Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-4-2009
January 14, 2009

RISK MANAGEMENT OF REMOTE DEPOSIT CAPTURE

Summary: The Federal Financial Institutions Examination Council has issued the attached guidance, "Risk Management of Remote Deposit Capture," to assist financial institutions in identifying risks in their remote deposit capture (RDC) systems and evaluating the adequacy of controls and applicable risk management practices. The guidance addresses the necessary elements of an RDC risk management process − risk identification, assessment, and mitigation − and the measurement and monitoring of residual risk exposure. The guidance also discusses the responsibilities of the board of directors and senior management in overseeing the development, implementation, and ongoing operation of RDC.

Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Officer
Chief Treasury Officer
Chief Compliance Officer
Chief Audit Officer

Related Topics:
- FFIEC Information Technology Handbook Booklets:
  . E-Banking
  . Information Security
  . Management
  . Operations; and
  . Retail Payment Systems
- FIL-116-2004, "Check Clearing for the 21st Century Act, Final Amendments to the Federal Reserve Board's Regulation CC," issued October 27, 2004

Attachment:
FFIEC Guidance: Risk Management of Remote Deposit Capture

Contacts:
Arleatha Kelly, Senior Technology Specialist, at arkelly@fdic.gov or (202) 898-3985; or Richard Schwartz, Counsel, at rischwartz@fdic.gov or (202) 898-7424

Note:
To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2008/index.html.

Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Highlights:

- Remote deposit capture, a deposit transaction delivery system, allows financial institution customers to deposit items electronically from remote locations. The primary RDC delivery method is the Internet.
- A financial institution offering RDC should have in place sound risk management and mitigation systems and require adequate risk management at customer locations including, but not limited to, controls over retained nonpublic personal information.
- Financial institutions whose RDC systems use the Internet as a communication channel should use effective methods to authenticate the identity of customers using those services. Single-factor authentication methods may not provide sufficient protection for Internet-based financial services.
- Customer awareness of RDC systems and education about associated RDC risks are effective deterrents to the online theft of assets and sensitive information.

Risk Management of Remote Deposit Capture

Background and Purpose

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 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 discussed here are also applicable to financial institutions' internal deployment and other forms of electronic deposit delivery systems (e.g., mobile banking and automated clearing house [ACH] check conversions).

Risk Management: Risk Assessment

Although deposit taking is not a new activity, RDC should be viewed as a new delivery system and not simply as a new service. Prior to implementing RDC, senior management should identify and assess the legal, compliance, reputation, and operational risks associated with the new system. They should ensure that RDC is compatible with the institution's business strategies and understand the return on investment and management's ability to manage the risks inherent in RDC. Management should incorporate their assessments of RDC systems, including products and services, into existing risk assessment processes. The Management Booklet of the *FFIEC*[1] *IT Examination Handbook* and the *FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual* provide high-level descriptions of risk management processes that include planning, risk identification and assessment, controls, and measuring and monitoring.[2]

The size and complexity of the financial institution, as well as the relative scale and impact of RDC to overall activities, should determine the appropriate level at which

---

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, and a representative of the State Liaison Committee.

[2] See the Audit, Management, Business Continuity Planning, and Information Security Booklets of the *FFIEC IT Examination Handbook*. All booklets that compose the handbook are available at http://www.ffiec.gov/ffiecinfobase/index.html. Also refer to the Risk Assessment section in the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual* at http://www.ffiec.gov/bsa_aml_infobase/default.htm.

governance, oversight, and risk management of RDC should occur. Accordingly, the board or management should approve plans, policies, and significant expenditures, and should review periodic performance and risk management reports on the implementation and ongoing operation of RDC systems and services.

A financial institution's RDC risk assessment should include a determination of the risks to the security and confidentiality of nonpublic personal information[3] consistent with the *Interagency Guidelines Establishing Information Security Standards* (Guidelines).[4] Under these Guidelines, financial institutions must adjust their information security programs in light of any relevant changes in technology, the sensitivity of customer information, internal or external threats to information, and their own changing business arrangements. Therefore, as an institution implements RDC systems, it must consider information security risks associated with RDC technology and operations.

