. The provision should state that the credit given for the file is provisional and that the customer indemnifies the bank for any loss sustained by the bank for acceptance of the file.

The bank should also reserve the right to reject the file without liability to the customer. This provision should also clearly state that the bank is not responsible for files which it does not receive or for images that are dropped during the transmission. Likewise, the bank should also disclaim liability for alterations made to files after they are transmitted to the bank.

Deposit and File Limits

Remote deposit is somewhat similar to allowing a customer to originate ACH credit files. While the nature of the potential liability is different, the risks are similar. Therefore, the bank should consider establishing deposit limits to reduce the amount of exposure to the bank. The bank may also consider establishing a limit to the number of files that may be transmitted each day. From a purely operational perspective, some banks may want to establish such a limit to prevent an unlimited number of files being transmitted each day by the same customer.

Deadlines and Missed Deadlines

The agreement should clearly establish deadlines for receipt of files and should define the disposition of files that are received after the cut-off time. The deadline should be based on when the file is received by the bank and not when the file is transmitted. Time zones should be considered when establishing the time for receipt of the files.

Method of Presentment of Items

The manner in which items are cleared or presented for payment should be left up to the bank in its sole discretion. The bank's deposit account agreement should be incorporated into the remote deposit agreement and referenced in this section of the agreement. The deposit account agreement will also contain a provision that addresses the collection of items. The bank should also reserve the right to select the clearing agents through which the bank clears items and establish that the customer agrees to be bound by any clearinghouse agreements, operating circulars, image exchange agreements, etc., to which the bank is a party. This provision will give the bank the flexibility on the manner in which the items are cleared and the clearing agent that will be used. The bank may decide to clear some items as images and others as substitute checks.

Availability of Funds

As stated in the regulation section of this paper, it appears that images that are transmitted to the bank will not be subject to the availability requirements of Reg CC. The availability of the items that are remotely deposited must be established by the agreement. The bank may decide to give next day availability with case-by-case holds, grant availability by availability schedule and make the determination as to whether items are local or non-local based on the place to which the items are transmitted, or consider all items as non-local items. The agreement should also establish the basis for placing case-by-case holds and exception holds. Again, if Reg CC does not apply, the agreement must establish these times.

Warranty and Indemnification

This provision should contain a number of warranties that are given by the customer to the bank. The customer should warrant that:

- Only acceptable items will be deposited
- The images meet the quality standards
- There are no duplicate files or items
- Customer will not deposit the original check
- The bank will not sustain a loss because the customer has deposited an image
- All information provided by the customer to the bank is accurate and true
- The customer has complied with all rules, regulations and laws
- Files do not contain viruses
- The customer indemnifies the bank from any loss for breach of the warranty provision

This is not intended to be a complete list of all warranty items. The items are listed to give an example of the types of warranties which should be included in an agreement.

Maintenance, Retention and Destruction of Original Items

The agreement should contain a provision that addresses the issue of retention, storage and destruction of the original items. One argument against requiring the customer to destroy the original after some period of time is that if the customer sustains a loss because the original cannot be produced, the customer will look to the bank, because the bank instructed the customer to destroy the original item. On the other hand, the risk to the bank if the item is not destroyed is equally as great, if not greater.

The agreement should certainly require the customer to securely store the checks and to establish security procedures that limit access to the checks. Perhaps the checks should be stored under dual control with segregation of duties. If the bank decides to require destruction, the agreement should contain the period of time after which the checks should be destroyed. It would appear that thirty to sixty days would be a reasonable time to retain the original items.

Return Items

It should be obvious that, since the original check is kept or destroyed by the customer, any return items will not be of original checks. However, the agreement should contain a provision stating that if an item is dishonored, the customer will receive an image of the original check or a substitute check as the charged-back item. This section should also address special instructions and any related fees.

Contingency Plan

The agreement should also contain a provision that specifies the contingency plan. Unless the bank or service provider has an alternative method for capturing and transmitting the images of the checks, the customer should be instructed to take the original checks to the closest office of the bank. If the bank does not have a local office, it may consider using overnight delivery to an office of the bank under emergency conditions.

Errors or Discrepancies

The agreement should include a provision that requires the customer to closely examine notices and statements sent to the customer by the bank. The customer should also be instructed to report any errors to the bank within some period of time (30 days). If the customer does not report the error within the specified timeframe, then the bank will consider the transaction correct and the customer will be prohibited from making a claim against the bank for the error.

