Remote Deposit Capture: A Primer

To remain competitive, financial institutions continually look for ways to cut costs, attract new customers, and boost revenues. Remote deposit capture (RDC) technology helps to streamline and improve the efficiency of one area of bank operations: processing check deposits. RDC allows financial institution customers to "deposit" checks electronically at remote locations, usually in the customers' offices, for virtually instant credit to their account. Paper checks are digitally scanned, and an image of the check is electronically transmitted to the customer's bank.

Most RDC customers are merchants who want to reduce the costs of transporting paper checks to their financial institution and gain faster access to their funds. Funds from a paper check are typically available within five business days. However, with RDC, funds from checks remotely deposited on Monday often are available on Tuesday or Wednesday of the same week—a significant financial advantage to all businesses, particularly for small- and medium-sized businesses. Some banks are marketing RDC to doctors and lawyers, two professions that often receive payment for their services by check.[1] Other types of businesses that are customarily paid in cash or by credit card, such as restaurants, would not necessarily benefit from RDC.

This article discusses the development and recent growth in the use of the RDC technology, identifies risks to financial institutions that offer this service, and highlights appropriate risk management techniques described in recently issued Federal Financial Institutions Examination Council (FFIEC) guidance.

Background

The Check Clearing for the 21st Century Act (Check 21 Act), which took effect October 28, 2004, paved the way for the development of RDC. The Check 21 Act created a new negotiable instrument called a "substitute check," which is the legal equivalent of an original check. A substitute check contains an image of the front and back of the original check that can be processed as the original check.[2] The customer transmits this image electronically, usually via the Internet, to the depository financial institution. The substitute check is cleared and settled electronically, thereby expediting credit to the customer's account.

First Tennessee Bank in Memphis was one of the first financial institutions to implement RDC. It introduced the "First Deposit Plus" product[3] in 2003 as a way to expand its deposit base. As of March 2008, First Tennessee had customers in 46 states using its RDC service.[4] In July 2007, Forrester Research, an information technology research company, reported that 88 percent of the top 25 U.S. banks were offering RDC to their business customers.[5] For example, Bank of America, Citibank, and PNC offer RDC to their commercial customers.[6]

[1] Anonymous, "Cherry-Picking Remote Deposit Customers," *US Banker*, August 2008, pp. A8–10.

[2] See FIL-116-2004, "Check Clearing for the 21st Century Act," October 27, 2004.

[3] First Tennessee Bank, "Every Office Needs a Time Machine" brochure, 2008.

[4] Peggy Bresnick Kendler, "Can Remote Deposit Capture Drive Growth?" *Bank Systems & Technology,* March 2008, http://www.banktech.com/channels/showArticle.jhtml?articleID=206900812.

[5] Forrester Research, "Coming Soon: Remote Deposit Capture for Consumers?" research note, July 27, 2007; updated August 3, 2007.

[6] Bank of America, "Bank of America Expands Remote Deposit Service Globally," press release, September 16, 2008, http://newsroom.bankofamerica.com/index.php?s=press_releases&item=8257; Citibank, "Citibank Introduces Remote Electronic Deposit Service for Business Clients," press release, June 7, 2007, http://www.citigroup.com/citi/press/2007/070607c.htm; PNC, "PNC Bank to Offer Ease of Online Deposit Service Integrated with QuickBooks to Small Businesses," press release, July 24, 2006.

Capital One
Exhibit 1043
Capital One v. Wapp Tech
IPR2025-01325
Ex. 1043-001

Remote Deposit Capture

continued from pg.19

As of year-end 2008, Celent, an international financial services consulting firm, estimated that two-thirds of all U.S. banks were offering RDC services.[7] And in March 2008, the *ABA Banking Journal* published the 12th Annual Community Bank Competitiveness Survey, which reported that 38 percent of the community banks surveyed offered RDC, and another 26 percent were planning to offer the service by year-end 2008. The survey noted that the adoption rate for RDC is "much faster than we saw with bank Web sites."[8]

