**Louisiana Legislative Auditor**

**BEST PRACTICES – CHANGING VENDOR BANKING INFORMATION IN THE MASTER FILE**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

***Background***

As more governments pay their vendors (and employees) electronically and move away from issuing paper checks, electronic payment fraud has become more prevalent and fraudsters have become more cunning. A common example of vendor fraud is a fraudster impersonating a vendor then requesting a change in banking information, which can ultimately lead to a government unknowingly paying the fraudster instead of the vendor. The Louisiana Legislative Auditor recommends implementation of this best practice, which may help a government reduce the risk of paying a fraudster posing as a vendor.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Written policies and procedures over changing vendor master file information should include **segregation of incompatible duties, written documentation of the vendor’s request to change information,** and **independent verification of the information changed through a secondary means of communication** to reduce the likelihood of changing a vendor’s master file information without the vendor’s knowledge or approval.

***Segregation of Incompatible Duties***

1. Good internal controls require separating the duties of custody, authorizing, recording, and reconciling to reduce the risk of fraud, or error occurring or going undetected.
2. To achieve a proper segregation of incompatible duties, the person who creates new vendors or makes changes to the vendor master file should not be the same person who generates payments or has access to checks, authorizes payments in any form, reconciles the bank statement, or receives cash.
3. If a full segregation of incompatible duties is not feasible, then the entity should consider the following compensating controls:
	1. Require management approval to set up new vendors or make changes to the master file of existing vendors;
	2. Require independent verification that new vendors are legitimate businesses before approving set up; and
	3. Periodically review a financial system report for any changes to vendor information and verify it is correct. (Note: even if segregation of duties is achieved, this type of periodic review should be conducted as a standard best practice.)

***Written Documentation of the Request to Change Vendor Banking Information***

1. When a vendor requests a change to their banking, address, or phone information, the government should **require that the vendor complete its Vendor Change Request Form and** **never accept banking, payment remittance address, or telephone change information in the body of an email or on any other form**.
2. The Vendor Change Request Form created by the government should require authentication criteria, including but not limited to:
	1. Existing banking, address, or phone information (banking institution name, name on bank account, routing number, and account number)
	2. New banking, address, or phone information (banking institution, name on bank account, routing number, and account number)
	3. The authorizer’s name, title, signature, and date
3. Require an original (“wet”) signature or a digital signature with a personal identification number (PIN) and a date signed on the Vendor Change Request Form.
4. On the Vendor Change Request Form, the vendor should sign statements agreeing to the following:
	1. The signer has authority to authorize the government to make deposits into the vendor’s account
	2. The direct deposit transactions comply with all applicable laws
	3. The government reserves the right to issue a check for payment when the situation warrants
	4. The signer authorizes the government to debit the account to correct erroneous credits and the account allows those transactions
	5. The signer agrees to notify the government immediately if information on the form changes and bears sole liability for lost or misdirected payments
5. The completed and signed Vendor Change Request Form should be encrypted before being emailed to an employee authorized to make changes to the vendor master file.

***Independent Verification of the Information Changed Through a Secondary Means of Communication***

1. When the employee authorized to make changes to the vendor master file receives the completed and signed Vendor Change Request Form from the vendor, the employee **should call the vendor using only the phone number in the accounting system’s existing vendor master file** and ask to speak with the signer of the form or that person’s designee to **independently verify the change request information.** This phone call should always be outbound by the government: inbound calls from the vendor to the government should never be an accepted method for independent verification.
	1. The employee should **ask the vendor to provide information that both the vendor and employee should know,** such as the vendor’s account number with the entity, the last four digits of the existing (old) bank account, last purchase order number, payment or invoice, etc. to verify that the employee is, indeed, talking to the legitimate vendor. If the person does not know these answers, ask to speak to the person who does and do not accept a response that the vendor will check with someone and let you know.
	2. Confirm that the bank account routing number and the bank name match bank records by looking up the routing number on the American Bankers Association’s [website.](https://www.aba.com/about-us/routing-number)
	3. Once the employee is satisfied that the legitimate vendor requested and authorized the change of information, and that the new information is accurate and approved by the vendor, then the employee should document on the Vendor Change Request Form the phone number called and the name and title of the person the employee independently verified the information with.
2. A person in the government other than the employee authorized to make changes to the vendor master file should review all applicable documentation and authorize, in writing and on the Vendor Change Request Form, that the change be made in the vendor master file.
3. The employee authorized to make changes should make the necessary changes then notify the vendor that their information has been updated and ask that the vendor notify the government immediately if the vendor did not request the change. Only after this step is taken should payment be made to the new bank account.
4. Periodically, a staff member who is independent of the processes listed above should review the master vendor listing and all change documentation and approvals, including the employees who have access to this information. This independent reviewer should follow-up on all irregularities until resolved (including contacting applicable vendors when necessary).