Financial Information

The customer should be required to submit financial information to the bank upon request. The bank should use this information in establishing or amending the deposit limit established by the agreement. The customer should also be required to notify the bank of any change in locations, transaction volumes or the financial condition of the customer.

Other Provisions

The contract should also contain the standard provisions of agreements including:

- The standard of care
- Limitation of Liability
- Confidentiality
- Attorneys' Fees
- Entire Agreement
- Waiver
- Severability
- Force Majeure
- Termination
- Governing Law
- Notices
- Etc.

Note: This section on contract terms is not a legal opinion and should not be used as Such. Competent legal counsel should be sought in drafting a remote deposit agreement.

Best Practices-Operational and Software Controls

The remote deposit capture product and process does create some unique business challenges. Three underlying changes become evident within the new process:

1. The check capture and storage process now begins in various remote physical locations that are not under the direct operational control of the bank.
2. The check capture process is completed by corporate staff and not banking staff.
3. The collection of the item through the banking system will be based upon the quality and integrity of the data and electronic image of the item captured at the remote location.

Since the capture and storage process starts at the remote corporate location, legal agreements need to be created and/or modified to address the roles, responsibilities, and risks within the new process.

The bank now needs to consider the corporate location not only a business client, but also a processing partner in the check collection process. New equipment (check scanners and personal computers), new procedures, and new people at the corporate remote location must all be successfully integrated into the collection process. Customer service programs and personnel within the bank must be trained to successfully support the new product and process. Operational readiness, disaster recovery and business continuity procedures must be considered. For example, a disaster recovery process that includes the customer physically taking the deposit to the nearest branch may work well, provided that the customer and the branch are in the same city, but does not work if the customer is in another state.

In addition, the bank must consider the “ripple effect” that remote deposit capture has on the other existing check collection processes. There will be impacts to the other check collection processes. However, the extent of the impacts will vary depending upon the definition of the remote capture process and how it is integrated into the existing check collection processes. The definition and integration of the remote capture process will differ by bank based upon the bank’s existing check processing capabilities and the manner chosen to collect the remote deposited item.

In today’s banking marketplace, check processing capabilities vary from legacy “paper-only” processes to complete electronic presentment and exchange. Operating models range from complete in-house processing to complete outsourced processing. Payment collection options range from the creation of image replacement documents to complete electronic exchange, or through the Automated Clearing House (ACH) environment. Each bank, therefore, must define and design its respective remote deposit capture product and process to both leverage and complement the existing processes and infrastructure.

All of the options and questions are identified and addressed via the mapping process. Regardless of the existing check capture and ACH processes, remote deposit capture can be successfully implemented. For example, even a bank with “paper-only” check processes can implement a remote capture product by capturing deposits at the remote corporate location, printing image replacement documents (IRDs) at its operations site and then feeding them into the existing check capture process.

Opportunity for Fraud

The introduction of new products and services often attract criminals eager to exploit vulnerabilities created by the confusion surrounding a new product or service and the eagerness on the part of the bank to sell a new service. Remote deposit capture will be no exception. In fact, remote deposit capture may create an irresistible temptation on the part of the bank’s own customers to take advantage of the vulnerabilities created by this new service.

Duplicate Deposits and /or Items

The electronic transmission of deposits creates the opportunity for the same check or checks to be deposited multiple times. A bank customer may transmit an image of a check to the bank and then deposit the original check at the same bank or at a different bank. Such activity could be an honest mistake or it could be an intentional act by the customer. The deposits could be made the same day, or the customer could hold the original and deposit it at a later date.

Another potential exposure that banks may face from its own customer is the potential for the customer to transmit duplicate files or duplicate images of checks to the bank. While the customer may not get away with this activity for very long, the amount of one duplicate image or file could be substantial under the right circumstances.

The bank’s remote deposit capture software should have the functionality to detect this type of activity even if the transactions occur weeks apart. Ideally, duplicate detection safeguards will be built into the software used by the customer to capture the checks, to deter fraud or prevent accidental deposit of the same item multiple times. Additionally the bank’s deposit receiving platform and deposit systems should have the capability to identify duplicate items. Deposited items suspected to be duplicates should be flagged for review by the bank at the earliest feasible point in the process.