For financial institutions using RDC, the numbers are impressive. For example, in 2008, Zions Bancorporation in Utah and its affiliates reported that more than 11,000 customers were using their RDC service, depositing more than $400 million daily. Zions reported adding 45 new RDC customers per week.[9]

Some banks offer RDC for free on the condition that the customer maintains a certain minimum deposit balance. Others charge a fee, perhaps $60 a month.[10] Specialized scanners record and transmit images of the front and back of the check being deposited.[11] Scanners, which cost between $225 and $2,500, can be purchased by the customer or leased from the financial institution as part of the RDC service. One bank reports that RDC costs less than $10,000 to implement, well below the $300,000 minimum capital cost of a new branch office.[12]

Although RDC offers considerable benefits to financial institutions and their customers, the service is not without risks. For example, an institution no longer has the opportunity to examine the physical item being deposited, which heightens risk in the check-clearing process. The operational, legal, and compliance risks associated with RDC are discussed below, with particular emphasis on the risk of fraud.

Managing RDC Risks

In response to the increasing use of RDC, in January 2009, the FFIEC issued guidance to help financial institutions identify risks in their RDC systems and evaluate the adequacy of controls and risk management practices.[13] The guidance also should be useful to bank examiners, especially those who may be examining a bank offering RDC for the first time. Examination procedures targeting the use of RDC, which are consistent with the guidance, are scheduled to be published in a revised and updated version of the *FFIEC Retail Payment Systems Booklet.*[14]

The risks associated with the use of RDC should be identified within the financial institution's overall risk assessment process. The primary risk is the potential for fraud. When an institution takes a risk-sensitive function, in this case accepting items for deposit and credit to a customer's account, and allows it to be conducted outside the

[7] Celent, "State of Remote Deposit Capture 2008: Sprint Becomes a Marathon," press release, October 15, 2008.

[8] 12th Annual Community Bank Competitiveness Survey, *ABA Banking Journal,* March 2008, http://www.aba.com/News/CBOnline_Mar08_1.htm.

[9] Anonymous, "Remote Deposit Capture Partnerships for Success," *US Banker,* August 2008, p. A11.

[10] Orla O'Sullivan, "Prized Deposits Grow for Boston Bank Using RDC," *Bank Systems & Technology,* November 2008, p. 41. See http://www.banktech.com/architecture-infrastructure/showArticle.jhtml?articleID=211600480.

[11] Financial institutions generally recommend specialized scanners that read a check's magnetic ink character recognition line and optical character recognition to determine the dollar amount of the check in characters and words.

[12] O'Sullivan, "Prized Deposits Grow for Boston Bank Using RDC."

[13] FIL-4-2009, "Risk Management of Remote Deposit Capture," January 14, 2009. See www.fdic.gov/news/news/financial/2009/fil09004.html.

[14] FFIEC IT Examination Handbook, *Retail Payment Systems Booklet,* March 2004.

Ex. 1043-002

"trusted zone" that includes its internal network and closed check-processing environment, the risk of fraud increases. A financial institution can control what occurs on its internal network or in its check-processing facility, including the implementation of fraud prevention processes, but it cannot exert the same control over items deposited remotely.

The FFIEC guidance identifies three categories of risk to financial institutions that offer RDC: operational, legal, and compliance. The following discussion identifies these risks and outlines effective risk management strategies.

Operational Risks and Controls

The FFIEC guidance covers several issues that require management attention. Many of these risks relate directly to the potential for fraud, while others may also result in fraud in certain circumstances. Some of the key risks are as follows:

- Redeposit of items/duplicate presentment
- Alteration of deposited items/forged endorsement
- Deposit of counterfeit items
- Poor image quality
- Safety and integrity of deposited items held by customers (i.e., protection of personal information)
- Proper disposal of deposited items by customers
- Customer authentication when accessing the RDC system
- Data security of and lack of encryption in the RDC system
- Reliability of the RDC vendor

Customer Screening

Customer screening is the single most effective risk mitigation technique that financial institutions should implement when offering RDC. Not all customers need RDC services, and not all may qualify for them. The institution should consider whether the customer is a long-standing client with effective management and close control of financial processes or a new customer whose business characteristics and transaction history are relatively unknown. Many financial institutions offering RDC services require customers to maintain minimum deposit balances to insulate the institution from the risk of fraudulent deposits or items that do not clear owing to insufficient funds.

