

## GFOA: FRAUD PREVENTION IN THE TREASURY OFFICE – RESOURCE

*This resource has been developed to assist governmental entities with having appropriate policies, procedures, and practices in place to prevent various types of internal and external fraud in the treasury office. This includes ways to deter vendor fraud, which is discussed separately at the end of this document.*

---

- Overview
- General Recommendations
- Banking Services Recommendations
- Payables Recommendations
- Receivables Recommendations

### **OVERVIEW**

Protecting public funds is a high priority for all governments. Fraud prevention includes the development and implementation of proper internal controls as well as education of employees to detect potential fraud. Effective fraud prevention is the result of a combination of controls, technology, and education. The goals are to limit exposure, reduce vulnerabilities, and safeguard the government's assets. Every government should develop a fraud prevention strategy (preemptive), and a fraud mitigation strategy (responsive); as fraud happens in large and small organizations alike.

Fraud can come from within an organization or from forces outside the organization. Internal fraud can include, but is not limited to:

- Mishandling currency
- Mishandling checks
- Misleading/mishandling invoicing
- Mishandling deposits
- Mishandling reconciliation
- Mishandling reporting
- Misappropriation of government assets (fictitious reimbursement claims or stealing non-cash assets)
- Corruption in the form of bribery, forgery, extortion, and conflict of interest
- Financial statement fraud due to fictitious revenues, hidden liabilities, inflated assets
- Misuse of purchasing cards, travel and entertainment cards, or card-less payable accounts

Likewise, external fraud can include the following:

- Counterfeit currency
- Check manipulation
- Credit card fraud, including skimming and other devices to steal customer information
- P-Cards/commercial credit card fraud
- ACH fraud/wire fraud including target email phishing, smishing and spearfishing or impersonation of government or vendor executives\*
- Vendor information and invoice processing

- Cyber threats and attacks to treasury's or an entity's web site that would include Treasury functions and systems (malware, phishing, for ransom).

Regardless of the source of fraud, it can generally be prevented or mitigated by leveraging effective internal controls, education of employees, and using the most up-to-date technology.

Governments should develop policies and procedures related to fraud and consider including the following:

### **GENERAL RECOMMENDATIONS**

- Establish a clearly defined written fraud risk policy.
- Develop well-structured fraud identification and reporting mechanisms that include anonymous reporting.
- Communicate clearly with staff about the entity's written fraud risk policy and components of identifying and reporting fraud, and reiterate policies and procedures in times of crises.
- Provide in-house fraud training.
- Determine who within your organization has authorization to contact local and federal authorities when fraud is discovered.
- Report fraud immediately to financial institutions, local authorities and federal authorities (e.g., FBI).
- Conduct periodic internal audits and annual reviews to assess effectiveness of fraud controls.
- Ensure proper segregation of duties among staff initiating, authorizing, preparing, signing, and mailing payments and reconciling bank statements.
- Ensure that controls exist for the storage and destruction of all documents that contain account and other related information.
- Avoid public dissemination of an entity's banking and financial information, including wire and ACH information.
- On at least an annual basis, request the government's legal counsel to research changes in laws that shift liability for fraudulent transactions to the government.
- Consider pre-emptive support services such as employee assistance plans to aid employees struggling with family, mental, financial problems – as a means to prevent an employee's decline into feelings of desperation.
- If you are aware of fraudulent account routing numbers, notify your bank and law enforcement. They may already be involved in a related investigation and might be able to help.
- Promote a "tone at the top" which emphasizes and encourages honesty and integrity.
- Consider periodic anonymous surveys to gauge employee morale, and encourage communication.
- Enhance fraud determination mechanisms to address issues that could arise during a crisis (e.g., COVID-19 shut downs, weather disasters, etc.).
- Have a business continuity plan in place for disasters/emergencies and other operational matters. The plan should include issues related to employees working remotely and having VPN and other security measures in place. Governments should also have a plan if electricity to government and other buildings is not in service.
  - When government buildings may be closed and offices are not fully staffed, segregation of duties related to treasury matters (e.g., printing checks, reviewing receivables, etc.) should still be maintained if at all possible.