The complexity of the risk identification and assessment process will vary depending on the scope of RDC implementation and exposures faced by the institution. In general, implementing RDC in the institution's backroom operations may present less risk and complexity than deploying RDC at remote locations, such as customers' business premises or homes, where the capture process is outside the direct control of the institution. Risks may differ if the institution uses image exchange for a portion of the process or elects to use the ACH network throughout. Therefore, depending on how RDC is implemented, the financial institution's risk assessment should include its own IT systems as well as those of its third-party service providers and RDC customers.

Financial institutions should approach their risk management responsibilities by involving all potential stakeholders in RDC. Depending on the size and complexity of the institution, stakeholders could include staff from information technology, deposit operations, treasury or cash management sales, business continuity, information security, audit, compliance (including BSA/AML), management, accounting, and legal. Some financial institutions may involve third parties in the risk assessment, implementation, or ongoing operations to provide additional expertise. Regardless of the parties involved, the board and senior management are ultimately responsible for safe and sound operations, including RDC products and services.

---

[3] See FRS: 12 CFR 216.3(n); FDIC: 12 CFR 332.3(n); NCUA: 12 CFR 716.3(q); OCC: 12 CFR 40.3(n); OTS: 12 CFR 573.3(n).

[4] See FRS: 12 CFR 208, Appendix D-2 and 12 CFR 225, Appendix F; FDIC: 12 CFR 364, Appendix B; NCUA: 12 CFR 748, Appendix A; OCC: 12 CFR 30, Appendix B; OTS: 12 CFR 570, Appendix B.

Legal and Compliance Risks

Senior management should identify and assess exposure to legal and compliance risks related to RDC. For example, if a financial institution accepts a deposit of check images from a customer through the RDC system, legal risk exposures may be related to the controls over the process used for image capture or image exchange and the institution's arrangements and contracts for clearing and settling checks. When a financial institution sends the deposited items, in either electronic or paper form, to another institution for collection or presentment, it should consider the risks it takes under the Check Clearing for the 21st Century Act (Check 21 Act),[5] Regulation CC, Regulation J, applicable state laws, or any agreements or clearinghouse rules.[6]

Some RDC systems employ "least cost routing," which allows items to be transmitted and settled either through the check collection system or as an ACH transaction. Financial institutions should understand the separate rules[7] and liabilities and consider them in the risk assessment.

For each clearing method, the financial institution should consider applicable legal and regulatory requirements, such as timing and amount of funds availability, as well as the timeframes for handling returned items. The institution should assess its agreements to verify that liability is allocated appropriately and that other matters, such as methods for resolving disputes and choice of legal jurisdiction, are addressed adequately. (See further discussion under *Contracts and Agreements*.)

The financial institution should evaluate potential risks and regulatory requirements under Bank Secrecy Act laws and regulations when designing and implementing RDC. The institution should consider whether and to what extent it could be exposed to the risk of money laundering activities as well as its ability to comply with anti-money laundering laws and regulations and suspicious activity monitoring.[8] In particular, the growing use of RDC by foreign correspondent financial institutions and foreign money services businesses to replace pouch and certain instrument processing and clearing activities

---

[5] Refer to the FFIEC Check 21 InfoBase for additional discussion of the Check 21 Act and the responsibilities associated with substitute checks at http://www.ffiec.gov/exam/check21.

[6] When a financial institution sends a check for collection or presentment, it makes warranties and takes on liabilities with respect to that check under Regulation CC, state law (the Uniform Commercial Code), and, if it sends the check to a Federal Reserve Bank, Regulation J. In addition, the financial institution may take on other responsibilities with respect to the check as agreed to between the participating institutions by contract or clearinghouse rules. The financial institution should consider applicable Federal Reserve Operating Circulars and governing agreements of relevant third parties involved in their check processing operations (e.g., Electronic Check Clearinghouse Organization [ECCHO]).

[7] See the rules of the National Automated Clearing House Association (NACHA) and Regulation E, 12 CFR 205.

