APPENDIX A: EXAMINATION PROCEDURES

EXAMINATION OBJECTIVE: Examiners should use the following Tier I and Tier II Retail Payment Systems examination procedures to evaluate the policies and procedures, business processes, personnel, and internal control systems of financial institutions and technology service providers. Retail payment system services include checks and share draft item processing, bankcards, payment cards, ACH, EFT/POS networks, electronic bill payment, person-to-person (P2P) and account-to-account (A2A) payment systems, and many other products and services resulting from emerging advances in technology. The examination scope should be based upon the risk profile of the financial institution or the technology service provider. The risk profile is determined through an assessment of the entity's risk environment and quality of risk management practices. This assessment should consider the formal policies and procedures established to provide these services, as well as the effectiveness of the financial institution's underlying internal control environment, including information security, business continuity, disaster recovery, and vendor management programs.

Retail payment services expose financial institutions to numerous risks, including legal, compliance, strategic, operational, credit and liquidity. Depending on the complexity of retail payment system activity, the scope of the examination may require an integrated team approach that includes the knowledge, skills, and expertise of, IT, credit, and compliance specialists.

The examination procedures may be part of either an IT or safety and soundness examination. Examiners can use the procedures in their entirety or in a modular fashion to focus on particular retail payment system products, services, or business lines. Depending on the size, complexity and risk profile of the financial institution or technology service provider, not all of the procedures may be necessary to develop overall conclusions. The examination of retail payment services may also support the institution's BSA/AML examination, which requires an evaluation of related risks in retail payment services.

The primary objectives of the Tier I procedures are to evaluate the effectiveness of the internal controls and risk management processes implemented by the financial institution or the technology service provider. Examiners should use the Tier II procedures to expand the scope of the examination further if the risk profile or organization's complexity requires additional information to establish comprehensive and accurate examination conclusions.

TIER I OBJECTIVES AND PROCEDURES

Objective 1: Assess the level of risk in retail payment systems function

1. Determine the types of retail payment products and services offered. Consider the following:
   - The types of customers using the products and services
   - The geographic service footprint (e.g., international usage)
   - Check processing, particularly check imaging, remotely created checks (RCCs), and remote deposit capture
   - ACH, including third-party originations, TEL, WEB, ARC, POP, and BOC
   - Card issuance
   - Card processing
   - Merchant acquisition and processing

2. Determine whether new retail payment products and emerging technologies pose increased risk due to the lack of maturity of the respective control environments. Consider:
   - New retail payment products and services that have been introduced within the past year.
   - Whether the institution introduced any existing products into new markets within the past year.

3. Determine if the quality of management and staff, and the staffing levels are adequate for the specific retail payment products and processes the institution provides.
   - Obtain and review the following:
     - Reports showing staffing levels, turnover, and trends.
     - Biographies of managers and key staff.
   - Consider:
     - The levels of skill and experience of key managers and staff, particularly in terms of the sophistication and complexity of the products, processes, and systems.
     - Whether the institution has appropriate depth of management and staff.
     - The adequacy of staffing levels for peak operating periods.
     - Management and staff turnover.
4. Determine if the quality of process design and control points are adequate for existing retail products, and if these factors are considered for new products. Consider whether:

- There is adequate capacity for current and planned transaction volumes.
- Processes are clearly designed.
- Processes are automated.
- There is a reasonable degree of manual intervention.
- Any processes have been re-engineered during the past year.
- Processes are outsourced or performed at the customer location.

5. Evaluate the use of in-house and outsourced data processing systems to support retail payment products and processes. Consider:
   - How stable are existing systems.
   - How current are existing systems.
   - Whether there is adequate capacity for current and planned transaction volumes.
   - Whether the institution uses leading edge technologies or only mature technologies.
   - To what extent are systems outsourced.
   - Whether outsourcing arrangements are governed by contracts and service level agreements.
   - Whether vendors are considered to be industry-recognized leaders.

Objective 2: Establish the scope and objectives of the examination of the retail payment systems function.

1. Review previous reports of examination for comments relating to retail payment systems. Review:
   - Regulatory reports of examination, including consumer and compliance information.
   - Prior examination work papers, including any documentation obtained through on-going supervision.
   - Internal control self-assessments completed by business lines.
   - Internal and external audit reports, including annual attestation letters.
   - Regulatory, audit, and information security reports from service providers.
   - Trade group, bankcard company, interchange, and clearing house documentation relating to services provided by the financial institution, particularly the NACHA required annual security audit and bankcard company self assessments.
   - Supervisory strategy documents, including risk assessments.

2. Review past examination reports for comments relating to the institution's internal control environment and technical infrastructure. Review:

   - The institution's processing architecture, including processing outsourcing arrangements.
   - Internal controls, including physical and logical access controls in the data entry area, data center, and item processing operations.
   - Electronic Funds Transfer (EFT)/Point of Sale (POS) network controls.
   - Comments related to controls over Remote Deposit Capture (RDC).
   - Inventory of computer hardware, software, and telecommunications protocols used to support check item processing, EFT/POS transaction processing, ACH, and bankcard issuance and acquiring transaction services.

3. Review the financial institution's risk and control assessments for comments relating to retail payment systems. Review the following risk assessments:

   - External and internal audit;
   - Management controls;
   - Information security;
   - Business continuity;
   - Regulatory compliance; and
   - BSA/AML.

4. Identify and obtain during discussions with management of financial institution or service provider:

   - A description of the retail payment system activities performed and scope of operations, including check item processing, RDC, lock-box services that provide ACH check conversion or check truncation, ACH, bankcard issuing and acquiring, clearance, settlement, and EFT/POS network activity.
   - Operational reports for retail payment system activities, including transaction volumes, dollar amounts, and trends. Where possible, compare levels and trends with peer financial institutions. Significant increases may indicate a change in risk to the financial institution and management awareness should be evaluated.
   - Organization charts of retail lines of business to determine reporting relationships and how the collective retail lines of business are structured and managed.
   - The retail payment system functions performed through outsourcing relationships and the financial institution's level of reliance on those services.
   - Any significant changes in retail payment system policies, personnel, products, strategy and services since the last examination, particularly the introduction of new and emerging

electronic retail payment systems incorporating RDC, wireless, telephone, web-based purchasing and bill payment, prepaid cards, or P2P and A2A payment systems.

- A listing of all payment processing and clearing house settlement arrangements in which the financial institution participates. Include any bilateral retail payment clearing arrangements the institution may have with other institutions that are outside traditional clearing houses such as FedACH and EPN. Evaluate the methodology used by the financial institution in assessing its operational and settlement risk from these arrangements.
- Documentation of any related operational or credit losses incurred, reasons for the losses, and actions taken by management to prevent future losses for each retail payment system.
- A network diagram of the transaction flow from the merchant end of the network, through any intermediary processors, to the financial institution, for all types of payment channels.

5. Review the financial institution's response to any retail payment systems issues raised at the last examination and any internal audits conducted since last review. Determine:
   - Adequacy and timing of corrective action.
   - Resolution of root causes rather than specific issues.
   - Existence of outstanding issues.

Objective 3: Assess the quality of oversight and support provided by the board of directors and management.

1. Determine the quality and effectiveness of the financial institution's retail payment systems management function. Consider:
   - The alignment of the institution's business plans with its technology and operational plans for retail payment systems.
   - Data center and network management and the quality of internal controls over internal ATM networks and gateway connectivity to regional, national, and international EFT/POS and bankcard networks.
   - Departmental management and the quality of internal controls, including separation of duties and dual control procedures, for bankcard, ATM and debit card, ACH, check items, and electronic banking payment transaction processing, clearance, and settlement activity.
   - Departmental management and the quality of information security and GLBA 501(b) compliance policies relating to retail payment system-generated customer data.

