Bank		**Date of Exam**	
Charter		**Prepared By**	

#15 - REMOTE DEPOSIT CAPTURE WORKPROGRAM

OVERVIEW

Remote Deposit Capture (RDC), a deposit transaction delivery system, allows a financial institution to receive digital information from deposit documents captured at remote locations. These locations may be the financial institution's branches, ATMs, domestic and foreign correspondents, or locations owned or controlled by commercial or retail customers of the financial institution. In practice, the vast majority of banks are only offering the RDC application to commercial customers. In substance, RDC is similar to traditional deposit delivery systems at financial institutions; however, it enables customers of financial institutions to deposit items electronically from remote locations. Generally, branch capture of deposits presents less risk, because internal controls have already been put in place. As a result, these procedures addresses the necessary elements of an RDC risk management process in an electronic environment, focusing on RDC deployed at a customer location.

Smaller financial institutions usually have outsourced the RDC function to vendor, where larger institutions will sometimes have this application in-house. Appropriate vendor management practices should include adequate review of the RDC vendor. RDC allows financial institution customers to deposit items electronically from remote locations. The primary RDC delivery method is the Internet, whether to the bank or the vendor. The RDC product is similar to Internet banking. The customer uses the Internet to sign on and then scans the deposit items. If the deposit balances then it is transmitted to the institution/vendor for processing. If the deposit does not balance then either the customer or the vendor will make corrections, prior to processing.

The FFIEC has issued guidance for examiners in FIL -4-2009 (for non-member banks) and SR 09-2 (for member banks). Additional guidance can be found in the FFIEC issued IT booklets and Safeguarding of Customer Information guidelines.

CORE ANALYSIS

1. General Service Delivery Environment

1a. Determine whether deficiencies noted in the last examination and most recent internal/external audit have been addressed and/or corrected by management. Does Internal Audit review RDC activities and compliance with the RDC policy/procedures? Detail how deficiencies were corrected. *Include copy of exam and/or audit exceptions and management response, if applicable.*

Comment:

1b. Identify the parties involved, their responsibilities and their experience/training in the Remote Deposit Capture (RDC) function**.**

Comment:

2. Risk Management: Program Management, Oversight and Monitoring

Refer to Appendix for Additional Guidance

2a. Verify if management has completed a risk assessment related to remote deposit capture. *Comment on any deficiencies noted.*

Comment:

2b. Determine if management has policies and procedures for RDC and if they have been reviewed by the Board. *Provide date reviewed by Board. Comment on any deficiencies.*

Comment:

2c. Determine if management's business continuity plan has been updated to address RDC. *Comment on any deficiencies.*

Comment:

2d. Describe management's efforts to monitor for fraud or otherwise attempt to mitigate risks.

a. Does management have a contract or agreement between the bank and the merchant client? (refer to the appendix for additional information)

b. Does management include physical check retention timeframes in the contract and is the RDC client complying with the contract stipulation? Does management include appropriate check destruction practices in the contract and is the RDC client complying with them**?**

Comment:

2e. If bank personnel perform any data entry functions (e.g. adjusting dollar amounts), determine if there is an independent review or reconciliation.

Comment:

3. RDC Customer

Refer to Appendix for Additional Guidance

3a. Describe management's customer due diligence process for RDC.

a. Does management review and rate potential candidates for the RDC delivery system?

b. Has the institution evaluated the RDC customer's information security infrastructure, including logical and physical security controls?

c. Is there ongoing or periodic monitoring of the RDC customer (financial and information security infrastructure)? (Explain what management is doing.)

Comment on management's customer due diligence process and ongoing monitoring.

Comment:

3b. Determine whether the FI provides training to the merchant/consumer clients to ensure they are appropriately educated on the use and risks of the system. *Comment on training provided.*

Comment:

3c. Determine if any data is stored locally on the RDC client PCs. If yes, is that data encrypted? This includes cache RAM and other storage devices.

Comment:

4. Final Analysis

4a. Complete the **Summary of Findings** page.

SUMMARY OF FINDINGS

#15- REMOTE DEPOSIT CAPTURE

Describe all strengths evident from the evaluation.

Describe all weaknesses evident from evaluation, including violations of law/regulation/rules; noncompliance with Departmental policies/guidelines; internal policy deficiencies/ noncompliance; internal control weaknesses; MIS problems; and deficiencies in management supervision.

Report Worthy:

Not Report Worthy:

Determine why weaknesses exist and comment on management's response and plan of action. Identify bank personnel making the response.