[8] Laws and regulations related to anti-money laundering include the Bank Secrecy Act (BSA), the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), and Office of Foreign Assets Control (OFAC) requirements.

raises money laundering risks the institution should understand and mitigate. Additional due diligence may be necessary where there is evidence that the RDC capture device is in a foreign location, or when a customer has been otherwise identified as being high risk.[9]

Operational Risks

Senior management should understand operational risks and ensure that appropriate policies, procedures, and other controls are in place to mitigate them, including physical and logical access controls over RDC systems, original deposit items at customer locations, electronic files, and retained nonpublic personal information. Management should assess carefully how RDC affects existing risks and mitigating controls. For example, for the various technological options, management should assess the risks associated with how and where nonpublic personal information is captured, transmitted, retained, and destroyed. Management should consider the confidentiality, integrity, and availability of data afforded by its IT systems and by the systems used by its service providers and RDC customers.

RDC processes at a customer location expose the financial institution to operational risks from the point of initial capture. These risks can be unique to each customer's location, RDC processing technology, and information security systems. Faulty equipment, inadequate procedures, or inadequate training of customers and their employees can lead to inappropriate document processing, poor image quality, and inaccurate electronic data. Ineffective controls at the customer location may lead to the intentional or unintentional alteration of deposit item information, resubmission of an electronic file, or re-deposit of physical items. Inadequate separation of duties at a customer location can afford an individual end-to-end access to the RDC process and the ability to alter logical and physical information without detection. In the typical RDC process, original deposit items are not submitted to the financial institution but are retained by the customer or the customer's service provider. Therefore, it is important for the financial institution to require customers to implement appropriate document management procedures to ensure the safety and integrity of deposited items from the time of receipt until the time of destruction or other voiding.

Depending on the type of RDC system implemented, information security risks may extend to the financial institution's own internal networks and networks of its service providers. These technology-related operational risks include failure to maintain compatible and integrated IT systems between the financial institution, service providers, and the customer. For example, a customer or service provider may modify RDC-associated software or hardware or fail to update or patch an associated operating system in a timely manner. There also may be risks related to Web application vulnerabilities, authentication of a customer to the RDC system, and encryption used at any point in the process. The Information Security Booklet of the *FFIEC IT Examination Handbook* provides further guidance in these areas.

---

[9] See USA PATRIOT Act §312, 31 CFR 103.176.

A financial institution should consider carefully the authentication method appropriate for RDC customers. As stated in the *Interagency Guidance on Authentication in an Internet Banking Environment,*[10] the FFIEC agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. The agencies consider transfer of deposit transaction information to represent "the movement of funds to other parties." Thus, for those RDC systems using the Internet as a communication medium, management should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate risks.

Risks associated with fraud are not unique to RDC; however, certain aspects of fraud risk are elevated in an RDC environment. Check alteration, including making unwarranted changes to the Magnetic Ink Character Recognition (MICR) line on the image of scanned items, may be more difficult to detect when deposited items are received through RDC and are not inspected by a qualified person. Similarly, forged or missing endorsements, which may be detected in person, may be less easily detected in an RDC environment. Certain check security features may be lost or the physical alteration of a deposited check – such as by "washing" or other alteration techniques – may be obscured in imaging or electronic conversion processes. Counterfeit items may be similarly difficult to detect. Duplicate presentment of checks and images at the institution or another depository institution represents both a business process and a fraud risk. The potential for insider fraud may be greater with RDC because the financial institution typically does not perform background checks on its customers' employees who may have access to physical deposit items or electronic files. Access by customers and their staffs to nonpublic personal information contained on, or represented by, deposit items may also increase the risk of identity theft.

Risk Management: Mitigation and Controls

If a comprehensive risk assessment supports a management conclusion that the risks associated with RDC can be effectively mitigated, measured, and monitored, management should implement appropriate risk management policies. These policies should establish risk tolerance levels, internal procedures and controls, risk transfer mechanisms where appropriate and available, and well-designed contracts that meet the institution's risk management needs.

