BEST PRACTICES

Bank Account Fraud Prevention

GFOA recommends that governments consider various steps to protect themselves against bank account fraud.

Protecting public funds is a high priority for all governments. 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. Consequently, to reduce liability in the event of a fraudulent transaction, it is important to have proper controls in place.

Advances in technology have reduced the effectiveness of traditional fraud prevention techniques and have even enabled new forms of fraud. For example, in the past, many governments relied upon physical security features embedded in check stock to prevent check fraud. These included watermarks, unique colors, and graphical designs. Advanced duplication technology and remote deposit capture have reduced the effectiveness of these physical measures to prevent fraud.

The banking industry has developed the following fraud prevention tools:

- **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.

- **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.

- **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.

- **Universal Payment Identification Codes (UPIC)** may be used instead of the government's bank account numbers so that the government's account numbers are not disclosed.

GFOA recommends that governments consider the following steps to protect themselves against bank account fraud:

Internal Controls

- Conduct periodic surprise audits and annual reviews of procedures.
- Provide for the physical security of all checks.
  - Maintain check images in preference to paper copies.
  - Keep check stock in a locked and secure location with a formal inventory listing maintained. Secure check stock daily. Remove continuous check stock from printers. Lock and secure check specific printers. Consider the use of blank or unprinted check stock with inventory control numbers. The actual check number may be generated through the financial accounting system.
  - Physically void returned checks and check copies, and retain in a locked and secure location or destroy on a schedule.
  - 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.)
- Ensure appropriate security over signature plates, cards, and software.
- Require additional review process for all checks over a specified amount.
- Consider using a Controlled Disbursement account, to the extent permitted by law, for all payroll and Accounts Payable disbursements to provide additional control. It is preferable to make payments via batch ACH (direct deposit) for both Payroll and Accounts Payable as opposed to checks to reduce fraud potential and payment

expenses.

- Require two party authorizations (initiation and release) on all wires and ACH files.
- Require daily staff reconciliation of wires and ACH releases.
- Ensure proper segregation of duties among staff initiating, authorizing, preparing, signing, and mailing payments and reconciling bank statements.
- Review signature cards and authority levels whenever any changes occur and annually at a minimum. Remove individuals from bank transaction authority immediately upon resignation or termination.
- Review all bank accounts at least annually. Consolidate or eliminate bank accounts that are not frequently utilized.
- Depending on the complexity, size and volume, 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.
- Ensure that controls exist for the storage and destruction of all documents that contain account and other related information.
- Determine that appropriate controls are present if employees access the government's financial and banking systems from remote sites (i.e., restrict the sharing of files).
- 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.

Fraud Prevention Measures in Cooperation with Government's Financial Institution(s)

- Implement positive pay, or preferably payee positive pay, on all disbursement bank

accounts and reconcile exceptions daily. Positive pay is the single best fraud prevention tool available. If a government's bank offers a positive pay service and the government chooses not to utilize it, then the government (not the bank) will be liable for fraudulent transactions.

- 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 because with this service the liability remains with the government.

- Direct the bank to reject or block any and all withdrawals not initiated by the government from accounts that only accept deposits.
- Place ACH filters and/or blocks on all accounts.
  - Place total or selective ACH blocks on all disbursement accounts. Selective ACH blocks, also known as ACH filters, allow electronic debits to occur only for pre-designated transactions.
  - Develop a formal plan to review ACH blocks/filters. This should be done on an annual basis, at a minimum.
- Consider the use of Universal Payments Identification Codes (UPIC) for all receivables accounts.
- Ensure that your financial institutions provides 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.

- Ensure that your financial institution provides a quarterly listing, by account, of all approved signers and access-only individuals.
- Utilize bank reconciliation services to reduce time on reconciliation and focus on exception items.
- Discuss enhanced or new account security features with your financial institution on at least an annual basis.

References:

- *Evaluating Internal Controls: A Local Government Manager's Guide*, Stephen J. Gauthier, GFOA, 1996.
- *Banking Services: A Guide for Governments*, Nick Greifer, GFOA, 2004.
- Uniform Commercial Code as cited on the following website: http://www.law.cornell.edu/ucc/ucc.table.html

Board approval date: Wednesday, October 31, 2012