2. Assess management's ability to manage outsourced relationships with technology service providers. Consider:
    - Process utilized to encrypt transactions while in route between technology service providers and the institution.
    - Adequacy of contract provisions including service level, performance agreements, responsibilities, liabilities, and management monitoring.
    - Management's determination of the service provider's compliance with applicable financial institution and consumer regulations and with third-party requirements (e.g., NACHA, GLBA, bankcard company, and interchange).
    - Adequacy of contract provisions for personnel, equipment, and related services.
    - Quality of management information systems (MIS) and reports needed to monitor the technology service provider's performance appropriately.

3. Evaluate the adequacy and effectiveness of financial institution and service provider contingency and business continuity planning. Consider:
    - Ability to recover transaction data and supporting books and records based on retail payment system business line requirements and time lines.
    - Level of testing conducted to ensure adequate preparation.
    - Stand-in arrangements established with other financial institutions in the event of an ATM and/or POS system outage.
    - Alternative access mechanisms in the event of an outage to primary access to bankcard, ACH, and other retail payment networks.

4. Evaluate retail payment system business line staff. Consider:
    - Adequacy and quality of staff resources, including certifications such as an Accredited ACH Professional (AAP).
    - Effectiveness of policies and procedures outlining department duties, including job descriptions.

Objective 4: Assess the quality of policies, procedures, and limits supporting retail payment services.

1. Review policies, procedures, and limits for supporting all retail payment services.
    - Determine if there are written policies.
    - Determine if the policies reflect the current business and processes.
    - Determine if the policies establish reasonable limits.

2. Review staff training programs and determine if they are appropriate for supporting policies.

3. Determine whether the institution monitors compliance with policies, procedures, and limits.
   - Determine if exception monitoring reports are elevated to appropriate levels of management.

Objective 5: Assess the quality of management information systems and reports used to manage retail payment services.

1. Review management reports for all retail payment services including reports from service providers.
   - Determine if the reports are appropriate to the businesses and processes in terms of scope and frequency.
   - Determine if the reports are reviewed at the appropriate levels of management.

Objective 6: Assess the quality of risk management and support for bankcard issuance and acquiring (merchant processing) activity.

1. Evaluate financial institution adherence to bankcard company rules and bylaws and regulatory requirements.

2. Evaluate whether card issuance processing is outsourced to a third party. If yes, evaluate the vendor management controls in place to govern the activities listed in steps 3 and 4.

3. Review internal procedures employed for each bankcard product and assess:
   - The integrity of plastic card and PIN issuance processing.
   - Whether processing includes appropriate separation of functions in card issuance, PIN issuance, control and storage of card stock, and the maintenance of software controlling PIN generation.
   - Whether the institution has established procedures focusing on controls preventing card fraud and abuse.

4. Determine whether the audit function periodically performs an inventory of all bankcards at each location owned or operated by the institution and that each location is included in the audit program, either directly or indirectly (e.g., as part of a branch audit).

5. Determine whether management has established inventory systems that include quality control activities such as self-monitoring for data accuracy.

6. Review a sample of consumer contracts for each bankcard service to ensure they describe adequately the responsibilities and liabilities of the institution and its customers (compliance with Regulation Z).

7. Evaluate the effectiveness of internal clearance and settlement activity as it relates to customer bankcard transactions. Consider the adequacy of:

   - Financial and accounting controls in place to clear and settle transactions.
   - Periodic reconciliation of all account postings.
   - Timely clearance or charge-off of missing items or out-of-balance situations.

8. Evaluate the effectiveness of internal credit monitoring and card authorization performed by the financial institution. Consider the adequacy of:

   - Policies and procedures for underwriting, account management, and collection activities.
   - Card authorization procedures to mitigate fraudulent use.
   - MIS reports and behavioral fraud analysis.

9. For financial institutions directly involved in, or outsource, bankcard acquiring (merchant processing) services, determine the appropriateness of controls over merchant services and ISO/MSP relationships. Consider the adequacy of:

   - New merchant approval and acceptance process, termination procedures, and underwriting guidelines for merchant accounts with particular attention to Web and telephone-based businesses.
   - Testing of web-based business to validate site's content.
   - Industry-standard MIS reports to identify negative trends and potential fraudulent activity. Potential indicators of fraud or money laundering include: a large number of manually keyed transactions, even dollar amount transactions, average sale ticket size as compared to history, same dollar amount repeated frequently in a single batch, or continuous or frequent zero balances in DDA account.
   - The financial institution's use of a front-end fraud detection application either in-house design or purchased.
   - Credit approval and monitoring procedures for all new and established merchant accounts. Consider use of Dun & Bradstreet reports, bank statements and credit reports.
   - Chargeback processing procedures and controls, including trend, volume, age, and losses associated with merchant chargebacks.
   - Agent bank programs (where the financial institution performs merchant processing for other institutions), and the level of liability assumed by the acquiring financial institution.

- Protection and storage of cardholder data and compliance with card company rules and guidelines on what data can and cannot be stored.
- Programs for requiring and monitoring merchant's and processor's compliance with card company and association standards such as PCI Data Security Standards. Review assessment document and process for completion.
- Policies and procedures relating to customer accounts that may have been the subject of security breach at the merchant/ISO location (i.e., reissue cards, monitoring and customer notification).

Objective 7: Assess the quality of risk management and support for EFT/POS processing activity.

1. Evaluate the financial institution's compliance with interchange rules and bylaws.

2. Review internal procedures employed for generating active ATM cards. Consider:
   - The integrity of PIN issuance and processing, including appropriate separation of functions between card issuance, PIN issuance, and card stock control and storage.
   - The maintenance of software controlling PIN generation. The review should focus on controls preventing card fraud and abuse resulting in financial loss to the institution.

3. Determine whether the audit function periodically performs an inventory of unused ATM card stock at each location owned or operated by the institution and that each location is included in the audit program, either directly or indirectly (e.g., as part of a branch audit).

4. Review a sample of consumer contracts for ATM services to ensure they adequately set forth responsibilities and liabilities of the institution and the customer. Evaluate compliance with applicable regulations.

5. Evaluate the effectiveness of internal clearance and settlement activities as it relates to customer ATM transactions. Consider whether:
   - Appropriate financial and accounting controls are in place to clear and settle ATM transactions.
   - Reconciliation is performed periodically for all account postings.
   - Processes have been established for handling disputed items.

Objective 8: Assess the quality of risk management and support for ACH processing activity.

1. Evaluate the financial institution's adherence to NACHA and clearing house operating rules and regulations.

2. Review operational reports showing monthly or quarterly ACH debit and credit activity and, if possible, compare levels with peer financial institutions. If ACH activity is greater than peer, determine whether institution is an originating institution (ODFI). Obtain reports listing those customers for which they originate and the volumes (number of items and dollars) originated. Be sure to ask for all customers that use the ODFI's originating account number with the Federal Reserve or EPN.

3. If the institution has bilateral clearing arrangements with other institutions, review the underlying contracts and determine how the institution monitors compliance with the contracts.

4. If the institution uses a technology service provider, determine whether it performed appropriate due diligence prior to engagement and has appropriate contractual agreements governing the relationship. Determine whether the institution monitors compliance with the governing contract. Determine if the institution has an adequate business continuity plan in the event the technology service provider experiences a service disruption.

5. If the institution is an ODFI and permits third-party sender payments, determine whether it requires the third-party sender to establish the identity of each originator using commercially reasonable methods to warrant that the originators will assume their responsibilities under NACHA rules and to warrant that it will assume the liabilities of the ODFI. Determine whether the ODFI has established limits and monitoring of the third-party sender's creditworthiness relative to its underlying originators and the nature and type of ACH activity that it warrants.

