



# **Loyola University of Chicago Electronic Funds Transfer (EFT) Policies and Procedures**

## **General Policy**

This policy relates to electronic funds transfer (EFT) which is defined to be the transmission of an electronic message to a financial institution instructing it to make an electronic entry reflecting the transfer of ownership of funds from one depositor to another. The Loyola University of Chicago (LUC) Treasurer's Office – Cash Management Services (CMS) is responsible for the daily management of University bank balances and the general oversight of EFT activity and should be consulted to provide assistance in determining when an EFT is the most cost effective and appropriate payment mechanism. The Vice President for Finance, CFO and Treasurer and Chief Investment Officer and Assistant Treasurer for LUC are responsible for the security and administration of EFTs and will provide EFT facilities for all appropriate banking institutions approved by the Board of Trustees. Subject to the system security and other procedures outlined in this document, the Director, Cash Management or other individuals designated by the CFO, Treasurer or Assistant Treasurer are authorized to initiate EFTs.

Although the University's primary method of disbursement is check based, EFT may also be used when a payment request meets one or more of the following conditions:

1. Legal or contractual requirements
2. Expedited payment required
3. Standard industry practice
4. Guaranteed payment delivery requested
5. Most cost-effective payment procedure

## **EFTs Between University Bank Accounts**

Because EFTs between LUC accounts have minimal risk, the Treasurer's Office may use EFT on a routine basis to concentrate funds for payment and investment purposes and to reallocate funds among investment accounts. Although risks are minimal for transfers between LUC accounts, reasonable controls should exist with regard to authorization, reconciliation, and review of these transactions.

## **Repetitive EFTs to Non-Loyola Bank Accounts (Vendors)**

This procedure relates to electronic funds transfer (EFT) which is defined to be the transmission of an electronic message to a financial institution instructing it to make an electronic entry reflecting the transfer of ownership of funds from one depositor to another. There are two EFT methods of payment, the first method is ACH (Automated Clearing House) and the second method is wire transfer. The difference in methods is an ACH payment takes LUC's bank one business day to transfer funds from LUC to the vendor and a wire transfer is processed on the same business day from LUC to the vendor. An ACH is the preferred method of payment, but in case of an emergency a wire transfer will be processed.

## **Repetitive ACH Processed by Accounts Payable**

The procedure to initiate a repetitive ACH to an unrelated party is subject to the same financial policies, procedures, and controls that govern disbursement by check:

The department providing signature approval of the ACH payment should complete the Payment Requisition form, all crediting instructions, bank name, ABA number, account number, account name and any additional information. Attached to the form will be a copy of the electronic funds transfer instructions received from the vendor. Once the Budget Administrator has approved the form it will be sent to Accounts Payable (AP) for approval and processing. If the ACH payment exceeds \$250,000 General Accounting will need to sign off on the payment.

AP will setup, change or delete the ACH payment information on the Lawson System.

The ACH payment information will stay active unless the same process is completed to delete or change.

If the Lawson ACH system is unavailable to process a vendor ACH payment due to additional addendum information that exceeds 40 characters, like Federal and State Tax Payments, etc. CMS will process the ACH payment.

AP will send the ACH vendor file to the bank when there are any ACH vendor payments that need to be processed. AP will electronically send forms AP265, and UI160 to CMS showing the total amount of the vendor ACH file. CMS will compare and review the reports showing the ACH payments. Once CMS has reviewed these reports, CMS will approve the ACH vendor file for processing at the bank.

General Accounting should reconcile the transaction to the General Ledger on a timely basis.

## Repetitive ACH or Wire Transfer Processed by CMS

The procedure to initiate a repetitive ACH or wire transfer to an unrelated party is subject to the same financial policies, procedures, and controls that govern disbursement by check:

All requests to set-up or revise a repetitive wire should be completed on the EFT Authorization Form (Form EFT01) by an authorized Budget Administrator and forwarded to AP for approval at least fourteen business days prior to the first payment request.