## **BANKING SERVICES RECOMMENDATIONS**

- The treasury office should annually send to banks that you work with and that are in your jurisdiction, your tax id number as a way to ensure there are no unauthorized accounts open.
- Consolidate or eliminate bank accounts that are not frequently utilized.
- Use secure communications channels when exchanging information with your bank.
- Governments should use filtering and blocking options available to them on all bank accounts.
- Review signature cards, authority levels, and appropriate controls for employee remote access to financial/banking systems and with merchant processing systems at least annually and whenever any staffing changes occur.
- Ensure that your financial institution provides a quarterly listing, by account, of all approved signers and access-only individuals.
- Ensure that your financial institutions provide for multi-factor identification for on-line banking services involving transactions and administrative functions. Ensure separation of duties (initiation and release/approved) for financial transactions and administration of the on-line system. Multi-factor identification may include numerous passwords and/or utilization of user specific tokens.
- Remove individuals from bank transaction authority immediately upon resignation or termination.
- Consider segregating cash inflow and outflow in separate accounts to allow for placement of appropriate fraud prevention practices and products.
  - When appropriate (i.e. if no restrictions exist) these types of separate accounts should be maintained as Zero Balance Accounts (ZBAs) that are swept into the governmental entity's concentration account.
- Determine responsible party for fraudulent behavior.
  - The Uniform Commercial Code (UCC) regulates and defines the responsibilities of counterparties in business and banking transactions. The UCC states that, in certain situations, liability and monetary loss in a fraudulent transaction is split between the counterparties in a transaction based on each party's due diligence and negligence.
- Discuss enhanced or new account security features with your financial institution on at least an annual basis.
- Reconcile bank accounts daily to identify potentially fraudulent transactions.
- Utilize banking services designed to detect/prevent fraudulent activity including positive pay, payee positive pay, and account reconciliation services.
  - **Positive pay** is a type of account reconciliation service provided by banks. In positive pay, a bank compares checks that it receives for payment against the record of the checks issued by the government. If the bank receives a check that does not match the information (date, check number, and amount) in the government's record, it identifies it as an exception item (i.e., a non-conforming positive pay item). Payee positive pay is an enhanced positive pay service that requires the validation of the payee name in addition to validating the date, check number, and amount.
    - Instruct the bank to return all non-conforming positive pay items as the default instruction.
    - Ensure that a clear policy exists to separate responsibilities between staff approving positive pay exceptions and staff initially requesting and/or preparing the check.
    - Avoid reverse positive pay as the liability remains with the government. Instead, utilize payee positive pay.
    - When a check is rejected, follow through and check routing for deposit and contact that bank's fraud department to find out why check was rejected and notify police/authorities.
    - Positive pay services for ACH payments should also be used.

- **Reconciliation tools** allow governments to extract information from their bank or have information sent from their bank that assists the government in performing period end reconciliation of bank accounts. The bank may also provide a tool that completes a full reconciliation of the account and produces detailed reports of reconciled items.
- **Intra-day access** allows a government to see bank account transactions that occur at various times throughout the business day. The information may be accessed via online systems provided by the bank, as well as through other methods including fax, email, and direct transmission of data from the bank to the government's computer systems.

## **PAYABLES RECOMMENDATIONS: Checks, ACH/Wires, Card Payments, Vendor Processing**

*Governments should also review the Special Resource on Protecting Against Vendor Fraud which is included at the end of this document.*

### **Checks**

- Follow state laws regarding escheatment of checks and have a written policy for contact with payees in advance of escheatment.
- Have an additional review process for all checks over a specified amount.
- Utilize electronic methods (e.g. ACH) to make payments, as opposed to checks.
- Controlled disbursement accounts (CDA) for payroll and accounts payable disbursements.
- Maintain check stock in a secured/locked area and keep a secure inventory control listing of blank or unprinted check stock.
- Remove continuous check stock from printers.
- Secure all signature plates, cards, and software, and check-specific printers.
- Use digital check images instead of paper images.
- Generate check numbers using the financial accounting system.
- Physically void returned checks and check copies.
- Retain voided checks in a locked and secure location or destroy on a schedule.
- Use chemically-sensitive paper and/or dual-tone watermarks to prevent alteration and heat-sensitive ink markings on check stock.
- Consider the use of use expiration dates on checks (if allowed by law) noting that banks will not honor the expiration date. Instead void checks after six months and remove from positive pay issued list.
- Stay abreast of holder in due course matters related to the checks the governments hold and discovery that the individual/business has placed a stop payment has been placed or that the check was rejected by the bank.
- If outsourcing the payables function, ensure fraud precautions are continuously being done. This includes having staff check for any system fraud incidents, stale-dating, and accounting for missed check numbers.