6. Determine whether the ODFI's contractual agreements with each originator clearly define the specific terms for funds availability.

7. Determine whether the institution has taken steps to ensure that originators are properly educated about their obligations for handling ARC and POP source documentation and all other NACHA rules.

8. Review policies and procedures for acquisition of originating customers and determine the appropriateness of these policies for the risk profile and risk management capabilities of the financial institution. Determine whether the policies identify and seek to limit exposure to higher risk customers; such as, adult entertainment and online gambling firms, adult bookstores, escort services, and massage parlors.

9. Review policies and procedures in place to monitor originating customer balances for credit payments (e.g., payroll) to ensure payments are made against collected funds or established credit limits and daily caps. Also determine whether payments in excess of established credit limits and daily caps are properly authorized.

10. Determine whether the institution treats deposits resulting from ACH transmitted debits on other accounts as uncollected funds until there is reasonable assurance the debits have been paid by the institution on which they were drawn. Also, determine whether management monitors drawings against uncollected funds to ensure they are within established guidelines.

11. Review a sample of contracts authorizing the institution to originate ACH items for customers and determine whether they adequately set forth the responsibilities of the institution and customer. Determine:

    - Whether contracted technology service providers originating customer entries are also customers of the financial institution.
    - Whether the agreements include recognition of all relevant NACHA requirements.
    - Whether ACH clearing houses, of which the financial institution is a member, stipulate the funding arrangements (outgoing), Expedited Funds Availability Act (Regulation CC), UCC Article 4A (credit transfer only), and Electronic Funds Transfers (Regulation E).

12. Determine whether the institution has a process in place for monitoring and acting on returned items, that includes third-party vendors, where applicable..

13. Determine whether the institution uses risk management reports that are appropriate to the ACH activities and level of risk.

14. Determine whether ACH activities are considered in the institution's overall business continuity plans and insurance program.

15. Determine whether management monitors originating customers for unreasonable numbers of unauthorized ACH debits. If the volume of unauthorized ACH debits is high, it could expose the institution to greater loss.

16. Determine whether management has addressed international ACH requirements, where applicable.

Objective 9: Assess the quality of risk management and support for electronic banking related retail payment transaction processing.

1. Determine the extent to which the financial institution engages in retail payment systems, including bill payment, prepaid cards, wireless systems, contactless payment devices, remote check capture, lock-box services that provide ACH check conversion or check truncation, and P2P and A2A payments. Consider:

    - Strategic plans relating to the introduction of new retail payment system products and services.

- The development of internal pilot programs and partnerships with technology service providers introducing new retail payment systems and delivery channels.
- The extent to which existing Internet and e-banking products and services include new retail payment mechanisms.

2. Evaluate the financial institution's ability to manage the development and implementation of new retail payment services, focusing on effectiveness of internal controls and provisions of consumer compliance regulations. Consider:
   - Information security, including identification and authentication systems, in the deployment of any smart cards, wireless payment devices, EBPP, P2P and A2A product offerings.
   - Customer disclosure and compliance information for retail payment systems using new technologies.
   - Technical resources to effectively manage retail payment systems including Internet technologies, telecommunications protocols, and operations support.

3. Evaluate the financial institution's ability to incorporate new retail payment product offerings into its existing retail business lines and its effectiveness in including these product offerings in its traditional retail payment operations. Consider:
   - The integration of new retail payment product offerings into existing clearance, settlement, and accounting functions.
   - Whether the financial institution relies on technology service providers for some or all of these services.

Objective 10: Assess the quality of risk management and support for checks.

1. Determine whether the accounting department handles check return item processing appropriately, reconciling all aged items.

2. If the institution offers its customers RDC services, review the appropriateness of:
   - Due diligence procedures for new and existing retail customers.
   - Due diligence procedures for new and existing third-party processing customers (ensure processors perform adequate due diligence over their originating retail customers).
   - Underlying contracts for:
     - Assignment of liability in the event of returned, disputed, or fraudulent items.
     - Limitations or reasonable parameters regarding activity volumes, including returns.

- Ongoing transaction activity monitoring procedures.

3. Determine whether the institution uses electronic check presentment (ECP) for payment. If yes, determine:
   - The effectiveness of the financial institution's ECP implementation, including logical access controls over electronic files storing MICR and related information.
   - Whether the financial institution is using positive pay.
   - Whether the logical access controls over the electronic files sent by commercial businesses are adequately controlled.

Objective 11: Assess the quality of risk - management of new and emerging technology risks

1. Determine the institution's processes for evaluating and deploying new and emerging technologies for retail payment systems. Of particular concern are retail payment products and services that do not use established networks such as ACH, or that extend operational processes to the customer location, as with RDC. Determine:
   - Whether the institution conducts risk assessments prior to deployment of new and emerging technologies.
   - Whether the processes involve the institution's compliance functions, including consumer compliance, BSA/AML, GLBA 501(b), and third party requirements (for example, NACHA, MasterCard, and Visa).
   - Whether risk assessment and compliance status are communicated to senior management and the board of directors.

2. Assess the vendor management program over the technology service providers offering new and emerging technologies for retail payment systems. Determine:
   - The adequacy of due diligence performed on the technology service provider.
   - Whether management regularly reviews the financial status of the technology service provider.
   - Whether management receives independent audits, third-party reviews, or data information security reviews performed on the technology service provider.
   - Whether the information exchanged with the technology service provider is documented and meets the bank's requirements.
   - Whether the dispute resolution process between the technology service provider and customer is documented and meets the bank's requirements.
   - Whether MIS received from the technology service provider is adequate.

CONCLUSIONS

1. Determine the need to conduct Tier II procedures for additional validation to support conclusions related to any of the Tier I objectives.

2. From the procedures performed, including any Tier II procedures performed:
   - Document conclusions related to the quality and effectiveness of the management of the retail payment systems function.
   - Determine and document to what extent, if any, the examiner may rely upon retail payment system procedures performed by internal or external audit.

3. Review your preliminary conclusions with the examiner-in-charge (EIC) regarding:
   - Violations of law, rulings, regulations, and third-party agreements.
   - Significant issues warranting inclusion as matters requiring board attention in the report of examination.
   - Potential impact of your conclusions on the Uniform Rating System for Information Technology (URSIT) composite and component ratings.
   - Where necessary, communicate relevant conclusions to the EIC for the BSA/AML, or retail credit, or compliance examinations.

4. Discuss your findings with management and obtain proposed corrective action, within reasonable timeframes, for significant deficiencies.

5. Document your conclusions in a memo to the EIC providing report-ready comments for all relevant sections of the FFIEC report of examination (ROE) and guidance to future examiners.

6. Organize work papers to ensure clear support for significant findings and conclusions.

TIER II OBJECTIVE AND PROCEDURES

Examination Objective: The Tier II Retail Payment Systems Examination Procedures provide additional validation steps to verify the effectiveness of a financial institution's internal control processes over ACH, EFT/POS network, check item, electronic banking-related retail payments, and bankcard processing, clearance, and settlement. These procedures assist in achieving examination objectives, and examiners may use them in their entirety or selectively, depending upon the scope of the examination and the need for additional verification.

Examiners should coordinate this coverage with other examiners involved in assessing the institution's information systems, operations, information security, business continuity planning, and vendor management effectiveness to avoid duplication of effort and to ensure there is an adequate understanding of the control environment as it pertains to retail payment business lines.

The procedures provided in this section should not be construed as requirements for control implementation. The selection of controls and control implementation should be guided by the risk profile of the institution. Therefore, the controls necessary for any single institution or any given area may differ from those noted in the following procedures.

