



Government Finance Officers Association

Recommended Practice

Bank Account Fraud Prevention (2007) (CASH)

(This RP replaces the RPs - *Check Fraud Protection* and *Use of Positive Pay or Reverse Positive Pay*)

Background. Financial assets held in bank accounts make attractive targets for criminals. Coupled with rapidly changing technology, including Check 21 authorized remote deposit capture, the need to protect public funds should be a top priority for all governmental entities. Traditional methods of fraud include forgery, identity theft, and check alteration. Newer forms of fraud have developed that take advantage of technological progress. These include unauthorized Automated Clearing House (ACH) drafts, multiple electronic deposits of the same check, and electronic intra-bank transfers. The Uniform Commercial Code has clearly stated that the liability for fraudulent items lies with the depositor, not the bank. Included with the law are significantly short lead times for the depositor to identify and report fraudulent items, especially if electronic account reporting is used.

In the past, many governmental entities relied upon physical security features embedded in the check stock. These included watermarks, unique colors, and graphical designs. With the rapid increase in the usage of remote deposit capture (Check 21) and image transfer, many of these physical measures have become obsolete and have limited effectiveness in preventing bank account fraud.

It is equally important to note that as remote deposit capture (Check 21) technology is adopted by each entity additional liability is created. In essence, each deposited check must be secured and destroyed in a timely fashion. It is critical when implementing this service to produce carefully written procedures specifically addressing the added concerns.

An important fraud prevention tool is positive pay. Positive pay is a type of account reconciliation service provided by banks. With 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 in the government's record, it identifies it as an exception item (i.e., a non-conforming positive pay item).

Recommendation. The Government Finance Officers Association (GFOA) recommends that governments consider the following steps to protect themselves against bank account fraud:

1. Implement positive pay on all disbursement bank accounts and reconcile daily. Positive pay is the single best fraud prevention device available.
2. Instruct your bank to *return* all non-conforming positive pay items as the default instruction.
3. Ensure that a clear policy exists to differentiate between staff approving positive pay exceptions and staff initially preparing the check.
4. Designate all depository accounts to reject any and all withdrawals other than intra-bank transfers.

5. Place total ACH blocks on all accounts that are not disbursement accounts. (Disbursement accounts should never be the depository accounts; see Recommendation 4 above.)
6. Place total or selective ACH blocks on all disbursement accounts.
7. Develop a formal plan to review ACH blocks. At a minimum, this should be done on an annual basis.
8. Conduct periodic and surprise audits or reviews of procedures. At a minimum, this should be done on an annual basis.
9. Provide for the physical security of returned checks and check copies or digital images. Electronic storage of check images is preferred over retaining paper copies.
10. Provide for the physical security of electronically deposited checks including storage in a secure facility, timely destruction via secure shredding and incineration, and dual control of the process. The depositing governmental entity is liable for any fraudulent usage of these checks.
11. Secure check stock daily. Remove continuous forms from printer, lock printer, and secure check stock in a locked environment.
12. Ensure that there is appropriate security over signature plates, cards, and software.
13. Require all checks over a specified amount to have an additional review process.
14. Ensure that your financial institution provides for multi-factor identification when using on-line banking services. Ensure appropriate separation of transaction duties for administration of the on-line system.
15. Consider the usage of Universal Payments Identification Codes (UPIC) for all disbursement accounts. This protects all bank accounts from identification from outside sources.
16. Review signature cards and authority levels at least annually and whenever any changes occur. Ensure that your financial institution provides a quarterly listing, by account, of all approved signers and access-only individuals.
17. Ensure proper segregation of duties among staff initiating, authorizing, preparing, signing, and mailing payments and reconciling bank statements.
18. Consider outsourcing the disbursements process.
19. Consider outsourcing the payment receipt process to an outside lockbox provider. This may provide additional separation of duties, security of confidential account information, and added reporting capabilities. A careful consideration of the cost versus benefit should accompany this consideration.

References

- *Banking Services: A Guide for Governments*, Nick Greifer, GFOA, 2004.
- *Evaluating Internal Controls: A Local Government Manager's Guide*, Stephen J. Gauthier, GFOA, 1996.

Approved by the GFOA's Executive Board, March 2, 2007