### **ACH/Wire**

- Establish a list of authorized individuals who can enter online wire transfers.
- Define which staff members are authorized to approve wire transfers.
- Require two party authorizations (initiation and release) on all wires and ACH files.
- Define when the majority of weekly online wires will be submitted.
- Set maximum wire transfer limits – per user, per day.
- Perform daily account reconciliations to detect unauthorized ACH debits.
- Require daily staff reconciliation of wires and ACH releases.

- Request to be informed by phone if a wire transfer received by the bank looks suspect.
- Use the telephone to validate the authenticity of requests of unexpected wire transfers.
- Utilize ACH debit blocks or ACH filters.
  - **ACH blocks and filters** stop any attempt by an outside entity to process an ACH transfer and remove funds from a checking account without prior permission. ACH blocks prevent all disbursements from an account. ACH filters prevent disbursements that do not match a list of pre-authorized transactions or identification numbers. ACH filters involve: (a) giving prior permission to certain approved business partners to draw upon the account, (b) establishing an approval process for pending ACH transmissions, and/or (c) setting maximum dollar limits on ACH debit transactions.
    - Develop a formal plan to review ACH blocks/filters. This should be done on an annual basis, at a minimum.

### **Purchasing and Credit Card Payments**

- Structure effective internal requisition and authorization procedures for usage of purchasing cards, travel cards, card-less (i.e. ghost card) accounts, and commercial credit cards.
- Institute audit policies and procedures to detect abnormal, inappropriate, or excessive usage.
- Implement spending limits.
- Implement controls such as limits on when, where and how cards may be used by employees.

### **RECEIVABLES RECOMMENDATIONS**

- Conduct robust cash handling and credit card training for employees to include chain of custody between accepting payments (including credit card processing) at the government and processing at bank/financial institutions.
- Train employees on how to detect a counterfeit currency (blue light, pen marking) and have procedures on what to do when counterfeit currency is found, including calling local police and US Secret Service (<https://www.uscurrency.gov/>).
- Train employees on how to detect a fraudulent check and have procedures on what to do when such check is discovered, including calling local police.
- Governments should utilize secure methods when making deposits at banks such as armored car service, smart safes or security escort to bank.
- Governments should take precautions against credit card fraud by having current customer processing machines, and secure lines for processing. Governments should also be familiar with PCI compliance standards.
- Ensure entity is PCI compliant.
- Provide for the temporary physical security of electronically deposited checks, including storage in a secure facility, timely destruction such as secure shredding (the depositing government is liable for any fraudulent usage of these checks).
- Continually evaluate that the online payment card processor is secure and software is updated.

## **SPECIAL RESOURCE: PREVENTING VENDOR FRAUD**

***This resource highlights areas in which governmental entities should review and develop robust policies, procedures and practices to deter vendor fraud.***

---

- Overview
- General Strategies
- Staffing Strategies
- Process Strategies
- Form/Information Change Strategies
- Follow-up Strategies

### **OVERVIEW**

Vendor fraud is often associated with submitting fake documentation to change the bank routing and account numbers for electronic vendor payment deposits. These schemes often involve multiple hacks and may attempt to compromise vendor information, along with e-mail or other forms of identification, in an attempt to disguise the fraudulent activity. For example, fraudsters might hack e-mail or use a fake e-mail domain to make themselves look like legitimate representatives of a vendor.

Some strategies to help mitigate risk are listed below. No one strategy will stop all types of fraud, but implementing several strategies will help create a system of controls that better mitigates the risk of fraud. Additionally, GFOA recommends that governments review all control procedures to ensure that they are current and relevant to current threats.

### **GENERAL STRATEGIES**

- **Do not make any changes to vendor information, particularly payment addresses and/or bank account information, or employee direct deposit, without carefully reviewing the information provided and corroborating it through other sources. Governments should place a phone call to a vendor using number they have on file to confirm information.**
- Confirm wire instructions verbally with vendors prior to sending a wire for the first time. Confirmation through email should be avoided in case this mode of communication has been compromised.
- Investigate applicable insurance policy coverage to understand which types of risks are covered. Contact your insurance broker for additional information and procure supplemental coverage if needed.
- Coordinate with your information technology team to establish and maintain up-to-date system security and e-mail spam filters.
- Internal controls must be in place to ensure the same staff is not involved at every stage of changes and approval of vendor information and payments – regardless of payment method and the posting of that information in the entity's general ledger. The same staff should also not be involved in the processing and approval process.
- Consider the options provided by third parties, such as using a bank to manage and store vendor account and other sensitive information. If you choose this option, consider requesting a SSAE 16 system audit report from the provider.