A. EFT/POS AND BANKCARD AGREEMENTS AND CONTRACTS

1. If the financial institution is a participant in a shared EFT/POS network or if it contracts with third-party bankcard-issuing or -acquiring processing service providers, determine whether:

   - Contracts with regional EFT/POS network switch and gateway operators and bankcard processors clearly set forth the rights and responsibilities of all parties, including the integrity and confidentiality of customer information, ownership of data, settlement terms, contingency and business recovery plans, and requirements for installing and servicing equipment and software.
   - Adequate agreements are in place with all technology service providers supplying services for retail EFT/POS and bankcard operations (plastic cards, ATM equipment and software maintenance, ATM cash replenishment) that clearly define the responsibilities of both the service provider and the institution.
   - Agreements include a provision of minimum acceptable control standards, the ability of the institution to audit the technology service provider's operations, periodic submission of financial statements to the institution, and contingency and business recovery plans.
   - Contracts and agreements clearly define responsibilities and limits of liability for both the customer and financial institution and include provisions of the Electronic Funds Transfer Act (Regulation E) and the Expedited Funds Availability Act (Regulation CC) for deposit activities.

2. Determine whether management periodically reviews individual sites providing retail EFT/POS and bankcard services to ensure policies, procedures, security measures, and equipment maintenance requirements are appropriate.

3. For retail EFT/POS and bankcard transaction processing activities contracted to third-party service providers, assess the adequacy of the review process performed by management regarding annual financial statements, audit reports, and Payment Card Industry (PCI) Data Security Standard assessment.

B. Personal Identification Numbers (PINs)

1. Assess staff access to PIN data. Ensure there is separation of duties between staff responsible for card operations and staff responsible for preparing or issuing bankcards.

2. Assess the adequacy of the PIN generation process. Ensure there is separation of duties between staff responsible for PIN generation and staff responsible for opening accounts or with access to customer account information.

3. For new PIN issuance, assess the adequacy of control procedures including accountability assigned to staff initiating such transactions.

4. Assess the adequacy of PIN generation and issuance procedures to determine whether they preclude matching an assigned PIN to a customer's account number or bankcard.

5. Assess the adequacy of threshold for PIN access attempts to customer account information and funds. The threshold parameter should be set at a reasonable number of unsuccessful attempts.

6. Assess the level of PIN encryption when stored on computer files or transmitted over telecommunication lines.

7. If resets are allowed, assess the adequacy of procedures and controls for PIN/password resets. The use of single-use and temporary PIN/password is preferred.

8. Assess the adequacy of procedures for prohibiting PIN information from being disclosed over the telephone.

9. Assess staff access to PIN-related databases and determine if management restricts access to authorized personnel. Assess database maintenance activities to ensure management closely supervises and logs staff access.

10. Assess the adequacy of customer PIN selection criteria, focusing on whether the institution discourages or prevents customers from using common words, social security numbers, sequences of numbers, or words or numbers that can easily identify the customer.

C. INFORMATION SECURITY

1. Evaluate the logical and physical security controls to ensure the availability and integrity of production retail payment systems applications. Determine:

   - Whether the physical and logical security controls established for retail payment transaction processing, clearance, and settlement services maintain transaction confidentiality and integrity.
   - Whether physical controls limit access to only those staff assigned responsibility for supporting the operations and business line centers processing retail payment and accounting transactions.
   - Whether physical controls provide for the ability to monitor and document access to all retail payment operations facilities.

2. Evaluate the effectiveness of all logical access controls assigned for staff responsible for retail payment-related services. Determine:

   - Whether management bases controls on separation-of-duties principles routinely implemented for the processing of financial transactions.
   - Whether management bases access controls on a need-to-know basis.
   - Whether management bases assigned access to retail payment applications and data on functional staff job duties and requirements.
   - Whether identification and authentication schemes include requiring unique logon identifiers with strong password requirements.
   - Whether displayed credit and debit card account data are partially masked to prevent full account numbers from being copied.
   - Whether network servers are satisfactorily hardened against the risk of internal or external hacking.
   - Whether servers simply used for data storage are unnecessarily connected to the Internet.
   - Whether sensitive customer information stored electronically is encrypted; if so, at what encryption level.
   - Whether internal audit or other third-party have conducted a security review.

3. Evaluate the security procedures for periodic password changes, the encryption of password files, password suppression on terminals, and automatic shutdown of terminals not in use.

4. Assess whether the institution encrypts telecommunications lines used to receive and transmit retail customer and financial institution counterparty data. If not encrypted, evaluate the compensating controls to secure retail payment data in transit. Assess whether any connecting technology service provider's networks used to transport transactions are transporting transaction data in the clear (not encrypted) or use weak forms of encryption.

5. Assess whether merchants use sufficient encryption for wireless sales terminal activity transmitting sensitive customer information.

6. Assess whether customer information being stored is beyond that required by industry standards.

D. CARD ISSUANCE

1. Assess bankcard issuance activities, and review control procedures. Determine whether management:
   - Issues bankcards only as requested.
   - Periodically inventories bankcards.
   - Maintains adequate controls for activating new accounts.

2. Assess effectiveness of the dual control procedures for blank card stock in each of the encoding, embossing, and mailing steps.

3. Assess adequacy of physical access controls for card encoding areas. Management should allow access to authorized personnel only.

4. Assess whether inventory controls for plastic card stock make them physically secure.

5. Assess whether management restricts the use of bankcard encoding equipment to authorized personnel only.

6. Assess adequacy of procedures for issuing cards from more than one location (e.g., branches) to ensure there are accountability and bankcard control procedures at each card-issuing location.

7. Assess adequacy of institution card-mailing procedures. Ensure the institution mails the card and associated PIN to customers in separate envelopes. Also ensure that the return address does not identify the institution.

8. Assess whether mailing procedures provide for a sufficient time between the card and PIN mailings.

9. Assess adequacy of returned card procedures. Determine whether adequate controls are in place to ensure returned cards are not sent to staff with access to, or responsibility for, issuing cards.

10. Assess whether there is appropriate follow-up to determine whether the correct customer received the card and PIN.

11. Assess the adequacy of control procedures (e.g., hot card lists and expiration dates) to limit the period of exposure if a card is lost, stolen, or purposely misused.

12. Determine whether the institution destroys captured and spoiled cards under dual control and maintains records of all destroyed cards.

13. Assess whether the institution adequately controls test or demonstration cards.

14. Assess whether management maintains satisfactory controls over the issuance of replacement or additional cards to the customer (e.g., temporary access cards issued to the customer).

15. Assess the adequacy of the vendor management program to determine whether the institution reviews card issuance services contracted to third parties for compliance with appropriate bankcard control procedures.

E. Business Continuity Planning

1. Assess the adequacy of the financial institution's business continuity plans for a partial or complete failure of each retail payment system. Determine whether the plans include:
   - Recovery of all required components linking the institution with third-party network switch, gateway, or related third-party data centers and bankcard processors.
   - Information relative to the volume and importance of the retail payment system activity to the institution's overall operation.
   - Provisions for acceptable store and forward procedures to protect against loss or duplication of data and to ensure full recovery within reasonable timeframes.
   - Provisions for secured transport and off-site storage of sensitive customer information.
   - Stand-in arrangements with other financial institutions, allowing for interim bankcard processing in the event of an outage.
   - Adequate testing of plans accounting for various recovery scenarios.

F. EFT/POS and Bankcard Accounting and Transaction Processing

1. Assess the adequacy of reconciliation processes for general ledger accounts related to bankcard and debit card transaction processing activity. Determine whether:
   - Accounting reconciles bankcard and ATM transaction activities daily.
   - Retail payment system supervisory personnel periodically review reconcilement and exception item reports.
   - Accounting periodically reconciles accounts used to control rejects, adjustments, and unposted items.