The department providing signature approval of the payment should complete form EFT01, which includes a description of the purpose of the transfer, all crediting instructions, the maximum dollar amount, the names of the Budget Administrators in the department who are authorized to approve the transfer and the approximate frequency. Attached to the form will be a copy of the electronic funds transfer instructions received from the vendor. The EFT01 form will be sent to the Budget Administrator for approval; once the Budget Administrator has approved the form it will be sent to AP for approval. If the maximum dollar value exceeds \$250,000 General Accounting will need to approve the EFT01 form. Once AP and General Accounting have approved the EFT01 form it should be sent to CMS for approval.

If any information on the EFT Authorization form changes the requesting Department is responsible for completing a new EFT01 form at least fourteen business days prior to the next repetitive transfer being initiated.

The ACH or wire transfer will stay active for a period of two years. Form EFT01 should be completed to renew or delete the ACH or wire transfer.

The EFT Requisition (Form EFT02A) will be completed by the requestor and sent to the Budget Administrator for approval, once the Budget Administrator has approved the form it will be sent or faxed to CMS for processing. The requesting department who is processing the EFT will attach backup for the dollar amount. CMS must receive EFT02A form prior to noon the day **BEFORE** the transfer is required.

General Accounting should reconcile the transaction to the General Ledger on a timely basis.

## Non-Repetitive Electronic Funds Transfers

The procedure to initiate a non-repetitive funds transfer to an unrelated party should follow a similar process but include additional controls to protect against unauthorized or unapproved use:

When a non-repetitive funds transfer is required, a written request or fax using form EFT02B should be sent to AP for signature approval. The non-repetitive EFT02B form must have supporting documentation attached to the form showing the wire transfer amount, the beneficiary bank and bank account number for the transfer to be processed. The department providing signature approval should forward the authorized form to AP for initiation prior to noon the day **before** the transfer is required. Once AP has approved the form, the form will be forwarded to General Accounting for approval if the payment amount exceeds \$250,000. Once AP and General Accounting have approved the transfer the form and back-up documentation will be sent to CMS for processing.

The transfer must be initiated via computer or telephone based system by the Director, Cash Management, or other designee of the CFO, Treasurer or Assistant Treasurer. The transfer but must be confirmed (released) via telephone or computer based system by the CFO, Treasurer, Assistant Treasurer, Director Cash Management or other designee of the CFO, Treasurer or Assistant Treasurer. The person who initiates the wire transfer CANNOT confirm or release the wire transfer, a second party must approve the transfer.

General Accounting should reconcile the transaction to the General Ledger on a timely basis.

Non-repetitive EFTs to unrelated parties present the highest security risk to LUC and should be used only when absolutely necessary. Repetitive EFTs should be established in all circumstances where a transfer routing is likely to be used more than once.

## **Repetitive Electronic Credit or Debit EFTs (Student Refunds, Donations, etc.)**

The procedure to establish a database of repetitive electronic credit or debit EFTs is subject to the same financial policies, procedures, and controls that govern collections and disbursements by check. An electronic credit is defined as an authorized electronic refund from LUC's bank account to a consumer's bank account. An electronic debit is defined as an authorized electronic payment from the consumer's bank account to LUC's bank account.

The EFT Database Authorization (EFT03) will be sent by the Budget Administrator to CMS for approval, once CMS has approved the form it will be sent to General Accounting for approval. This request for approval must be sent at least fourteen business days prior to the first payment. EFT03 form should include a description regarding the purpose of the transfer, the names of the persons in the department authorized to approve the transfer, the maximum dollar amount, and the approximate frequency. If any information on the EFT Authorization form changes the requesting Department is responsible for completing a new EFT03 form at least fourteen business days prior to the next transfer being initiated. The Database Authorization EFT03 will stay active for a period of two years. Form EFT03 should be completed to renew or delete the database authorization.