- Governments may wish to include procedures that ensure that the vendor is authorized to provide services to the government and a W-9 has been obtained; that there is a system to review the work of employees who either initiate the invoice or authorized its payment; and that there is a final review and approval of all vendor payments.
- Once you become aware of a fraudulent account, scrub your vendor file data for other vendor accounts that might use the same bank routing number or account number. Inactivate any questionable vendor accounts immediately, until you are satisfied that the vendor has resolved the issue.
- Guard against invoice fraud to avoid (internal or external) manipulation of invoices that would call into question the credibility and accuracy of said invoice.
- Annually review your entity's vendor list to identify stale vendors and to confirm that new vendors are included.
- Be sure to apply an entity's internal control measures with input of vendor information in the ERP system.

### **STAFFING STRATEGIES**

- Train and empower accounts payable and vendor staff to routinely ask questions of both vendors and department staff.
- Involve additional staff members in the process of changing vendors. Proper segregation of duties helps ensure that the individual who enters information into the system or approves the change is not the same person who conducts due diligence on the vendor changes.
- Make sure that staff and outside departments understand the importance of prioritizing outstanding balance inquiries from vendors and resolving them quickly, following up on questions via telephone instead of e-mail. Payment questions need to be addressed as quickly as possible, because they may uncover vendor or payment fraud.
- Insist that staff use telephones, faxes, or the postal service for correspondence rather than e-mail to address issues with vendors (if the government or vendor has been recently hacked, an e-mail response will likely go to the fraudster rather than the vendor).
- Understand the practices of fraudsters and the ways in which their practices evolve with technology so you can be prepared for ever-changing assaults.
- Have the vendor manager or a supervisor review all vendor changes for a given day, week, or month. Provide the paperwork for vendor changes to the manager, along with a system report. Use this review process as a training tool to make your vendor staff more aware of risk.

### **PROCESS STRATEGIES**

- Using information you already have in your records, call the vendor to verify the existing account information and the information to be changed.
- Conduct an Internet search or validate the street address and phone numbers provided against reputable databases. Do not call a new phone number to verify changes; you may be talking to the fraudster.
- Before releasing payments, use an auditing tool to compare recent vendor account changes with check registers for a given check run. Follow up with the vendors included in the check run to verify account or address changes verbally before releasing payments. Incorporate this process into your daily pre-check run process.

- Do not rely on e-mail to confirm changes to vendor payment information. Fraudsters often hack the e-mail of one or both parties involved, so confirm changes by telephone instead.
- Do not give out vendor information over the phone. When confirming changes, provide staff with a script to use and always ask vendors to identify both old and new account information. The vendor should provide the information without assistance.
- When using systems that provide online tools vendors can use to update their own information, require that they use strong passwords, and consider the verification strategies listed above to confirm all changes.
- Vendor self-service capability should include an approval or notification process for staff and audit trail reporting.

### **FORM/INFORMATION CHANGE STRATEGIES**

- Remove vendor change forms from your government's website. Have the vendors contact government staff directly for forms.
- Vendors must use the government's form for changes to their information. Information from a vendor invoice should not be accepted.
- Revise your forms so they require vendors to provide both old and new bank routing and account numbers or billing addresses when requesting a banking change or a payment mailing change. A fraudster may have this information and use it to complete your form, but any additional information you request creates another barrier to keep him or her from getting through your internal controls.
- Beware of any vendor form changes that ask for revisions to more than one item in its account. For example; a vendor may change bank accounts, but is it also likely to request changes to its street address, contact, and e-mail address at the same time?
- Compare the vendor domain name with new domains provided on the form, and use the Internet to verify all changes.
- Look closely at the information and documentation provided by the vendor, such as a very low check number with a small number of digits. Is the paperwork provided what you'd expect to see from a large vendor with many business transactions?
- Is the vendor local but updating an account with an international bank or online-only bank? Is the language or wording of an e-mail unusual? While none of this may itself indicate fraud staff should nonetheless confirm changes through a phone call to the vendor using a known number.
- Determine if using a third party verification process to confirm vendor changes may be warranted. Governments should be aware of new solutions to verify vendor accounts will also be emerging from the entire banking and credit union community in 2021. Governments should ask their banker to be notified when the service is available.
- When using outsourced payables processors determine how the confirmation of vendor information changes are reviewed and made appropriately and ensure that liability for fraud is clear in the contract with the third party.

**September 2021**