2. Assess the adequacy of the daily settlement process for institutions participating in shared EFT/POS networks or gateway systems.

3. Assess the adequacy of transaction reconstruction procedures. Transaction files should be duplicated or otherwise retained for a minimum of 60 days, as required by Regulation E, in order to identify unauthorized transactions.

4. Assess the adequacy of the investigative unit in place to address customer inquiries and control non-posted items, rejects, and differences. Management should periodically receive aging reports that list outstanding items.

5. Assess the adequacy of separation of duties for the bankcard and EFT/POS account posting process including receipt of transactions, file updates, adjustments, internal reconcilement, preparation of general ledger entries, posting to customers accounts, investigations, and reconcilement with third-party service provider network switches and card processors.

6. Assess the effectiveness and accuracy of the adjustment process (e.g., changes to deposits and reversals) relating to retail EFT/POS and bankcard transactions processed by staff.

7. For institutions involved in bankcard issuing or acquiring services, determine whether the institution has established:

   - Proper accounting controls for the balancing, settling, and reconciliation of all bankcard and acquiring accounts under its control.
   - Appropriate credit and liquidity risk measures for the bankcard and acquiring business lines.
   - Appropriate controls for the processing of customer or merchant transaction flows.

G. EFT/POS Operational Controls

1. Assess the effectiveness of personnel responsible for internal ATM processing. Determine whether there are:

   - Controls prohibiting staff members who originate entries from processing and physically handling cash.
   - Proper control of all source documents (e.g., checks for deposit) maintained throughout the daily processing cycle relative to:
     - Input preparation,
     - Reconcilement of item counts and totals,
     - Output distribution, and
     - Storage of the instruments.

2. Determine whether terminal and operator identification codes are used for all retail ATM and POS transactions.

3. Assess the adequacy of controls in place to prevent customer charges from exceeding the available balance in the account or approved overdraft lines.

4. Assess the adequacy of access controls for terminals used to change customer credit lines and account information.

5. Determine whether retail EFT equipment keyboards or display units are properly shielded to avoid disclosure of customer IDs or PINs.

6. Determine whether receipt issuance ensures customers receive a receipt showing the amount, date, time, and location for retail EFT transactions in compliance with Regulation E.

7. Assess whether each retail EFT transaction is assigned a sequence number and terminal ID to provide an audit trail.

8. Assess whether the institution regularly updates hot card or customer suspect lists and distributes them to branch banking locations.

9. Assess the adequacy of verification procedures for telephone-initiated payments or transfers and ensure confirmations are promptly sent to customers and merchants.

10. Assess the adequacy of security devices and access control procedures for EFT/POS, bankcard, and acquiring processing facilities to ensure appropriate physical and logical access controls are in place.

H. ACH ODFI AND RDFI RESPONSIBILITIES

1. Determine whether agreements between the ODFI and originators adequately address
   - Liabilities and warranties,
   - Responsibilities for processing arrangements, and
   - Other originator obligations such as security and audit requirements.

2. Determine whether the ODFI has established procedures to monitor the creditworthiness of its originator customers on an ongoing basis. Determine whether:
   - The ODFI assigns credit ratings to originators.
   - Competent credit personnel perform monitoring, independent of ACH operations.
   - Written agreements with originators require the submission of periodic financial information.

3. Determine whether the ODFI has established ACH exposure limits for originators. Determine whether:
    - The limit is based on the originator's credit rating and activity levels.
    - The limit is reasonable relative to the originator's exposure across all services (lending, cash management, foreign exchange, etc.).
    - Limits have been established for originators whose entries are transmitted to the ACH operator by a technology service provider.
    - Written agreements with originators address exposure limits.
    - A separate limit for WEB entries and other high-risk ACH transactions, as warranted, has been established.

4. Determine whether the ODFI reviews exposure limits periodically. Determine whether:
    - The ODFI adjusts limits for changes in an originator's credit rating and activity levels.
    - Increases in an originator's ACH debit return volume trigger a re-evaluation of the exposure limit.
    - The ODFI reviews the limits in conjunction with the review of an originator's exposure limit across all services.

5. Determine whether the ODFI has implemented procedures to monitor ACH entries initiated by an originator relative to its exposure limit across multiple settlement dates. Determine whether:
    - The monitoring system is automated and accumulates entries for a period at least as long as the average ACH debits return time (60–75 days).
    - Entries in excess of the exposure limit receive prior approval from a credit officer.
    - WEB entries and other high-risk ACH transactions (as warranted) are accumulated and monitored separately, yet integrated into the overall ACH transaction monitoring system.

6. Assess the RDFI's overdraft and funds availability policies and practices and determine whether they adequately mitigate its credit exposures to ACH transactions.

7. Determine the adequacy of the ODFI's practices regarding originators' annual or more frequent security audits of physical, logical, and network security. Determine whether:
    - The ODFI receives summaries or full audit reports from the originators.
    - The audits are adequate in scope and performed by independent and qualified personnel.
    - Corrective actions regarding exceptions are satisfactory.

8. Determine how the ODFI or RDFI manages its relationship with technology service providers. Determine whether:
   - The service provider's financial information is obtained and satisfactorily analyzed.
   - Service-level agreements are established and monitored.

9. Determine whether the ODFI allows technology service providers direct access to an ACH operator. Consider whether agreements between the ODFI and the service providers include:
   - A requirement that the service provider obtain the prior approval of the ODFI before originating ACH transactions for originators under the ODFI routing number.
   - The establishment by the ODFI of dollar limits for files that the service provider deposits with the ACH operator.
   - A provision that restricts the service provider's ability to initiate corrections to files that have already been transmitted to the ACH operator.
   - Provisions regarding warranty and liability responsibilities.
   - Appropriate handling of files (physical and logical access controls).

10. Determine whether the RDFI has established procedures to deal with consumers' notifications regarding unauthorized or improperly originated entries or entries where authorization was revoked.

11. Determine whether the RDFI acts promptly on consumers' stop-payment orders.

12. Determine whether the RDFI has procedures that enable it to freeze proceeds of ACH transactions in favor of blocked parties (under OFAC sanctions) for whom the RDFI holds an account.

13. Determine whether the financial institution considers the volume of its uncollected ACH transactions as part of its liquidity risk management practices.

14. Determine whether management and personnel display adequate knowledge and technical skills in managing and performing duties related to ACH transactions.

15. Review results from the financial institution's NACHA rule compliance audit. Determine:
   - The independence and competence of the party performing the audit.
   - Whether the board or its committee reviewed and approved the audit.
   - Whether responsibilities for high-risk entries, such as WEB, were included in the scope.
   - Whether corrective actions on audit exceptions are satisfactory.

I. ACH Accounting and Transaction Processing

1. Assess the adequacy of logs maintained for ACH payments received from, and delivered to, each customer.

2. Assess the adequacy of the balancing procedures used for all ACH payments received and whether they include balancing to the aggregate payments sent to an ACH operator.

3. Determine whether the institution balances all payments received from an ACH operator to the aggregate of payments delivered to customers.

4. Determine whether the institution verifies and authorizes the source of all ACH files received for processing.

5. Determine whether the institution reconciles all general ledger accounts related to ACH activities on a timely basis.

6. Determine whether ACH supervisory personnel perform reconcilement and regularly review exception items.

7. Determine whether the institution reconciles the ACH activity and pending file totals daily with the ACH operator.

8. Assess the effectiveness of the reconcilement with third-party service providers preparing ACH transaction files and ensure daily reconciliation.

9. Assess the effectiveness of ACH holdover transactions and determine whether the institution adequately controls them.

10. Determine whether accounting staff reconciles individual outgoing ACH batches before merging them with other ACH transactions.