Forged Endorsements

One type of fraud that is experienced by many banks in today's paper process is forged endorsements. Even though most banks have teller procedures to check for endorsements on checks before deposits are made at the teller window, many checks contain forged endorsements. Given the potential number of images that will be scanned and transmitted, it is not likely that a bank will be able to detect a missing or forged endorsement on the images of checks. A bank could, however, establish a dollar threshold over which items will be flagged for bank review, including the examination of endorsements.

Another potential method to detect this type of fraud is to use image technology to read the name of the payee on a check and compare that name to the name on the account to which the item is deposited. This method could reduce fraud unless the bank allows the customer to deposit third-party checks. While the customer warrants the authenticity of endorsements and that the customer has good title to the instrument, the depositing customer may not know that the original endorsement has been forged. Because of the exposure, some banks will not allow a customer to deposit a third-party check.

Alterations

Receipt of an image of a check instead of the original check may increase the bank's exposure to loss from alterations. While banks already experience this type of loss, it would appear that the potential for loss will be increased. Alterations are often difficult to detect on original items because of the advanced techniques used by criminals to make the alteration. Detection of alterations on a black and white image of an item will be even more difficult to detect. Discoloration and erasures will not be as apparent on an image.

Financial institutions should consider offering Positive Pay with payee name recognition to assist in detecting this type of fraud. Payee name verification utilizes automated recognition technologies to compare the name of the payee on the check when the item is presented to the name of the payee at the time the check was issued.

Counterfeit Items

The potential for fraud loss may also be increased because of counterfeit items. As in the case of alterations, the advances in technology have made detection of counterfeit original checks difficult. A fraudster can produce a counterfeit that exactly duplicates an original check.

An image of a counterfeit check will likewise be almost impossible to detect. The bank will not have the ability to examine the texture of the check, discoloration, watermarks, borders, heat sensors, and other physical fraud detection features.

The potential for loss may have an impact on the depository bank and the drawee. A counterfeit check is not a properly payable item but it is an item under the UCC and must be returned by the drawee by its midnight deadline. If the drawee fails to return the check by the midnight deadline, the drawee becomes accountable for the amount of the item. After the expiration of the midnight deadline, which is midnight of the next banking day after the day on which the item is presented, the drawee bank loses its right to charge the item back. Therefore, if the drawee pays the counterfeit check, it may not return the item and the drawee sustains the loss.

On the other hand, if the drawee sustains a loss because a substitute check was presented for payment instead of the original check, the drawee may have a claim under the indemnity provision of Check 21. In the above example, if the drawee can show that it would have detected the counterfeit item if the original check had been presented because of the physical fraud detection features on the original check, then the drawee would have an indemnity claim. The bottom line is that both the depository bank and the drawee have reason to be concerned about counterfeit items as they relate to remote deposit capture.

Changing the Payee

A number of banks have been in disputes over losses incurred as the result of changing the payee on checks. In this scam, a valid check is issued by a drawer to a payee and, in most cases, is mailed to the payee. The check is intercepted and the payee is changed either by alteration of the payee on the original check or by counterfeiting the check with all of the information the same as the original check except for the payee. Upon discovery of the fraud, the drawer makes a claim to the drawee that, in-turn, makes a claim back upstream to the depository bank. The drawee bank claims that the depository bank breached its transfer and presentment warranty because the payee on the check has been altered. The depository bank refuses to pay claiming that the check was not altered and is a counterfeit check that must be returned by the bank's midnight deadline. If the check were captured remotely, the original check will have been destroyed by the time the fraud is discovered making it virtually impossible to determine if the item was altered or was a counterfeit.

In the fraud scam previously described, the outcome may very well be determined on whether the payee was changed on the original check or by counterfeiting the check. If the payee were changed on the original check, the drawee bank would have a valid claim against the depository bank based on breach of warranty. The Uniform Commercial Code provides that the depository bank warrants that the item does not contain an alteration. If the original check were replaced with a counterfeit check, the depository bank very well may have a valid claim that the check must be returned by the drawee bank's midnight deadline. Therefore, the question of alteration versus counterfeit is a significant issue that is made much more difficult after the original check is destroyed. For this reason, banks should consider providing Positive Pay with payee name verification. As an alternative to payee name verification, the drawee could transmit images of checks over some dollar threshold that is presented for payment to the drawer to validate the payee on the check.