The LUC department authorized to process an electronic credit or debit against a consumer's account will be required to maintain the file of authorizations signed by the consumers authorizing the electronic credit or debit.

The LUC department will establish the proper internal security procedures and controls to verify that only authorized electronic credits or debits are processed. If the LUC department needs assistance in establishing these procedures CMS will assist.

The EFT Database Requisition (EFT03B) will be sent or faxed to CMS for processing. The requesting department who is processing the EFT03B will attach backup for the dollar amount.

General Accounting should reconcile the transaction to the General Ledger on a timely basis.

## **Repetitive Transfers Between LUC Bank Accounts Excluding Treasurer's Office**

The procedure is to initiate a repetitive EFT between LUC bank accounts excluding Treasurer's Office.

All requests to set-up or revise a repetitive LUC Bank Account to LUC Bank electronic funds transfer (Form LUtoLU.1) should be completed by an authorized Budget Administrator and forwarded to CMS for approval at least fourteen business days prior to the first payment request.

The department providing signature approval of the payment should complete form LUtoLU.1 which includes a description regarding the purpose of the transfer, all crediting instructions, the maximum dollar amount, the names of the persons in the department authorized to approve the transfer, and the approximate frequency. Once the Budget Administrator has approved the form it will be sent to CMS for approval.

If any information on the EFT Authorization form changes the requesting Department is responsible for completing a new (LUtoLU.1) form at least fourteen business days prior to the next repetitive transfer being initiated.

The Database Authorization LUtoLU.1 will stay active for a period of two years. Form LUtoLU.1 should be completed to renew or delete the EFT authorization.

CMS will set up, change or delete the repetitive code.

The EFT Requisition for LUC Bank Account to LUC Bank Account (LUtoLU.2) will be completed by the requestor and sent or faxed to CMS for processing. Form LUtoLU.2 must be received by CMS by noon on the day the transfer is required.

General Accounting should reconcile the transaction to the General Ledger on a timely basis.

### **EFT System Security Policy**

The following policies will guide LUC's Security Administrators as well as authorized individuals and departments utilizing any portion of the EFT system. The EFT system is

defined to include equipment, procedures and personnel used to send or receive transmissions related to maintaining and monitoring LUC's cash balances. As examples, activities accessed through the EFT system would include wire transfers, ACHs, direct deposit of payroll, stop payments and balance reporting.

### **Security Administrator Responsibilities**

Any combination of the CFO, Treasurer or Assistant Treasurer will appoint a Security Administrator to be responsible for the following: to protect the integrity of system user profiles. This includes assigning system IDs to users, changing user IDs as necessary, determining how frequently users must change passwords and assisting users with technical problems related to the EFT system. In addition, as specified by department heads the Security Administrator will assign users access to functions. The Security Administrator is authorized to lock out personnel as directed by the appropriate department head, the CFO, Treasurer and Assistant Treasurer.

### **EFT System Security Procedures**

1. All persons using the EFT system must be assigned individual user IDs by the Security Administrator. No department IDs will be assigned. The department head must request all IDs. Under no circumstances should IDs be shared.
2. All persons using the EFT system will be required to use passwords to gain access to EFT systems. Under no circumstances should passwords be shared.
3. Personnel outside of Financial Services must receive specific written authorization from the CFO, Treasurer and Assistant Treasurer to initiate or confirm electronic funds transfers. This authorization should be requested by the department head and directed to the CFO.
4. Personnel authorized to complete non-repetitive EFTs will be authorized to initiate or confirm a wire. They will NOT have the authority to initiate and confirm the same wire transfer.
5. All EFTs should be initiated by computer-based systems. Phone transfers should be used only as a backup should the computer systems be unavailable.
6. Computers used for EFT activity should be located in a secure area that is restricted to authorized personnel.
7. Departments initiating EFTs will be responsible for the timely review and reconciling of all EFTs. Departments needing guidance on appropriate reconciling procedures should seek the advice of Financial Services.