SUMMARY RISK RATING ASSIGNED:

Definitions:

1-Strong; 2-Satisfactory; 3-Less than satisfactory; 4-Deficient; 5-Critically deficient; NR-Not Rated

(Return to Core Analysis)

Provide copy of this page to EIC/AEIC. Receipt and review of this form by the EIC/AEIC will be evidenced by his/her initials in the appropriate column for this procedure on the SCOPE AND WAIVER FORM (Planning and Control Worksheet #1).

APPENDIX

2. RISK MANAGEMENT: PROGRAM MANAGEMENT, OVERSIGHT & MONITORING

- **Risk Assessment:** Development of the risk assessment will assist bank management to identify possible risks related to RDC and to establish controls that mitigate those risks. The risk assessment should be reviewed and approved by the Board annually. The risk assessment should encompass factors such as:
  - Scope of product
  - Type of customer
  - Financial institution position in payment process (BOFD vs. non-BOFD)
  - Anticipated volume of RDC transaction
  - Customer role/responsibility in RDC process
  - Customer ability to download/retain NPI (non-public information)
  - FI-approved vendors and equipment
  - System: image-only or can customer create ACH

- **Policies and Procedures:** Policies and procedures define the function, responsibilities, and controls of RDC. ***Do they define the function, responsibilities, operational controls, vendor management, customer due diligence, and reporting functions, etc.?***

- **Fraud:** Management should be aware that RDC presents new fraud exposures that must be controlled.
  - **Fraud Mitgation- (e.g. duplicate check detection, establishing deposit limits, safeguarding checks, etc.)** Without monitoring mechanisms, it could take days or weeks to determine that fraudulent activity occurred.
  - **Check Retention**- Several TSPs offer duplicate check detection and retain check images for up to 180 days. This should provide an adequate window of review to minimize the risk of an RDC client attempting to redeposit checks.

(Return to Core Analysis)

3. RDC CUSTOMER

- **Due Diligence:** Given the customer's involvement in the check processing, client due diligence will ensure appropriate clients and potentially minimize fraud. If the FI does not pre-qualify and "know" their customers, they will not know the risks associated with providing them this system.
  - How does the FI risk rate existing customers?
  - How does the FI qualify potential customers?
  - Does the FI review: customer application, financial analysis, years in business (for commercial customers), loan/deposit history, credit score, business

practices, sufficiency of staff, compliance with PCI standards?
    - For companies, does the FI review Dun & Bradstreet or other publicly available reports?
    - Does the FI review Visa/Mastercard terminated merchant file or ChexSystems report?
    - Does the FI have procedures that address the performance of CIP (customer identification program) as explained in the BSA manual?

- **Access Controls:** (Physical/Logical) Clients are responsible for non-public information (NPI) whether in transmission or at rest.
    - Physical Security- **(e.g. secure building - locks, alarm system, secure storage of checks - safe, shredder for check destruction)**
    - Logical Security- **(e.g. encrypted data transmission, multi-factor authentication, access level controls, password security parameters, virus protection, etc.)**

- **Contracts & Agreements:** Contracts define each party's responsibility in the event of a dispute. FI management must ensure that they use the contract/agreement to appropriately transfer liability to the merchant / consumer. Consider the following when reviewing the customer contract:
    - Funds availability and reject/return guidelines
    - Liability transference
    - Warranty and indemnification provisions
    - System maintenance and administration guidelines (change control & logical access admin)
    - Dispute resolution/contract termination provisions
    - Information security guidelines and procedures
    - FI's right to audit provision, request self-assessment
    - Security incident reporting
    - Customer service support
    - Responsibility for network connectivity
    - Establish controls such as deposit limits, overdraft limits, and payment on uncollected funds
    - Physical check retention timeframes and secure storage at RDC client
    - BCP/DR provision (advise customer of responsibility to plan for service interruptions)
    - Scalability
    - Limiting item capture to one account
    - Retention timeframes of check images (at the FI or the TSP)

- **Audit/Monitoring**: Prudent practices dictate that FI management have some method of review to ensure their RDC clients are adhering to contract stipulations.
    - Does the FI perform any on-site reviews at the merchants?
    - Does the FI review self-assessments from the RDC merchants/consumers?
    - Do they receive/review penetration tests, audit reports, vulnerability assessments, etc.?

- **Training:** Training will reduce errors, reduce customer calls, and increase efficiency. The training should include:
  - demonstrating the application and scanner,
  - how the scanner works and problems with it (e.g. bad MICR, rejects),
  - manual data entry, and
  - forced balancing, etc.

(Return to Core Analysis)