CliftonLarsonAllen

Auditing of Wire Transfers, ACH Transactions and Remote Deposit Capture

Wire Transfer Audit Objectives and Risks Associated

- Ensure there are adequate policies and procedures in place.
  - Having adequate policies and procedures in place ensures that all Bank personnel know and understand what is required of them. Also ensure all employees have received the proper training on the policies and procedures. This should help the Bank minimize its risk of financial losses.
  - The policies should address at a minimum the following: segregation of duties, reporting and monitoring, OFAC verification, collection of funds, limits, record retention and information security.
  - Wire transfer agreements should be executed with all corporate customers.
  - Any customer who initiates repeat wire transfers should have a wire transfer agreement.

Wire Transfer Audit Objectives and Risks Associated (continued)

- Review of outgoing wire transfers to ensure wire transfers were properly authorized by reviewing completed wire transfer form.
  - The wire transfer form should include all required information to generate the transfer including the originator and beneficiary information, the dollar amount, the Bank authorizations and the customer authorizations.
  - When developing a form to use make sure the form is as robust as possible to capture all required information.

Wire Transfer Audit Objectives and Risks Associated (continued)

- If the customer is not able to sign the wire transfer form then proper call back procedures should be performed.
  - The call back number needs to be the number the Bank has on file and not any other number provided with this request.
  - This will help ensure the Bank is verifying the request with the actual customer and not a fraudster.
  - The name of call back verification should be authorized on the wire transfer agreement (if a corporate customer).
  - Voice recognition should be minimized.

Wire Transfer Audit Objectives and Risks Associated (continued)

- Ensure at least two individuals authorize outgoing wire transfers.
- Review access of the wire transfer department.
- Review access of the wire transfer application including password, tokens, etc.
- Review of duties to ensure there is adequate segregation of duties among the following tasks:
  - Posting and receiving funds
  - Initiation
  - Approval
  - Account reconciliation.
  - For example, individuals processing wire transfers should be separate from the loan origination function.

Wire Transfer Audit Objectives and Risks Associated (continued)

- Ensure proper reconciliation procedures are followed. Reconciliations of the main correspondent bank account should be performed daily.
  - The individual reconciling the correspondent bank account should not make entries into that account or have authority to initiate or approve wire transfers.
  - This will help ensure that fraudulent wire transfers are not being hidden within the reconciliation.
  - If this is not possible, the reconciliation should be reviewed by another individual on a regular basis.

How to Reduce the Risk of Wire Transfer Fraud

- Develop adequate policies and procedures.
- Execute wire transfer agreements on all corporate customers or repeat wire customers.
- Ensure proper adequate segregation of duties.
- Set prudent system limits.
- Limit acceptable methods of wire transfer requests.
- Get customer verification.
- Perform internal audit procedures.
- Watch for red flags (see next slide). Coach individuals responsible for accepting and verifying wire transfer requests to be skeptical.

Red Flags

- Wire transfers to and from other countries.
- Intentional circumvention of approval authority by splitting transactions.
- Frequent or large wire transfers for non-customers.
- Wire transfers against uncollected funds.
- Wire transfers from accounts with numerous cash deposits of just under $10,000 each.
- Lack of security controls surrounding wire transfer requests initiated by telephone, fax, etc.

ACH Audit Requirements

- An audit has to be performed annually and no later than December 31 each year.
- The audit can be done either internally or externally.
- Retain proof that an audit has been completed for a period of six years.
- Actual audit requirements are set forth in in Appendix Eight of the NACHA operating rules.
  - General procedures.
  - Procedures relating to the receiving of ACH entries.
  - Procedures relating to the origination of ACH entries.

ACH General Procedures

- Verify that records of entries are retained for 6 years and have all the necessary information.
- Verify that required encryption or a secure session is used for information transmitted via an Unsecured Electronic Network.
  - At a minimum a 128-bit RC4 encryption technology is required.
- Verify that Institutions have established, implemented and updated security policies, procedures and systems.
  - Institutions should either include the ACH risk assessment within the annual IT risk assessment or conduct a separate ACH risk assessment of the Bank's entire ACH operations. Ensure that ACH items are addressed within the Bank's IT policies and procedures.

Procedures Relating to the Receiving of ACH Entries

- Review of Prenotifications (Prenote).
  - Generally the auditor will select a sample of Prenotes and ensure the Prenote was for a valid account. If the Prenote was not for a valid account then a Notification of Change or a Return Entry should be processed.
- Review of Notifications of Changes (NOCs).
  - The auditor will select a sample of NOCs and ensure they were transmitted within two banking days of the Settlement Date.
- Ensure the Institution accepts all types of Entries.
  - The auditor will review a sample and determine all types of Entries were accepted.