Financial institutions also should consider the customer's business line, geographic location, and client base. In evaluating a customer's client base, the institution should carefully scrutinize those from higher-risk industries, such as mail order or Internet retailers, adult entertainment, offshore businesses, and online gambling. These industries have demonstrated a greater risk of fraud and nonpayment than more traditional, domestic, face-to-face businesses. Customers that serve these higher-risk businesses may not be appropriate candidates for RDC or may be required to maintain higher deposit balances or agree to more stringent on-site audit procedures.

To date, the federal financial institution regulatory agencies have not observed increased fraud rates related to RDC services. In fact, the RDC fraud rate is lower than the average for general item processing.[15] The consensus among the agencies is that this is due primarily to satisfactory customer screening on the part of financial institutions offering RDC.[16]

[15] Risk Management of Remote Deposit Capture, internal presentation for FFIEC supervisory staff, January 28, 2009.

[16] Ibid.

Ex. 1043-003

Remote Deposit Capture

continued from pg. 21

Monitoring and Reporting

Financial institutions should regularly produce internal reports on the status of their RDC service. For example, the reports should cover duplicate deposits, violations of deposit thresholds (the total value of checks that may be deposited daily via RDC), velocity metrics (the number of items being deposited daily), transaction dollar volume, return item dollar volume, the number of checks rejected owing to poor image quality or other factors, and other adjustments made after deposit owing to discrepancies in the check amount. Management should review these reports in a timely manner, and any aberrations should be addressed promptly within the institution or with the customer or the RDC vendor.

Vendor Screening

Most banks offering RDC services work with a vendor that provides, installs, maintains, and updates the hardware and software. Although this is generally a sound approach, management should evaluate the track record of RDC vendors to ensure that they are reputable and competent. Financial institutions should look for vendors with experience in providing RDC services and should check references. Either the institution or the vendor should ensure that the customer's employees are trained in the use of the RDC system. The FFIEC *Outsourcing Technology Services Booklet* contains information and recommendations on how financial institutions should screen, evaluate, and monitor technology vendors, including those providing RDC services.[17]

Customer Audits

After determining that a customer's business is suitable for RDC services, the institution may consider evaluating the customer's operational controls (i.e., separation of duties, implementation of dual controls, endorsement of items to prevent redeposit, and secure storage and disposal of original checks) on-site; assessing how the customer's employees responsible for depositing items will be trained; and reviewing the physical and logical security measures surrounding the RDC system. Confirming that the customer securely stores and disposes of the original paper checks is particularly important as these items contain sensitive financial information (name, address, bank name, and account number) that can be used by identity thieves. In some cases, an independent audit of the customer may be warranted.

Business Continuity Planning

The FFIEC requires every financial institution to have a business continuity plan (BCP) in place.[18] If an institution offers RDC, its BCP should describe actions to be taken if the RDC system fails and the steps to return the RDC service to operation.

Change Control Processes

As is the case with any technology system, RDC hardware, software, and procedures will need to be updated over time. Financial institutions and, if appropriate, their RDC vendor should have in place written change control procedures (i.e., mutually agreed-upon procedures governing how software and hardware will be updated and how policies will be revised) with all customers using the RDC service. Thus, all parties will be on the same page when software or hardware is updated or policies and procedures are revised. Change control procedures can help avoid glitches from checks not being deposited or funds not being credited to the customer's account.

[17] FFIEC IT Examination Handbook, *Outsourcing Technology Services Booklet,* June 2004.

[18] FFIEC IT Examination Handbook, *Business Continuity Planning Booklet,* March 2008.

Ex. 1043-004

Insurance

Financial institutions should investigate whether commercial insurance coverage is available to protect them from liability in the event of problems with the RDC service. Management will need to determine whether the amount of coverage available justifies the cost of the insurance.

