Policy 2600: Electronic Fund Transfers

Model Policy Revised Date: 6/30/2020

General Policy Statement:

Mountain Laurel Federal Credit Union (Credit Union) utilizes electronic fund transfer services (EFT) to manage cash resources more efficiently. Specifically, the Credit Union uses the FedWire FEDLINE system to transfer funds related to its own operations and to transfer funds on behalf of its members. The Credit Union also provides other electronic services to members, such as automatic teller machines, telephone audio response, and debit cards.

The purpose of this policy is to ensure quality internal controls and minimize the inherent risks associated with various EFT systems. Systems covered under this policy include any transfer of funds initiated through an electronic terminal, telephonic instrument, computer, or magnetic tape that orders, instructs, or authorizes the Credit Union or any other financial institution to debit or credit an account. The Board will periodically assess the risks associated with EFT and will update this policy at least annually.

Guidelines:

1. **EFT SYSTEMS.** The Credit Union utilizes the following EFT systems:

    A. **FEDLINE.** The FedWire Fedline system allows the Credit Union to transfer funds from its Federal Reserve account to any other depository institution. Likewise, the Credit Union may receive funds from sending depository institutions. Under the operating rules of FedWire, each transfer is final and irrevocable when the receiving depository institution is notified of the transfer.

    B. **Retail Systems.** The Credit Union offers the following electronic services to members:

        i. Automatic Teller Machines.

        ii. Telephone audio response.

        iii. Debit cards.

        iv. Point of sale.

2. **EFT RISK ASSESSMENT.**

A. **Credit Risk.**

i. **Receiver Risk.** Receiver risk arises from the possibility that a sending institution will not honor a transfer. The Credit Union eliminates receiver risk by avoiding revocable transfers. Under the FedWire system all payments are final and irrevocable.

ii. **Sender Risk.** The Credit Union assumes sender risk whenever it makes an irrevocable payment on behalf of a member through extension of credit. The Credit Union minimizes this risk by:

a. Monitoring loans and any payments against uncollected funds or insufficient balances; and

b. Initiating effective collection procedures where necessary.

B. **Settlement Risk.** Settlement risk arises from the possibility that one participant in the payment system may be unable to honor its obligations at time of settlement, which in turn deprives other participants including the Credit Union of expected funds. Like receiver risk, settlement risk is minimized by only initiating and receiving irrevocable transfers.

C. **Systemic Risk.** The Board acknowledges that EFT systems may expose the Credit Union to systemic risk arising from the failure of one participant to honor settlement. However, the Credit Union has determined that these risk levels are within the Credit Union's risk tolerance.

D. **Legal Risk and Sovereign Risk.** The Board recognizes that the Credit Union is exposed to a certain degree of legal risk since there is no binding system of international commercial law for electronic payments. The Credit Union minimizes this risk by not participating in international transactions. In addition, by limiting transactions to the United States the Credit Union effectively eliminates sovereign risk resulting from adverse foreign government action.

E. **Operational Risk.** Operational risk is the Credit Union's most significant source of EFT risk exposure. The Board delegates responsibility to management for developing adequate procedures that reduce operational risk to acceptable levels. Such procedures shall provide for physical security, data security, systems testing, contingency planning, segregation of duties, and adequate backup.

3. **IDENTIFICATION AND CONTROL OF OPERATIONAL RISKS.** The Credit Union has identified three areas of operational risk:

A. **System Failure.** The risk that hardware or software will malfunction due to design defects, insufficient capacity, or mechanical breakdown. The Credit Union

controls this risk by periodically evaluating the systems design and capacity.

B. **System Disruption.** The risk that the EFT system is unable to process transactions due to system failure, natural disasters, fires, terrorists, or any other reason that could cause Credit Union operations to cease. The Credit Union minimizes this risk through contingency planning. In the event of system failure, wire transfers will be made through corporate central. In the event of a disaster, fire, or terrorist attack, sensitive information will be adequately secured whenever possible.

C. **System Compromise.** The risk of improper transfers due to error, fraud, or malicious acts, including the risk that records will be damaged or that funds will be diverted, altered, or manipulated. The Credit Union controls this risk through the development and implementation of internal controls.

4. **INTERNAL CONTROLS.** The Board delegates to management the responsibility for developing, implementing, reviewing, updating, and periodically testing internal controls. Internal controls should include procedures written in accordance with the following guidelines.

