

FINDINGS REPORT

NOTE: The FFIEC's Risk Management of Remote Deposit Capture Guidance dated January 14, 2009 and the FFIEC's BSA/AML Examination Manual (Electronic Banking) dated August 24, 2007 were used to conduct this audit.

Introduction:

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 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. RDC can decrease processing costs, support new and existing banking products, and improve customers' access to their deposits; however, it introduces additional risks to those typically inherent in traditional deposit delivery systems.

This FFIEC's Guidance addresses the necessary elements of an RDC risk management process in an electronic environment, focusing on RDC deployed at a customer location. The general principles of RDC risk management are also applicable to financial institutions' internal deployment and other forms of electronic deposit delivery systems (e.g., branch capture, mobile banking and automated clearing house [ACH] check conversions).

Risks associated with this service include the following:

- Legal Risk
- Compliance Risk
- Operational Risk
- Transaction Risk
- Reputation Risk

Objectives:

- Evaluate the effectiveness of the financial institution and service provider's RDC system internal controls and risk management processes that may be relied upon for the purpose of identifying and managing risks.
- Validate as warranted by the risks the effectiveness of the financial institution's and service provider's RDC system function.
- Assess the adequacy of the financial institution's systems to manage Bank Secrecy Act (BSA) Anti-Money Laundering risks associated with RDC activity and Management's ability to implement effective monitoring and reporting systems.

Audit Procedures:

- Confirm Senior Management has identified and assessed the legal, compliance, reputation, and operational risks associated with the RDC system.
- Verify the RDC Policy establishes the Board's risk tolerance levels, provides guidance for risk mitigating internal procedures and controls, identifies risk transfer mechanisms where appropriate and available, and provides guidance for well-designed contracts.

- Ensure when the level of risk warrants, Bank staff include visits to the customer's physical location - evaluates management, operational controls, risk management practices, staffing, and the need for training and support.
- Review Management's selection and oversight of the RDC service provider to ensure a sound vendor management process.
- Review the manner in which the Bank controls the RDC systems, original deposit items at customer locations, electronic files, and retention of nonpublic information.
- Ensure Management considers confidentiality, integrity, and availability of data from systems used by its service providers and RDC customers.
- Review the manner in which Management addresses:
 - controls at the customer location to prevent intentional or unintentional alteration of deposit item information
 - separation of duties at a customer location to limit an individual end-to-end access to the RDC process and the ability to alter logical and physical information without detection.
 - a customer cannot modify RDC-associated software
 - a customer cannot fail to update or patch an associated system in a timely manner
 - multi-factor authentication
 - detection of check alteration, including MICR received through RDC for deposited items; forged or missing endorsements in the RDC environment; and counterfeit items
 - risk of items being processed more than once, deposit items can be endorsed, franked, or otherwise notified as already processed
 - sufficient training for customers using the RDC system.
- Confirm contracts and customer agreements are well constructed to mitigate risk associated with the RDC environment.
- Verify the Bank has a monitoring process in place to ensure customers have implemented operation and risk processes appropriate to RDC technology.
- Confirm Management has ensured the bank's ability to recover and resume RDC operations to meet customer service requirements when an unexpected disruption occurs.
- Verify when appropriate, insurance coverage is considered with RDC operations.

BSA/AML

- Review the policies, procedures, and processes related to RDC activity. Evaluate the adequacy of the policies, procedures, and processes given the Bank's RDC activities and the risks they present. Assess whether the controls are adequate to reasonably protect the Bank from money laundering and terrorist financing.
- From a review of management information systems (MIS) and internal risk rating factors, determine whether the Bank effectively identifies and monitors high-risk RDC activities.
- Determine whether the Bank's system for monitoring RDC activity for suspicious activities, and for reporting suspicious activities, is adequate given the Bank's size, complexity, location, and types of customer relationships.
- Review procedures related to RDC activity for compliance with the Office of Foreign Assets Control (OFAC).

BSA/AML Transaction Testing

- On the basis of the Bank's risk assessment of its RDC activities, as well as prior audit reports, select a sample of RDC accounts. From the sample selected, perform the following procedures:
 - Review account opening documentation, including Customer Identification Program (CIP) and transaction history.
 - Compare expected activity with actual activity.
 - Determine whether the activity is consistent with the nature of the customer's business.
 - Identify any unusual or suspicious activity.
- On the basis of audit procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with RDC relationships to maintain BSA/AML compliance.

Findings:**Recommendations:****Conclusion:**

Overall compliance with bank procedures and policies, internal controls and applicable laws and regulations appears to be **SATISFACTORY OR UNSATISFACTORY**. Overall, the delivery of Remote Deposit Capture products are executed APPROPRIATELY OR INAPPROPRIATELY and SUFFICIENT OR INSUFFICIENT to support the Bank's current customer-base, size, complexity, and risk profile. Individual findings are considered RISK LEVEL. Due to regulatory requirements and additional risks, Remote Deposit Capture has an automatic **High** inherent risk while the internal defined risk rating is currently a RISK RATING.

Management Response:

REQUIRED OR NOT REQUIRED