Legal Risks and Controls

When a bank accepts a check image for deposit through its RDC system and clears and settles the check, it exposes itself to certain legal risks under the Check 21 Act, Regulation CC,[19] Regulation J,[20] and applicable state laws, as well as under clearinghouse rules or other agreements. Most legal risks associated with offering RDC services can be mitigated through the use of appropriate contracts and customer agreements. The RDC service agreement should describe the responsibilities and liabilities of the financial institution and its customer, including record retention periods for the original deposited items, physical and logical security measures protecting the RDC scanner, and proper disposal of the original deposited items once the retention period has expired. The agreement also should describe the types of items that can be deposited remotely, individual item dollar limits, overall per-day dollar limits, and minimum image quality standards. The institution should consider requiring a periodic audit of RDC processes at the customer location and, if so, include such terms in the agreement. Banks also should ensure that customer agreements describe the policies and procedures that must be followed at the customer's RDC location, including applicable operational controls to help mitigate possible fraud, such as dual controls and appropriate separation of duties.

Compliance Risks and Controls

Financial institutions must determine whether and to what extent the use of RDC systems increases exposure to the risk of money laundering or other suspicious activities. Institutions should refer to the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual* for a description of their responsibilities.[21] In general, when less personal interaction occurs between a bank and its customers, or a bank's ability to examine financial instruments is limited, the risk of violating laws and regulations in these areas increases.

Financial institutions and their customers are legally obligated to comply with laws and regulations implemented to help prevent and detect money laundering and international terrorist financing. Banks offering RDC services should ensure their own Bank Secrecy Act compliance experts or outside consultants, if used, consider how these laws and regulations may impact RDC and develop policies, procedures, and processes to mitigate this risk. Bank staff responsible for RDC services should receive appropriate training to ensure compliance with bank policies and procedures as well as existing laws and regulations.

Conclusion

Because of the significant business advantages provided through the use of RDC, the number of financial institutions offering RDC services and the number of customers using these services are expected to continue to increase in the near term. However, along with the

[19] Regulation CC governs the availability of funds.

[20] Regulation J governs check collection and funds transfer.

[21] *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual,* pp. 189–190, http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

Ex. 1043-005

Remote Deposit Capture

continued from pg. 23

advantages comes the responsibility of bank management and examiners to be aware of the risks associated with providing RDC services and how those risks should be mitigated.

The primary risks are operational, specifically the risk of fraud, and these risks can be mitigated by using effective risk management techniques, such as those outlined in the FFIEC guidance. These techniques are not costly or complex, and they can easily be implemented by both large and small banks. All risk management strategies described in this article should be considered; however, customer screening is the first step financial institutions should take when deciding to provide RDC services to a particular customer.

Future Prospects

When considering what lies ahead for the use of RDC technology in the longer term, institutions should note that the number of checks being written in this country has declined steadily since 1995. Conversely, the number of electronic payments has grown, and as of 2003, exceeded the number of checks for the first time. These statistics suggest that RDC may be a "gap" technology that perhaps will exist only for the next five to ten years.

In the very near future, financial institutions may apply RDC technology in other ways to reduce deposit-processing costs and expand their deposit base. The first way is making RDC available to retail customers in their homes. Consumers would not need to visit a branch or ATM to deposit checks, but rather would simply run the check through a scanner connected to a personal computer with Internet access.[22]

The second is offering RDC to mobile professionals who travel to client sites and are paid in person by check. The technology exists to enable these individuals to deposit checks at a client's location or in their car using a cell phone camera.[23] Although neither of these applications is now in widespread use, both suggest intriguing opportunities for the future of RDC for banks and customers alike.

Jeffrey Kopchik
Senior Policy Analyst
Division of Supervision and Consumer Protection
jkopchik@fdic.gov

[22] CheckFree, Remote Deposit Capture for Consumers, http://www.checkfreesoftware.com/cda/software/L5.jsp?layoutId=51629&contentId=51624&menuId=51633&pId=60524. (Note: CheckFree is now Fiserv.)

[23] J&B Software, Using Your Mobile Phone for Remote Capture.

Ex. 1043-006