Procedures Relating to the Receiving of ACH Entries (continued)

- Ensure credit and debit Entries are posted to the customers' accounts within the appropriate time frame.
  - The auditor will review a sample of Entries to ensure the following:
    - Credit Entries posted no later than the Settlement Date.
    - Debit Entries posted no earlier than the Settlement Date.
- Review of Stop Payments including reason codes.
  - The auditor will select a sample of stop payments to ensure the correct reason codes were used. Generally you will see code R08.

Procedures Related to the Receiving of ACH Entries (continued)

- Review of Written Statements of Unauthorized Debit (WSUD) including reason codes.
  - The auditor will select a sample of WSUDs to ensure the correct reason codes were used. Generally you will see codes R05, R07, R10, R37, R51 and R53.
  - Ensure these Entries were transmitted timely (no later than the sixtieth calendar day following the Settlement Date of the original entry).

Procedures Relating to the Originating of ACH Entries

- Ensure the Institution has entered into Origination Agreements with all Originators. The agreements should have at least the following:
  - The Originator must authorize the Institution to originate entries on behalf of the Originator.
  - The Originator must agree to be bound by these Rules.
  - The Originator must agree not to originate Entries that violate the laws of the United States.
  - Any restrictions on the types of Entries that may be originated.
  - The right of the Institution to terminate or suspend the agreement for breach of these Rules.
  - The right of the Institution to audit the Originator's compliance with the Origination Agreement and these Rules.

Procedures Relating to the Originating of ACH Entries (continued)

- Verify the Institution has performed due diligence on all Originators. This includes the following:
  - Assess the nature of the Originator's ACH activity and the risk it presents. This assessment should include an analysis of the types of transactions that will occur, the dollar amount of transactions, the number of transactions, how often they will occur, etc.
  - Establish, implement and periodically review an exposure limit for the Originator.

(continued on next slide)

Procedures Relating to the Originating of ACH Entries (continued)

- Verify the Institution has performed due diligence on all Originators. This includes the following:
  - Establish and implement procedures to:
    - Monitor the Originator's origination and return activity across multiple settlement dates.
    - Enforce restrictions on the types of Entries that may be initiated.
    - Enforce exposure limits.
  - This assessment needs to be completed initially before accepting the ACH originator and also annually.
  - This tends to be where findings occur as the Institution is not assessing the risks of the originators annually.

Procedures Relating to the Originating of ACH Entries (continued)

- Verify that the Institution has provided Originators with proper notice to ensure compliance with UCC Article 4A. This is generally included in the Origination Agreement and also the new account disclosures.
- Verify that the Institution has kept Originators informed of their responsibilities under these rules.

2016 Changes

- Same Day ACH: Moving Payments Faster
  - This will enable ACH Originators that desire same-day processing the option to send same-day ACH transactions to accounts at any receiving institution.
  - The Rule includes a “Same Day Fee” on each Same Day ACH transaction so that receivers would recover, on average, their costs for enabling and supporting Same Day ACH.
  - Originating institutions will be able to submit files of Same-Day ACH payments through two new clearing windows provided by the ACH Operators:
    - A morning submission deadline at 10:30 AM ET, with settlement occurring at 1:00 PM.
    - An afternoon submission deadline at 2:45 PM ET, with settlement occurring at 5:00 PM.

2016 Changes (continued)

- Same Day ACH: Moving Payments Faster (continued)
  - Virtually all types of ACH payments, including both credits and debits, will be eligible for same-day processing. Only international transactions and high-value transactions above $25,000 will not be eligible.
  - See checklists provided to help with implementation.

2016 Changes (continued)

- Improving ACH Network Quality - Unauthorized Entry Fee
  - Under this Rule, an originating Institution would pay a fee to the receiving Institution for each ACH debit that is returned as unauthorized.
  - Under this Rule, the originating Institution will have an economic incentive to improve the quality of the ACH transactions they originate. And will encourage them to perform enhanced risk management monitoring of Originators with high volumes or rates of Entries that result in unauthorized returns.
  - Receiving Institutions will be compensated for a portion of the costs they bear for handling authorized transactions, and will experience reduced costs due to a reduction in unauthorized transactions over time.

Common Wire Transfer and ACH Fraud Schemes

- Corporate Account Takeover
- Malware
- Social Engineering
- Phishing
- Vishing & Smishing
- Email Compromise

Generally, the Institution MUST follow accepted Cybersecurity practices to combat these fraud schemes.