***Other***

1. Each vendor’s banking information should be secured and access to this confidential information should be severely limited to only those persons who need this information to perform their specific job duties.
2. The Vendor Change Request Form should not be posted on the government’s website, since it should not be readily available to all. Instead, vendors should be required to contact the government to request the form.
3. A government should exercise extreme caution and due diligence when a vendor requests to change not only its banking information, but also a mailing address, phone, or email at the same time, since it is unusual for vendors to change all this information at the same time.

***Steps to Take When a Fraudulent Payment Occurs***

1. Notify the government’s bank and follow all their instructions.
2. Notify the Federal Bureau of Investigation by submitting a complaint at [www.ic3.gov](http://www.ic3.gov) (Internet Crime Complaint Center) and follow all their instructions. Follow up with a call to the New Orleans FBI Field Office (504-816-3000) and reference the IC3 report that was filed.
3. Notify local law enforcement and follow all their instructions.
4. Per Revised Statute [24:523](https://legis.la.gov/Legis/Law.aspx?d=84144), notify the Legislative Auditor and District Attorney in writing when there is actual knowledge or reasonable cause to believe that a misappropriation of public funds has occurred.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The Louisiana Legislative Auditor (LLA) is providing the following best practice to help local government entities create their own written policies and procedures. Because this document may not include all legal provisions applicable to different types of local government entities, entities should consult with legal counsel when developing written policies and procedures. Also, many of the legal provisions referenced in this document may not apply to quasi-public organizations, such as non-profits. Quasi-public organizations should refer to the LLA’s legal FAQs for additional guidance.

**Sources:**

Government Finance Officers Association (GFOA) Best Practice, [Payments Made by Governments](https://www.gfoa.org/materials/payments-made-by-governments)

GFOA Advisory, [Electronic Vendor Fraud](https://www.gfoa.org/materials/electronic-vendor-fraud)

Federal Bureau of Investigation’s Internet Crime Complaint Center [www.ic3.gov](https://www.ic3.gov/)

American Bankers Association [www.aba.com](https://www.aba.com/about-us/routing-number)

Notification of the legislative auditor and district attorney – [La. R.S. 24:523](https://legis.la.gov/Legis/Law.aspx?d=84144)

Louisiana Cybersecurity Information Sharing Act – [La. R.S. 51:2101 et seq](https://legis.la.gov/Legis/Law.aspx?p=y&d=104223)

Database Security Breach Notification Law – [La. R.S. 51:3071 et seq](https://legis.la.gov/Legis/Law.aspx?d=322027)

Print on government’s letterhead

**Instructions for Completing the Vendor Request to Change Information**

Because vendor master file accuracy and security are very important to us, please follow the instructions below to submit a request for us to change your vendor information.

1. Please attach a Form W-9 so our records can be kept current.
2. If changing banking information, please provide a voided and pre-printed check which shows the new routing and/or bank account information.
3. Please complete only the information that you are requesting that we change in our master file and leave blank the information that does not need to be changed at this time.
4. To keep your information safe and secure, we ask that you encrypt the completed form and any attachments before emailing to us.

Upon receipt of the completed Vendor Request to Change Information, we will contact you by phone to verify this and other information which we both have in our files.

As an additional security measure, we will notify you that a request to change your information has been submitted. **If you did not request the change, please notify us immediately so we will not process the change.** If we do not receive a reply in 24 hours, then we will make the change in our master file upon completion of our internal control processes and procedures.

If you have any questions, please feel free to contact us.

 Employee’s Name

 Employee’s Title

 Employee’s Phone Number

 Employee’s Email

Print on government’s letterhead

**Vendor Request to Change Information**

Vendor Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Vendor #: \_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
|   | **Changing From ("old" information)** | **Changing To ("new" information)** |
| Banking Institution Name |   |   |
| ABA Routing Number |   |    |
| Name on Bank Account |   |   |
| Bank Account Number |   |   |
| Address (physical or remit-to) |   |   |
| Phone Number |   |   |
| Email |   |   |
| Other (specify) |   |   |

Reason for change: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Terms and Conditions**

My signature below indicates that I am agreeing that I am either the account holder or have the authority of the account holder to authorize the [name of entity] to make direct deposits into the account. I agree that direct deposit transactions I authorize comply with all applicable laws. The [name of entity] reserves the right to issue a check for payment.

I authorize the [name of entity], if necessary, to debit the above account only to correct erroneous credits. I certify that this account allows these transactions. I agree to notify the [name of entity] immediately if the information on this form changes. Failure to provide the [name of entity] with the correct information or failure to notify the [name of entity] of changes to my bank or account information will result in me, the vendor, bearing sole liability for lost or misdirected payments.

Authorizer Name and Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorizer Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

(Only an original signature or signature with PIN is acceptable)

This completed form should be encrypted and emailed to [insert person’s name and email address] or mailed to his or her attention at the physical or remit-to address above.

For [Government’s Name] Use Only

Information verified by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_ Phone # called: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Information verified (provide at least two):

PO # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Check/Voucher # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Invoice # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Verifier’s (vendor’s) name and title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approved to change information: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_