11. Determine whether there are separate accounts to control holdovers, adjustments, return items, rejects, etc. and whether they are periodically reconciled.

12. Assess the effectiveness of the investigation unit to address customer inquiries and control return items, rejected/unposted items, differences, etc. Determine whether the unit periodically generates aging reports of outstanding items for management.

13. Assess whether management adequately tracks exceptions to credit limit policies and legal contracts.

14. Determine whether exception reports (e.g., rejects, return items, and aging of open items) receive appropriate management attention.

15. Assess the adequacy of separation of duties throughout the ACH process including origination, data entry, adjustments, internal reconcilement, preparing general ledger entries, posting to customer accounts, investigations, and reconcilement with ACH operators.

16. Determine whether adjustments (e.g., added payments, stop payments, reroutes, and reversals) to original ACH instructions are received in an area that does not have access to the original data files.

17. Assess whether controls are appropriate for the adjustment process, including authorization (e.g., signature verification and callbacks on telephone instructions) and whether the institution maintains adequate records (e.g., logs and taping of telephone calls) of individuals making requests.

18. Determine the adequacy of the customer profile origination and change request process. Consider whether requests:
    - Are in writing or equivalent confirmation for online activities.
    - Identify the originating personnel.
    - Document supervisory approval.
    - Are verified by staff unable to make changes.

J. ACH Funding and Credit

1. Assess the adequacy of the process for releasing payments to an ACH operator, and determine whether assurances are obtained that sufficient collected funds (e.g., on deposit or prefunded) or credit facilities are available. The institution should monitor customer intraday and interday positions based on defined thresholds.

2. For third-party service providers contracted to process outgoing ACH transactions, determine whether there are procedures to monitor ACH activity and ensure that funds are collected (collected balances, prefunding, credit lines) before the institution settles with the ACH operator.

3. For prefunding arrangements in place for customers without credit lines, determine whether management blocks funds (held for disposition) or maintains them in separate accounts until the transaction date.

4. For non prefunded arrangements determine whether the institution places blocks on outgoing payments to deposit accounts, applies them as reductions to credit lines, or includes them in the overall funds transfer monitoring process.

5. Determine whether management approves payments resulting in extensions of credit lines or drawings against uncollected funds and retains documentation to support the approvals. Determine whether the institution performs credit assessments of customers originating large

dollar volumes of ACH credit transactions. Credit assessments should also be reviewed periodically to evaluate creditworthiness of the customer and current economic conditions.

6. Determine whether management treats ACH debits deposited as uncollected funds and whether they monitor any draws against these funds for debits originated by high- risk customers.

7. Determine whether management approves draws against uncollected ACH deposits and maintains documentation to support approvals for debits originated by high-risk customers.

8. Determine the adequacy of Internet and telephone ACH transaction processing procedures and determine whether there are appropriate authentication controls and procedures to ensure the proper identities of parties invoking ACH transactions.

9. Assess the adequacy of management's risk assessment of ACH services in terms of the importance of this function to the overall corporate treasury services function.

10. Ensure that the financial institution obtains and analyzes all audits conducted by the ACH service provider, pursuant to the NACHA rule compliance audit requirement.

K. WEB AND TELEPHONE-INITIATED ACH TRANSACTIONS

1. Determine whether the financial institution has adopted adequate policies and procedures regarding ACH transactions involving Internet-initiated (WEB) entries. Determine whether they:
   - Are in writing and approved by the board or a designated committee.
   - Adequately address ODFI or RDFI responsibilities.
   - Establish management accountability.
   - Include a process to monitor policy compliance.
   - Include a mechanism for periodic reviews and updates.

2. Determine whether the ODFI has implemented telephone-initiated (TEL) ACH entries. Determine whether:
   - There are significant return rates for these transactions.
   - The institution adheres to NACHA guidelines concerning merchant management and their business practices.
   - Written agreements are in place with all originators submitting TEL transactions, and include adequate consumer (receiver) authentication and authorization.
   - The institution makes tape recordings of all consumer oral authorizations.

- The institution provides written notice to the consumer, prior to settlement date for the TEL entry, confirming the terms of the oral authorization.

3. Determine whether the ODFI requires its originator to employ a commercially reasonable method to authenticate the consumer/business. Determine whether:
   - Documentation of the method is adequate.
   - The frequency of the review of commercially reasonable standards is sufficient.

4. Determine whether the ODFI conducts risk assessments of its originators and whether they reflect a reasonable exercise of business judgment. Consider whether the risk assessment includes evaluations of:
   - Receiver authorizations.
   - Originator's Internet security capability, including;
     - Commercially reasonable fraudulent transaction detection systems and routing number verification,
     - Secure customer Internet sessions, and
     - Annual (or more frequent) security audits based on risk.
   - Frequency of risk assessments.
   - Documentation and approval standards.

L. ACH CONTINGENCY PLANS

1. Evaluate the adequacy of the ACH contingency plan; determine whether the financial institution has tested it and whether it includes provisions for partial or complete failure of the system or communication lines between the institution, ACH operators, customers, and associated data centers.

2. Based on the volume and importance of ACH activity, evaluate whether the plan is reasonable and whether it provides for a reasonable recovery period.

3. Determine whether the institution duplicates or retains transaction files for input reconstruction for a minimum of 24 hours. Note that NACHA rules require the retention of all entries, including return and adjustment entries, transmitted to and received from the ACH for a period of six years after the date of transmittal.

4. Determine whether data and program files are adequately secured, retained, and backed up at off-premises facilities, including secured transport mechanisms for those resources.

5. Determine whether the center has established and tested procedures to recover and restore data under various contingency scenarios.

6. Determine whether the frequency and methods of testing contingency plans are adequate.

M. CHECK 21

(A more comprehensive set of examination procedures that are designed to test transactions can be found at the FFIEC Check 21 InfoBase at www.ffiec.gov/exam/check21/default.htm.)

1. Determine whether:
   - The institution manages check return items effectively and whether there are significant numbers of return items.
   - The institution records source-document images for recovery if the originals are lost in transit.
   - The institution reconciles batch-dollar totals after processing.
   - Reject items are properly segregated from other work.
   - Exception items are controlled and tracked adequately.
   - Item processing duties are segregated appropriately.

2. If a financial institution has begun to image checks or retrieve imaged checks pursuant to Check 21, determine whether the institution has the following:
   - Consumer awareness program.
   - Customer service – training and education process.
   - Procedures for expedited re-credit.
   - Procedures to qualify returns of substitute checks.
   - Procedures to identify duplicate checks.
   - Procedures for statement preparation and processing.
   - Procedures for item repair.
   - Procedures for managing corporate customers wanting to submit substitute checks.

3. If the financial institution is a reconverting institution pursuant to Check 21, determine whether it has the following:
   - Procedures to identify, measure, and monitor fraud risk.
   - Security features for substitute checks.
   - Procedures for retention and retrieval of original items.
   - Procedures for identifying/controlling duplicate checks.

- Procedures or processes to control substitute check shrinkage.
- Procedures and processes to manage quality.
- Procedures and processes to manage endorsements (includes electronic).
- Procedures and processes to manage re-presentments.
- Procedures to ensure full MICR line is on all substitute checks.
- Procedures and processes to control cash letters.