Solutions for Detecting Wire Transfer and ACH Fraud

- Manual Review
  - This may be tedious and time consuming but the advantage is there is no technology investment needed but will come at the cost of staff time.
- Rules-Based Solutions
  - This may take a significant amount of time for updating as threats change, policies change, maintenance, a large number of false positives, etc.

Solutions for Detecting Wire Transfer and ACH Fraud (continued)

- Behavior-Based Prevention
  - Automatically monitor activity of every originator and beneficiary for every transaction.
  - Creates and continually updates models of individual behavior.
  - Easy to set up and doesn't require rules to be established or maintained.
  - Creates fewer false positives.
  - Overall this should reduce personnel costs, improve customer service and have a higher rate to detect fraud.

Remote Deposit Capture (RDC) Risks

- Legal and Compliance Risk
  - Controls over image capture process
  - Institution's contracts for clearing and settling checks
  - Check 21, Reg CC, Reg J, state laws, other agreements/clearinghouse rules
  - Liability allocation, dispute resolution, choice of legal jurisdiction
  - Risks and regulatory requirements under BSA laws
    - Money laundering
    - Compliance with AML laws and suspicious activity monitoring and reporting
  - Risks involved with foreign or high-risk RDC members

RDC Risks (continued)

- Operational Risk
  - Risks at member location
    - Faulty equipment, inadequate procedures or controls may lead to inappropriate document processing, poor image quality, and inaccurate electronic data
    - Ineffective security controls may lead to the alteration of deposit items, electronic check resubmission, or re-deposit of physical checks
    - Inadequate separation of duties can allow full access to the RDC process and alteration of information without detection.

RDC Risks (continued)

- Operational Risk (continued)
  - May extend to Institution's/service provider's internal networks through incompatible IT systems
    - Unauthorized software modifications
    - Ineffective or non-existent patching
    - Inadequate member authentication
    - Inadequate encryption of electronic information
- Fraud Risk
  - Identification of check alterations or counterfeit items
  - Forged or missing endorsements
  - Duplicate presentment at the Institution or another location
  - Insider fraud
  - Member access to non-public personal information

RDC Audit Objectives

- Ensure the Bank has the appropriate policies and procedures in place documenting the following:
  - Risk tolerance levels
  - Internal procedures and controls
  - Comprehensive customer agreements.
- Ensure the Bank has performed due diligence on the customer to ensure they are suitable for this product.

RDC Audit Objectives (continued)

- Ensure all RDC customers have signed agreements and include at least the following:
  - Roles and responsibilities of the parties for software and equipment
  - Item handling, storage, and retention requirements
  - Types of items that may be transmitted
  - Image quality requirements
  - Allocation of liability, warranties, indemnification, and dispute resolution
  - Periodic audits
  - Performance standards
  - Funds availability, collateral, and collected funds requirements
  - Governing laws, regulations, and rules
  - Institution's authority to mandate specific controls at member location
  - Institution's authority to terminate the relationship

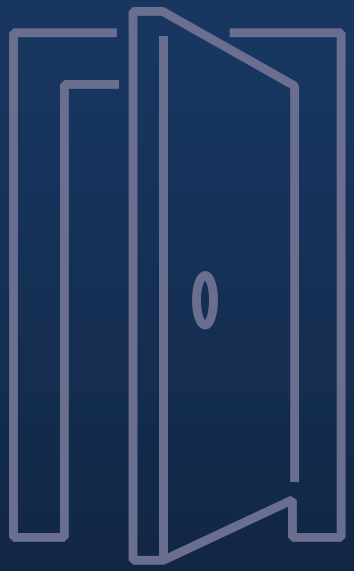
RDC Audit Objectives (continued)

- Determine if the Bank has provided onsite training and setup, including a review of the information security controls at the location.
- Verify that Institutions have established, implemented and updated security policies, procedures and systems.
  - Institutions should either include the RDC risk assessment within the annual IT risk assessment or conduct a separate RDC risk assessment of the Bank's entire RDC operations. Ensure that RDC items are addressed within the Bank's IT policies and procedures.
- Ensure the Bank's Business Continuity Plan includes RDC services and testing.

RDC Audit Objectives (continued)

- Ensure the Bank has developed and implemented risk measuring and monitoring systems, including:
  - Operational performance metrics
  - Regular management review of reports
    - Duplicate entries
    - Violations of deposit thresholds
    - Velocity metrics, including file size, number of files, transaction and return item dollar amounts and volume
    - Rejected items and corrections
    - Monthly, quarterly, annual trends

Questions?



Missy Roseberry
319-363-2697
missy.roseberry@claconnect.com

CLAconnect.com