Electronic Banking — Overview

Objective. *Assess the adequacy of the bank's systems to manage the risks associated with electronic banking (e-banking) customers, including Remote Deposit Capture (RDC) activity, and management's ability to implement effective monitoring and reporting systems.*

E-banking systems, which provide electronic delivery of banking products to customers, include automated teller machine (ATM) transactions; online account opening; Internet banking transactions; and telephone banking. For example, credit cards, deposit accounts, mortgage loans, and funds transfers can all be initiated online, without face-to-face contact. Management needs to recognize this as a potentially higher-risk area and develop adequate policies, procedures, and processes for customer identification and monitoring for specific areas of banking. Refer to the core examination procedures, "Customer Identification Program" (CIP), page 53, for further guidance. Additional information on e-banking is available in the FFIEC *Information Technology Examination Handbook*.[197]

Risk Factors

Banks should ensure that their monitoring systems adequately capture transactions conducted electronically. As with any account, they should be alert to anomalies in account behavior. Red flags may include the velocity of funds in the account or, in the case of ATMs, the number of debit cards associated with the account.

Accounts that are opened without face-to-face contact may be a higher risk for money laundering and terrorist financing for the following reasons:

- More difficult to positively verify the individual's identity.
- Customer may be out of the bank's targeted geographic area or country.
- Customer may perceive the transactions as less transparent.
- Transactions are instantaneous.
- May be used by a "front" company or unknown third party.

Risk Mitigation

Banks should establish BSA/AML monitoring, identification, and reporting for unusual and suspicious activities occurring through e-banking systems. Useful MIS for detecting unusual activity in higher-risk accounts include ATM activity reports, funds transfer reports, new account activity reports, change of Internet address reports, Internet Protocol (IP) address reports, and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses, and taxpayer identification numbers). In determining the level of monitoring required for an account, banks should include how the account was opened as a factor. Banks engaging in transactional Internet banking should have effective and reliable methods to authenticate a customer's identity when opening accounts online and should establish policies for when a customer should be required to open accounts on a face-to-face

[197] Refer to the FFIEC *Information Technology Examination Handbook*.

basis.[198] Banks may also institute other controls, such as establishing transaction dollar limits for large items that require manual intervention to exceed the preset limit.

Remote Deposit Capture

Remote Deposit Capture (RDC) is a deposit transaction delivery system that has made check and monetary instrument processing (e.g., traveler's checks or money orders) more efficient. In broad terms, RDC allows a bank's customers to scan a check or monetary instrument, and then transmit the scanned or digitized image to the institution. Scanning and transmission activities occur at remote locations that include the bank's branches, ATMs, domestic and foreign correspondents, and locations owned or controlled by commercial or retail customers. By eliminating face-to-face transactions, RDC decreases the cost and volume of paper associated with physically mailing or depositing items. RDC also supports new and existing banking products and improves customers' access to their deposits.

On January 14, 2009, the FFIEC published guidance titled, "Risk Management of Remote Deposit Capture." The guidance addresses the essential components of RDC risk management: the identification, assessment, and mitigation of risk. It includes a comprehensive discussion of RDC risk factors and mitigants. Refer to the FFIEC Web site.

Risk Factors

RDC may expose banks to various risks, including money laundering, fraud, and information security. Fraudulent, sequentially numbered, or physically altered documents, particularly money orders and traveler's checks, may be more difficult to detect when submitted by RDC and not inspected by a qualified person. Banks may face challenges in controlling or knowing the location of RDC equipment, because the equipment can be readily transported from one jurisdiction to another. This challenge is increased as foreign correspondents and foreign money services businesses are increasingly using RDC services to replace pouch and certain instrument processing and clearing activities. Inadequate controls could result in intentional or unintentional alterations to deposit item data, resubmission of a data file, or duplicate presentment of checks and images at one or multiple financial institutions. In addition, original deposit items are not typically forwarded to banks, but instead the customer or the customer's service provider retains them. As a result, record keeping, data safety, and integrity issues may increase.

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.

Risk Mitigation

Management should develop appropriate policies, procedures, and processes to mitigate the risks associated with RDC services and to effectively monitor for unusual or suspicious activity. Examples of risk mitigants include:

[198] For additional information, refer to *Authentication in an Internet Banking Environment* issued by the FFIEC, October 13, 2005.

- Comprehensively identifying and assessing RDC risk prior to implementation. Senior management should identify BSA/AML, operational, information security, compliance, legal, and reputation risks. Depending on the bank's size and complexity, this comprehensive risk assessment process should include staff from BSA/AML, information technology and security, deposit operations, treasury or cash management sales, business continuity, audit, compliance, accounting and legal.
- Conducting appropriate customer CDD and EDD.
- Creating risk-based parameters that can be used to conduct RDC customer suitability reviews. Parameters may include a list of acceptable industries, standardized underwriting criteria (e.g., credit history, financial statements, and ownership structure of business), and other risk factors (customer's risk management processes, geographic location, and customer base). When the level of risk warrants, bank staff should consider visiting the customer's physical location as part of the suitability review. During these visits, the customer's operational controls and risk management processes should be evaluated.
- Conducting vendor due diligence when banks use a service provider for RDC activities. Management should ensure implementation of sound vendor management processes.
- Obtaining expected account activity from the RDC customer, such as the anticipated RDC transaction volume, dollar volume, and type (e.g., payroll checks, third-party checks, or traveler's checks), comparing it to actual activity, and resolving significant deviations. Comparing expected activity to business type to ensure they are reasonable and consistent.
- Establishing or modifying customer RDC transaction limits.
- Developing well-constructed contracts that clearly identify each party's role, responsibilities, and liabilities, and that detail record-retention procedures for RDC data. These procedures should include physical and logical security expectations for access, transmission, storage, and ultimate disposal of original documents. The contract should also address the customer's responsibility for properly securing RDC equipment and preventing inappropriate use, including establishing effective equipment security controls (e.g., passwords, dual control access). In addition, contracts should detail the RDC customer's obligation to provide original documents to the bank in order to facilitate investigations related to unusual transactions or poor quality transmissions, or to resolve disputes. Contracts should clearly detail the authority of the bank to mandate specific internal controls, conduct audits, or terminate the RDC relationship.
- Implementing additional monitoring or review when significant changes occur in the type or volume of transactions, or when significant changes occur in the underwriting criteria, customer base, customer risk management processes, or geographic location that the bank relied on when establishing RDC services.
- Ensuring that RDC customers receive adequate training. The training should include documentation that addresses issues such as routine operations and procedures, duplicate presentment, and problem resolution.

- Using improved aggregation and monitoring capabilities as facilitated by the digitized data.
- As appropriate, using technology to minimize errors (e.g., the use of franking to stamp or identify a deposit as being processed).[199]

[199] Franking involves printing or stamping such phrases as "Processed" or "Electronically Processed" on the front of the original check. This process is used as an indicator that the paper check has already been electronically processed, and, therefore, should not be subsequently physically deposited.