Original Check Retention

The concept behind remote deposit is that the customer scans the checks, transmits an image of the check to the bank and retains the original check. The question of whether the customer should be required to destroy the check after some period of time was addressed in the contract section of this paper. The fact that the customer retains the original check creates the opportunity for fraud to occur. One problem is that an employee or some other person could use the information on the check to commit identity theft. At a minimum, the check will contain the drawer's name, address, phone number, bank information including the customer's account number, and the check may contain a social security number or some other form of identification. Although the customer has possession of the check, the bank should ensure that the customer maintains the check in a secure manner to keep this exposure to a minimum.

Another problem associated with the retention of the check by the customer is the potential of customer fraud or fraud by the customer's employee. As long as the customer has possession of the original check, the customer could (unintentionally or intentionally) deposit the original check in addition to remotely depositing an image of the check. If the checks are not securely maintained with proper security procedures, employees of the customer or other third parties could steal the checks and cash or deposit them. The potential for this type of fraud is significantly higher than it is prior to implementing remote deposit. Prior to remote deposit of items, customers have experienced employee fraud when employees take checks payable to the customer and cash or deposit them. The employee takes the check even though the employer may miss the payment. After the implementation of remote deposit, the employer will receive credit for the payment when the image of the check is deposited with the employer's bank. The point here is that the temptation will be elevated. The fear of getting caught will not be as great when the employee knows that the employer will not miss the money.

Conclusion

Each bank should review its business plan, technology and procedures to ensure that it has addressed the following critical areas:

- Regulatory compliance, impacts and areas of exposure
- Implementation of customer agreements that are comprehensive and protect the interests of the bank
- Acquisition of technology that provides safeguards and controls to prevent or, at a minimum, provide earlier detection of suspicious activity
- Operational procedures that support protection of the bank

Financial institutions around the country are at various stages of taking advantage of remote deposit capture. Some leading-edge banks have been offering the service since the passage of Check 21 and are well into the process. Some banks are in the middle of the process or have just started. Many banks fall into the last category and are putting this decision off until the last minute. Without regard to which stage a bank may be in, it is never too late to assess the risks and implement controls to reduce those risks.

About the Authors

Paul A. Carrubba

Special Counsel
Adams and Reese LLP

Paul is an accomplished legal, banking and business authority. His current legal work is primarily focused on Banking Law and legal issues dealing with payment system fraud.

Most recently, Paul was a shareholder in the law firm of Watkins Ludlam Winter & Stennis, P.A. in The Regulated Industries Group. Paul was Executive Vice President and Managing Director of the Global Payments Group of Carreker Corp., where he had responsibility for the management of the P&L for the software business units. Paul's banking career includes positions as Senior Vice President and Manager of Operations for Deposit Guaranty National Bank, Chairman of the Board of Directors of the Southern Financial Exchange, and a member of the Executive Committee and Board of Directors of the National Automated Clearing House Association (NACHA). Paul's work has been published in a number of banking publications.

Paul holds a B.S. in Banking and Finance from University of Southern Mississippi and a J.D. from the Mississippi College School of Law (Cum Laude).

Mary Hockridge

Executive Vice President
NetDeposit, Inc.

Mary brings over 20 years of executive experience in software product management, marketing, and sales in the financial services industry. Mary joined NetDeposit in 2004 and oversees the strategic development, ongoing evolution and marketing of NetDeposit's products and services. From 1997-2004, she was a member of the management team at Carreker Corporation, most recently as Senior Vice President for the company's image exchange and archive business units. Previously Mary provided product and sales services for QuestPoint Remittance Services and Security Pacific Bank.

Mary holds a B.A. in Business Economics from the University of California, Santa Barbara, and is a Certified Cash Manager (CCM).

Michael K. Harris

Consultant
Executive Project Support

Mike has over 31 years of experience as a banker, vendor, consultant, and teacher in the payments arena.

Mike has served in senior management positions and provided services to BAI, the Federal Reserve, NetDeposit Inc., Carreker Corporation, Chase, The Texas State Bankers Association, Thomson Financial Publishing, and Vector SGI, all focusing on the enhancement of payment processing. Earlier in his career, Mike was employed by Equitable Trust Company in Baltimore, and Mercantile Safe Deposit and Trust Company. He has worked on various payment projects with major U.S. and U.K. banks as well as IBM, Unisys, and NCR.

Mike holds a B.S. degree in Mathematics from Towson State University (Summa Cum Laude): 1974 and has completed various IBM, Unisys, and MS technical and general business courses.