4. If the financial institution accepts RCCs from retail business customers or payment processing customers, assess the appropriateness of, and adherence to, policies and procedures regarding customer due diligence, customer contracts, third-party service provider's due diligence, and activity/transaction monitoring. Consider the following elements relative to the institution's retail customers, its payment processing customers, and any processors' retail customers:
   - Customer due diligence performed at the initiation and periodically throughout the business relationship, including;
     - Assessment of risk exposure associated with the customer's underlying business models;
     - Review of operational history of customer (e.g., length of time in business, relocations of operations, and business reputation);
     - Performance of background checks on customer's principals and/or key operators.
   - Execution of contracts with customers containing provisions addressing;
     - Customer's agreement to operate in accordance with applicable laws and regulations (i.e., FTC Telemarketing Rule, UCC provisions);
     - The parties' responsibilities and warrants under Regulation CC;
     - Customer activity and/or transaction parameters and limits, including expected/allowable unauthorized return levels;
     - Auditing and/or access rights to customers' marketing scripts and consumer authorization/verification files;
     - The financial institution's ability to terminate the business relationship.
   - Routine monitoring and reporting of customer activity and transaction levels, including:
     - The integrity and timeliness of MIS reports on individual and aggregate customer activity/transaction and exposure levels;
     - Established management accountability throughout the business line, including an established process to report monitoring conclusions and exceptions to executive management;

- Periodic re-assessment of customer exposure and/or transaction limits in association with customer due diligence and contract reviews;
- The application of independent quality assurance or internal audit reviews to customer relationships in general and to customer monitoring activities in particular;
- Performance of on-site verification of customer authorization files where warranted.

N. REMOTE DEPOSIT CAPTURE RISK MANAGEMENT

1. Identify the key elements of the RDC environment.
   - Identify the bank staff, customers, and technology service providers (if applicable) involved in the RDC function. Obtain and review reports of RDC volume (number of transactions and dollar ranges) for the financial institution as a whole and for individual customers.
   - Obtain and review the topology of the financial institution's network, and determine the components involved in the RDC process. Identify the network interfaces with customers using RDC and the technology controls in place.
   - Obtain and review the financial institution's data flow or process flow diagram, including relationships with any third-party service providers (if applicable) and the relationships with RDC customers. Identify when the diagram was last updated, and assess whether it is consistent with the system currently implemented.
   - Identify whether the RDC system has the following features or functionality:
     - Duplicate item detection.
     - Scanner options (simplex/duplex, MICR/OCR, franking/spraying, CAR/LAR, etc.).
     - Interoperability with existing systems and/or ancillary applications (e.g., QuickBooks).
     - MIS and reporting (audit logs, activity reports).
     - Image quality.
     - Ability to change routing number, account number, and amount.
     - Least-cost routing functionality (conversion into different payment stream).
     - ABA validations (to identify deposits drawn on US versus foreign financial institution).
     - Ability to integrate with BSA/AML systems and processes.
     - Ability to integrate with OFAC systems.
     - Integration with enterprise-wide BCP.

- Information security (authentication, access controls, encryption, etc.).

2. Assess the RDC strategic planning and the risk assessment process.

- Obtain and review the financial institution's strategic plan for the implementation of RDC.
- Review board or board committee minutes involving discussion and approval of RDC implementation. Note the date of approval.
- Summarize the key objectives of the strategic plan, including:
  - The rationale for offering RDC (e.g., maintaining existing customers or attracting new customers; maintaining existing geographic footprint or penetrating new market/geographic area; wholesale only [merchant/commercial] or retail [consumer]).
  - The type of RDC to be offered (e.g., thick vs. thin client) or if multiple types will be offered to a single client.
  - The use of technology service providers.
  - Other key objectives.
- Describe the risk assessment process. Identify the financial institution's participants (e.g., representation from such functions as credit, IT, compliance, deposit operations, internal audit, and legal).
- Obtain and review the most recent risk assessment related to RDC. Evaluate the quality of the risk assessment and whether it encompasses factors such as:
  - Scope of product implementation.
  - Type of customer (e.g., commercial, retail, foreign correspondent).
  - Type of cash letter instrument and the geographic location of the originator.
  - Financial institution position in payment process and settlement channels used (bank of first deposit vs. nonbank of first deposit).
  - Current and anticipated volume of RDC transactions (number and dollar amounts of transactions).
  - Customer role and responsibility in the RDC process.
  - Customer ability to download and retain nonpublic information (NPI).
  - Financial institution's approved technology service providers and equipment.
  - Clearing and settlement channels: image exchange, ACH, or both.
  - Ability to integrate RDC into:
    - Anti-money laundering systems and processes.
    - BCP.
    - Information security planning.

        - Staffing and customer support.
    - Determine whether the RDC risk assessment is updated on a periodic basis as technology, market, customer base, industry, or processes change. Identify the date of the last risk assessment or update.

3. Customer due diligence and suitability.
    - Describe the process, the financial institution staff involved, and the decision criteria the financial institution uses to conduct a due diligence review to qualify potential customers for the RDC delivery system. Consider the following:
        - The function and level of the financial institution's staff who conduct the due diligence, and those who have the authority to approve a customer for RDC;
        - How the financial institution risk rates existing customers, on a recurring basis, and how they qualify potential customers;
        - The information the financial institution reviews for potential customers such as:
            - Customer application.
            - Financial analysis.
            - Years in business (for commercial customers).
            - Loan/deposit history.
            - Credit score.
            - Business practices.
            - Sufficiency of staff.
            - Compliance with PCI standards (when appropriate).
            - Publicly available reports for customers that are companies (e.g., Dun & Bradstreet).
            - Visa/MasterCard terminated merchant file or ChexSystems reports, when appropriate to the customer
        - Whether the financial institution has procedures that address customer identification as explained in the BSA/AML manual.
        - Whether the financial institution has procedures to address foreign correspondent relationships and international cash letter pouch activity as explained in the BSA/AML manual.
    - Describe the process and criteria used by financial institution management to evaluate the RDC customers' information security infrastructure and risk management processes.

4. Vendor Management

- Where technology service providers are used, determine whether RDC is included in the institution's vendor management program.
- Describe any service-level agreements between the financial institution and its service providers, and determine whether management of these relationships conforms to the Outsourcing Technology Services booklet.
- Determine whether any of the financial institution's RDC customers use a service provider in the RDC process. If so, evaluate how the financial institution manages risks, and whether the process is adequate.

5. Contracts and Agreements

- Determine whether legal counsel was involved in drafting any RDC-related contracts or agreements with technology service providers or customers.
- Obtain and review a sample contract or agreement between the financial institution and the RDC customer and technology service provider, where applicable. Consider whether contracts or agreements address the following:
    - Governing laws, regulations, guidelines, payment system rules, and other operational considerations relevant to traditional deposit processing.
    - Roles, responsibilities, and performance standards of the parties, including those related to the sale or lease of equipment needed for RDC at the customer location.
    - Liabilities, warranties, and indemnifications of all parties.
    - Types of items that may be transmitted.
    - Processes and procedures that the customer must follow (e.g., image quality).
    - Funds availability, collateral, collected funds, and reject/return requirements.
    - System maintenance and administration guidelines (e.g., change control and logical access administration).
    - Dispute resolution.
    - Information security requirements and procedures.
    - Security incident reporting.
    - Customer service and technical support.
    - Responsibility for network connectivity.
    - Establishment of controls, such as deposit limits, overdraft limits, and payment on uncollected funds.
    - Retention requirements and physical and logical security over deposit items and electronic files at the RDC customer location.
    - Business continuity planning requirements, including the back-up of data and periodic testing of such plans.

- Limiting high-risk customers to one account for RDC.
- Authority of the financial institution to mandate specific internal controls at the customer's location(s); audits of customer operations; and requests for additional customer information, as necessary.
- Authority of the financial institution to terminate the RDC relationship.

6. Insurance

- Determine whether financial institution management assessed the availability, coverage, and suitability of insurance related to RDC. If coverage has been obtained, describe.