   A. **Personnel Procedures.**

      i. The Credit Union will run security checks on all personnel hired for sensitive positions in the wire transfer area. In addition, employees in sensitive positions are required to submit periodic statements of indebtedness.

      ii. The Credit Union will develop and implement a training program designed to ensure accurate performance of wire transfer activities and a thorough understanding of the necessity for internal controls. The program will also train employees to identify and report possible schemes to defraud.

      iii. Supervisors will afford special attention to new employees assigned to work in the wire transfer function to ensure proper training and compliance with Credit Union procedures and policies. As a general rule, new employees are prohibited from working in sensitive areas of the wire transfer function.

      iv. The Credit Union will inform employees that their responsibilities could be rotated at any time without prior notice.

      v. Relatives of employees in the wire transfer function may NOT work in the Credit Union's bookkeeping or data processing department.

      vi. The Credit Union will immediately reassign employees from sensitive areas of the wire transfer function upon receiving notice of resignation or

upon giving notice of termination.

B. **Operating Procedures.**

i. **Separation of Duties.**

1. The receipt, data entry, and authentication functions will be adequately segregated.

2. The function of determining the propriety of transactions will be performed by someone who does NOT receive orders and requests.

3. The function of reviewing rejects and exceptions is performed by someone who does NOT perform the receipt, preparation, or transmittal functions.

4. Investigations of failed payments are conducted by someone independent of the operating unit.

ii. **Security.**

1. **Access to Area.** Access to the wire transfer area is restricted to authorized personnel. Unauthorized individuals visiting the area must be accompanied by an authorized individual at all times.

2. **Access to Terminals.**

a. **Passwords.** The Credit Union restricts access to wire terminals and sensitive functions through password protection. Passwords are frequently changed to ensure integrity.

b. **Time-of-Day Controls.** Wire terminals are regulated by time-of-day controls. All terminals in the transfer area are shut down after normal working hours. Access during unauthorized times requires supervisory approval.

c. **Dual Operation.** At least two authorized employees must be present during operation of the terminal.

iii. **Records.** The wire transfer area will maintain current records and retain them for at least five years (See Policy 10000, Table 11). Records include:

1. List of authorized signatures and amounts for member transfers.

2. List of officers authorized to initiate transfers relating to Credit Union investments and any limits or restrictions. See Investment Policy.

3. Advices, requests, or instructions involving transfers over $10,000. Funds transfer message requests will contain:

    a. Sequence number;

    b. Amount if funds are to be paid;

    c. Name of member making request;

    d. Date;

    e. Evidence of authentication;

    f. Paying instructions; and

    g. Authorizing signatures.

iv. **Order Control.** All incoming and outgoing payment orders and message requests will be received in the wire transfer area, and all payment orders will be:

1. Time stamped or sequentially numbered;

2. Documented in a log book;

3. Examined for signature authenticity; and

4. Reviewed to determine whether persons initiating transfer requests have proper authority.

v. **End-of-Day Controls.** The following will be accounted for in an end-of-day proof to ensure that all requests have been processed.

1. All payment orders and message requests.

2. All pre-numbered forms including cancellations

3. Daily reconcilement of funds sent and received.

vi. **Testing.**

1. The testing area will be separated from the remainder of the operation area.

2. Test codes are:

    a. Required for telephonic requests;

    b. Used for transactions verified by someone other than the person who receives the request;

    c. Restricted to authorized personnel; and

    d. Maintained in a secure environment when not used.

vii. **Supervisory Review.** A supervisor will review:

1. All transactions prior to release of payments.

2. Daily reconcilement of funds transfer and message request activity;

3. Adjustments, open items, and reversals.

5. **MANAGEMENT REVIEW.**

A. **Reports.** Management will regularly review the following reports and promptly report significant matters to the Board.

i. Fund transfer activity reports documenting the number of items received and paid as well as total volume;

ii. Large overdrafts and drawings against uncollected funds;

iii. Payment activity for daylight overdrafts;

iv. List of suspense accounts;

v. Income and expenses relating to wire transfer operations; and

vi. Other reports as directed by the Board.

B. **Monitoring.** Management will regularly review:

i. Staff and employee compliance with credit and personnel procedures, operating instructions, and other internal controls.

ii. Capabilities of staff and employees.

iii. Adequacy of equipment relative to current and expected volume.

iv. Creditworthiness of funds transfer members.

6. **INTERNAL AUDITS.** The Supervisory Committee will oversee an annual comprehensive audit of operational internal controls and submit its findings to the Board.

   A. **Audit Findings.** The Board report should include an assessment of risks, evaluation of the adequacy of controls, and determination of compliance with this policy and applicable laws, regulations, and rules.

   B. **Board Action.** The Board will review audit findings and institute corrective action to address deficiencies noted.

7. **INTERNATIONAL REMITTANCE TRANSFERS**. See ***Policy 2605, International Remittance Transfers***.