Customer Due Diligence and Suitability

A financial institution may determine that risks associated with RDC warrant greater customer selectivity than the risks associated with traditional deposit services and may choose to reduce and control those risks by limiting the availability of this system. Management should establish appropriate risk-based guidelines to qualify customers for this service. In general, information gathered while conducting customer identification and customer due diligence procedures in fulfillment of the institution's BSA/AML

[10] See FRS: SR 05-19; FDIC: FIL 103-2005; NCUA: LTCU 05-CU-18; OCC: Bulletin 2006-35; OTS: CEO Memo 228.

program can support the assessment of customer suitability. Foreign correspondent accounts are subject to due diligence requirements prescribed in regulations issued pursuant to the USA PATRIOT Act amendments to the BSA.[11]

For new and existing customers, a suitability review should involve consideration of the customer's business activities and risk management processes, geographic location, and customer base.[12] The depth of such review should be commensurate with the level of risk.[13] When the level of risk warrants, financial institution staff should include visits to the customer's physical location as part of the suitability review. During these visits, the institution should evaluate management, operational controls and risk management practices, staffing and the need for training and ongoing support, and the IT infrastructure. In addition, the financial institution should review available reports of independent audits performed at the customer location related to IT, RDC, and associated operational processes. When appropriate, based on risk, financial institutions may choose to rely on self-assessments by their RDC customers when these address the controls and risk management practices that would otherwise be reviewed during on-site visits by financial institution staff.

Vendor Due Diligence and Suitability

Financial institutions' interest in RDC has led to a proliferation of RDC technology service providers and RDC hardware and software suppliers. Financial institutions that rely on service providers for RDC activities should ensure implementation of sound vendor management processes as described in the Outsourcing Technology Services Booklet of the *FFIEC IT Examination Handbook*.

RDC Training for Customers

Without effective periodic training, RDC customers may have unrealistic expectations of the system or may not understand their roles in managing risks and monitoring for

---

[11] RDC risk factors and risk mitigation, as well as sound customer due diligence processes and enhanced due diligence processes for certain foreign correspondent accounts, can also be found at http://www.ffiec.gov/bsa_aml_infobase/default.htm. Sections 312, 313, and 319(b) of the USA PATRIOT Act; 31 CFR 103.175 - 103.177, 103.185. Refer to the Foreign Correspondent Account Recordkeeping and Due Diligence section and the Correspondent Accounts (Foreign) section in the *FFIEC Bank Secrecy Act / Anti-Money Laundering Examination Manual* for specific information. In addition, a foreign correspondent relationship may be subject to special measures imposed by the Secretary of the Treasury under Section 311 of the USA PATRIOT Act. Also refer to the Special Measures section of the BSA/AML Manual and to the specific discussion of RDC risks and risk mitigation therein.

[12] A financial institution may have relationships with multiple third parties that transmit items by RDC on behalf of merchants and other customers. When deposit items are converted into ACH transactions, such external parties are effectively acting as third-party senders as in an ACH transaction. See NACHA publication "Third-Party Senders & the ACH Network: An Implementation Guide."

[13] Higher risk customers may be defined by industry, incidence of fraud, or other criteria. Examples of higher risk parties include online payment processors, certain credit-repair services, certain mail order and telephone order companies, online gambling operations, businesses located offshore, and adult entertainment businesses.

processing errors or unauthorized activity. Management should ensure that customers receive sufficient training, whether the customer obtains the RDC system from the financial institution or from a third-party servicer. 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. The financial institution's legal counsel should help develop contracts and agreements with other financial institutions that accept checks in the form of electronic files, third-party service providers, and customers that participate in the RDC process. Contracts and agreements should be appropriate for the institution's specific RDC environment and should identify clearly each party's roles, responsibilities, and liabilities. RDC agreements should establish the control requirements identified during the risk assessment process and the consequences of noncompliance.