7. Physical and Logical Access Controls

- Describe how financial institution management ensures that appropriate physical security controls exist at the RDC customer location, such as:
  - Building security.
  - Check storage.
  - Ensuring appropriate controls over portable RDC-related equipment, such as computers and scanner equipment and software.
  - Transport mechanisms for moving data to off-site storage locations.
- Describe how financial institution management ensures that appropriate logical security controls exist at the RDC customer location, such as:
  - Encrypted data transmission and storage.
  - Multifactor or other strong authentication.
  - Access level controls.
  - Password security parameters.
  - Equipment enrollment.

8. Separation of Duties

- Describe how financial institution management has established appropriate separation of duties for the system administration and security monitoring functions. For example, does one person assign users or rights and another review the activity reports?
- Describe how the financial institution and its RDC customers have implemented appropriate separation of duties controls over the remote capture and transmission process.
- Determine whether the financial institution performs any data entry functions (e.g., adjusting dollar amounts), and whether there is an independent review or reconciliation.

- Determine whether the financial institution requires separation of duties at the RDC customer location and how it monitors for compliance. If separation of duties is not mandatory or possible, describe any required compensating controls required at the RDC customer location.

9. Oversight and Monitoring

- Obtain and review the financial institution's policies and procedures for RDC. Assess whether they define the function, responsibilities, operational controls, vendor management, customer due diligence, BSA/AML compliance monitoring, and reporting functions, etc. Identify the date they were last reviewed and approved by the board or a board committee.
- Identify the financial institution staff members who perform periodic monitoring of RDC customer activity and describe the process used.
- Determine the frequency and process for management review of logical and physical access privileges and audit trails/logs.
- Identify and describe the monitoring reports used by the financial institution to manage risk. Obtain copies of reports used and review the monitoring process with appropriate financial institution staff. Discuss with appropriate financial institution staff the internal processes for responding to established threshold breaches and any escalation process. Examples include:
    - Duplicate Presentment Report (to detect duplicate batches prior to submission);
    - Daily Batch Totals Report;
    - Velocity Exception Report (to detect merchant spikes in volume or exceeding approved dollar limits);
    - Large Item Report (exception report to detect whether transactions are outside of normal parameters); and,
    - Customer Activity Report (detailed log of activity by merchant, including batch delivery date, time, value, receipt acknowledgement, and merchant operator ID).
- Identify and describe the RDC customer risk management reports recommended by financial institution management. Discuss how financial institution management validates that RDC customers review the reports. Examples include:
    - Pending Batch Report (items queued for processing for reasonableness and timeliness reviews);
    - Batch Total Report (allows the merchant to reconcile processed RDC work to the batch prepped for submission to the FI);
    - Return Item Report (alerts management to operational deficiencies, e.g., poor image quality);

- Duplicate Presentment Report (to detect duplicate batches prior to submissions); and,
- FI Reports (report would provide list of received imaged items).

- Select a sample of RDC customers and review the nature of account activity relative to the business type.

10. Training

- Determine whether financial institution management has established a training program to ensure that all parties involved are trained appropriately. If yes, describe the training programs for financial institution and customer staff.
- Determine whether the financial institution provides or plans to provide customer technical service or support to the RDC customers. If yes, discuss whether the financial institution considered the need for, or has added, additional staff.
- Determine whether the financial institution provides the merchant/consumer customers with a procedural or instructional document and a user guide for the application/scanner.

11. Change Management

- Determine whether the financial institution has enhanced its change management program to address the procedures involved in the RDC function and ensure ongoing compatibility between financial institution and customer systems. Describe the coordination process.
- If the financial institution maintains the application in-house, describe how it ensures that all relevant operating system and application patches are up-to-date.
- Describe how financial institution management ensures that RDC customers implement an effective change management program to maintain updated and patched network and desktop operating systems, RDC application, anti-virus, etc.

12. Records Management

Assess the process by which financial institution management verifies customer compliance with contract requirements related to the secure retention, storage, and destruction requirements for physical deposit items and electronic files.

13. Business Continuity Planning (BCP)

- Determine whether the financial institution's BCP has been updated to address:
  - The financial institution's relationship with the RDC service provider and BCP assurance.
  - The financial institution's relationship with the RDC customer.
- Determine whether the financial institution's BCP testing activities include:

- RDC systems and processes.
- RDC customers.
- Technology service providers, where appropriate.

14. Fraud

- Describe how financial institution management monitors for fraud associated with RDC.

- Describe how the financial institution attempts to mitigate fraud risks (e.g., duplicate check detection, establishing deposit limits, safeguarding checks).
- Describe how the financial institution monitors items that originated in foreign countries (i.e., foreign locations owned or controlled by customers of the financial institution or items received and processed by correspondent banks).

O. VENDOR MANAGEMENT

Assess the adequacy of vendor management program over a service provider that provides a new and emerging retail payment technology. (Select one or more projects involving the development and deployment of a new and emerging retail payment technology and complete the following procedures.)

1. Review documentation supporting the business case for the application
   - Scope and nature;
   - Standards for controls;
   - Minimum acceptable service provider characteristics;
   - Monitoring and reporting;
   - Transition requirements;
   - Contract duration, termination, and assignment; and
   - Contractual protections against liability.

2. Assess the extent to which the institution
   - Reviews the financial stability of the technology service provider;
   - Analyzes the service provider's audited financial statements and annual reports;
   - Assesses the service provider's length of operation and market share;
   - Considers the size of the institution's contract in relation to the size of the service provider;

- Reviews the service provider's level of technological expenditures to ensure on-going support; and
- Assesses the impact of economic, political, or environmental risk on the service provider's financial stability.

3. Evaluate whether the institution's due diligence considers the following:
   - References from current users or user groups about a particular technology service provider's reputation and performance;
   - The service provider's experience and ability in the industry;
   - The service provider's experience and ability in dealing with situations similar to the institution's environment and operations;
   - The cost for additional system and data conversions or interfaces presented by the various technology service providers;
   - Shortcomings in the service provider's expertise that the institution would need to supplement in order to fully mitigate risks;
   - The service provider's proposed use of third parties, subcontractors, or partners to support the outsourced activities;
   - The service provider's ability to respond to service disruptions;
   - Key service provider personnel that would be assigned to support the financial institution;
   - The service provider's ability to comply with appropriate federal and state laws. In particular, ensure management has assessed the service providers' ability to comply with federal laws (including GLBA and BSA); and
   - Country, state, or local risk.

4. Verify that the contract appropriately addresses:
   - Scope of services;
   - Performance standards;
   - Pricing;
   - Controls;
   - Financial and control reporting;
   - Right to audit;
   - Ownership of data and programs;
   - Confidentiality and security;
   - Regulatory compliance;
   - Indemnification;

- Limitation of liability;
- Dispute resolution;
- Contract duration;
- Restrictions on, or prior approval for, subcontractors;
- Termination and assignment, including timely return of data in a machine-readable format;
- Insurance coverage;
- Prevailing jurisdiction (where applicable);
- Choice of Law (foreign outsourcing arrangements);
- Regulatory access to data and information necessary for supervision; and
- Business Continuity Planning.

5. Review service level agreements to ensure they are adequate and measurable. Determine whether:
   - Significant elements of the service are identified and based on the institution's requirements;
   - Objective measurements for each significant element are defined;
   - Reporting of measurements is required;
   - Measurements specify what constitutes inadequate performance; and
   - Inadequate performance is met with appropriate sanctions, such as reduction in contract fees or contract termination.

6. Evaluate the institution's periodic monitoring of the service provider relationship(s), including:
   - Timeliness of review, given the risk from the relationship;
   - Changes in the risk due to the function outsourced;
   - Changing circumstances at the service provider, including financial and control environment changes;
   - Conformance with the contract, including the service level agreement; and
   - Audit reports and other required reporting addressing business continuity, security, and other facets of the outsourcing relationship.