



## **Highlights of FFIEC Guidance Risk Management of Remote Data Capture January 14, 2009**

The Federal Financial Institutions Examination Council (FFIEC) has issued guidance, *Risk Management of Remote Deposit Capture* (the Guidance), for examiners, financial institutions, and technology service providers regarding remote deposit capture (RDC) systems. The Guidance focuses on three basic principles of RDC risk management -- assessment, mitigation, and identification.

The Guidance is also applicable to other forms of electronic deposit delivery such as mobile banking and check conversion as well as a banks' internal deployments.

### **RDC Risk Assessment**

The Guidance states that while deposit taking is a traditional role for financial institutions, RDC is a new delivery system, rather than just a new service. Prior to implementation, senior management should assess the following risks and incorporate RDC assessment into existing risk assessment processes:

- *Legal and Compliance Risks* - The assessment should identify compliance exposure related to RDC, including risks related to Check 21, Regulation CC, Regulation J, and applicable state laws or clearinghouse agreements. RDC systems employing "least cost routing" using check collection or the ACH should understand the separate rule and liabilities. Care should be taken to evaluate the risks and regulatory requirements under the Bank Secrecy Act as well as the ability to comply with anti-money laundering laws and suspicious activity monitoring.
- *Operational Risks* - The assessment should evaluate the confidentiality, integrity and availability of data afforded by the IT systems of financial institutions, service providers, and RDC customers. Operational risks at the customer level can be unique to each location. The assessment should carefully consider the authentication method appropriate for RDC customers. Certain aspects of fraud risks are elevated with RDC, such as check altering and duplicate presentment. Therefore, RDC customers should institute appropriate document management procedures to ensure the ongoing safety and integrity of deposited items.

### **RDC Risk Mitigation and Controls**

The Guidance states that financial institutions should develop risk management policies that establish risk tolerance levels, internal procedures and controls, risk transfer mechanisms and well-designed contracts.

- *Customer Due Diligence and Suitability* - Management should establish appropriate risk-based guidelines to qualify customers for RDC. Information gathered while conducting customer identification and customer due diligence procedures in fulfillment of the institution's BSA/AML program can support the assessment of customer suitability. A suitability review should involve consideration of the customer's business activities and risk management processes, geographic location, and customer base. The depth of such review should be commensurate with the level of risk.
- *Vendor Due Diligence and Suitability* - Financial institutions that rely on service providers for RDC activities should ensure implementation of sound vendor management processes.
- *RDC Training for Customers* - Management should ensure that customers receive sufficient training, whether the customer obtains the RDC system from the financial institution or from a third-party service provider. Sound training should include documentation that addresses routine operations and procedures, including those related to the risk of duplicate presentment and problem resolution.
- *Contracts and Agreements* - Strong, well-constructed contracts and customer agreements are critical in mitigating the financial institution's risks. Specific contract provisions should address:
  - Roles/responsibilities (including leasing of equipment)
  - Record retention and storage
  - Types of items that may be transmitted
  - Mandatory processes and procedures
  - Image quality; periodic audits
  - Performance standards
  - Allocation of liability warranties
  - Indemnification and dispute resolution
  - Funds availability
  - Collateral and collected funds requirements
  - Governing laws/rules/regulations
  - Mandatory internal controls
  - Right of financial institution to terminate the RDC relationship
- *Business Continuity* - Management should ensure the financial institution's ability to recover and resume RDC operations to meet customer service requirements when an unexpected disruption occurs. The financial institution's business continuity plan testing activities should assess whether restoration of systems and processes meets recovery objectives and time frames.
- *Other Considerations* - Management should implement, as appropriate, other controls that mitigate the operational risks of RDC, including those related to item processing.

## **RDC Risk Measurement and Monitoring**

According to the Guidance, financial institutions should develop and implement risk measuring and monitoring systems for effective oversight of RDC activities. Management should establish key operational performance metrics that support accurate and timely monitoring of risk within

RDC processes and should be used to set operational benchmarks and standards, as well as, to develop reports for monitoring results against the standards.

A variety of reports can facilitate management oversight of RDC operations.

1. Reports on duplicate entries (file and/or item recognition and interception) and violations of deposit thresholds.
2. Velocity metrics such as file size and number of files, transaction dollar value and volume, and return item dollar value and volume.
3. Reports on reject items and corrections, and CAR/LAR/ICR15 adjustments.