There are many elements that management should consider when developing customer contracts. For example, the contracts should cover risks and responsibilities relative to the physical equipment used by the customer in the RDC process. Specific contract provisions for consideration include:

- Roles and responsibilities of the parties, including those related to the sale or lease of equipment and software needed for RDC at the customer location;
- Handling and record retention procedures for the information in RDC, including physical and logical security expectations for access, transmission, storage, and disposal of deposit items containing nonpublic personal information;
- Types of items that may be transmitted;
- Processes and procedures that the customer must follow, including those related to image quality;
- Imaged documents (or original documents, if available) RDC customers must provide to facilitate investigations related to unusual transactions or poor quality transmissions, or to resolve disputes;
- Periodic audits of the RDC process, including the IT infrastructure;
- Performance standards for the financial institution and the customer;
- Allocation of liability, warranties, indemnification, and dispute resolution;
- Funds availability, collateral, and collected funds requirements;[14]
- Governing laws, regulations, and rules;
- Authority of the financial institution to mandate specific internal controls at the customer's locations, audit customer operations, or request additional customer information; and,
- Authority of the financial institution to terminate the RDC relationship.

[14] The financial institution should consider including in its contracts and agreements provisions establishing cut-off times and specifying how and when the customer will know the institution has accepted the deposit.

Business Continuity

Senior 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 should address RDC systems and business processes, and the testing activities should assess whether restoration of systems and processes meets recovery objectives and time frames. To the extent possible, contingency plan development and testing should be coordinated with customers using RDC. The Business Continuity Planning Booklet of the *FFIEC IT Examination Handbook* provides more guidance on the process.

Other Mitigation and Control Considerations

Management should implement as appropriate other controls that mitigate the operational risks of RDC, including those related to item processing as discussed in the Operations Booklet of the *FFIEC IT Examination Handbook*. These controls should be designed and implemented to ensure the security and integrity of nonpublic personal information throughout the transmission flow and while in storage. Separation of duties or other compensating controls at both the institution and the customer location can mitigate the risk of one person having responsibility for end-to-end RDC processing. Strong change control processes coordinated between the institution and customer can help to ensure synchronized RDC platforms, operating systems and applications, and business processes. To reduce the risk of items being processed more than once, deposit items can be endorsed, franked, or otherwise noted as already processed. When insurance coverage is available and cost effective, institutions may be able to mitigate risk further.

Risk Management: Measuring and Monitoring

Financial institutions should develop and implement risk measuring and monitoring systems for effective oversight of RDC activities. Institutions should ensure that customers using RDC have implemented operational and risk monitoring processes appropriate to their choice of technology. Management should establish key operational performance metrics that support accurate and timely monitoring of risk within RDC processes. This information should be used to set operational benchmarks and standards, as well as to develop reports for monitoring results against the standards. Effective management oversight involves regularly reviewing the reports and periodically conducting reviews and operational risk assessments. This will help ensure that the monitoring and reporting process accurately reflects current policies and procedures and sound practices.

A variety of reports can facilitate management oversight of RDC operations, customer compliance with agreements or contracts, and instances of anomalous or questionable activity. Reports on duplicate entries (file and/or item recognition and interception) and violations of deposit thresholds may help monitor for unauthorized activities. Velocity metrics such as file size and number of files, transaction dollar value and volume, and return item dollar value and volume also assist in monitoring for fraudulent activity and capacity utilization. In addition, reporting on reject items and corrections, and

CAR/LAR/ICR[15] adjustments supports monitoring of operational efficiency. Report content should be structured to meet the needs of the various levels of management. Reports should address point-in-time activities as well as trends for individual customers, groups of customers with similar characteristics, and for the RDC product as a whole.

Conclusion

A financial institution offering RDC should have sound risk management and mitigation systems in place and should require adequate risk management at customer locations. Prior to implementing RDC, and periodically thereafter, management should conduct a risk assessment to identify the related types and levels of risk exposure. Comprehensive contracts and customer agreements should identify clearly the roles, responsibilities, and liabilities of all parties in the RDC process to minimize exposure to legal and compliance risks. Appropriate technology and process controls should be implemented at both the financial institution and the customer locations to address operational risk. Financial institution management and the customer should implement effective risk measurement and monitoring systems. When appropriate and available, insurance coverage should be considered as a risk transfer mechanism. As with other financial services, RDC may not be appropriate for all customers or for all financial institutions.

[15] The CAR (Courtesy Amount Recognition) field contains the amount of the check in numeric form. The LAR (Legal Amount Recognition) field contains the amount of the check in written form. ICR (Intelligent Character Recognition) is the process by which scanning software interprets information on a deposit item and converts it into electronic data.