

BEST Practices



Volume 3, Issue 1, Part 2

Spring 2006

INSIDE

Fraud Indicators - "Red Flags"		2
General Red Flags		2
Red Flags in Purchasing and Disbursement		3
Red Flags in Sales/Receipts/Accounts Receivable		3
Red Flags in Payroll		4
Reactions to Fraud Indicators		4
Fraud and Small Governments		5
Receipts		5
Expenditures		5
Payroll		6
Petty Cash Funds		6
Procurement/Credit Cards		6
Other Preventive Techniques		7
Village of Mechanicsburg		7
Words of Wisdom		13
The Tips Page		14



A Message from Auditor of State Betty Montgomery

Dear Colleague,

My office is pleased to present the latest edition of *The Ohio Auditor of State's Best Practices* publication. As promised, this edition is the second in a two-part series dedicated to occupational fraud in government. While the last issue provided guidance on how governments

can assess and mitigate their risk for fraud, this issue discusses what governments should do when they are confronted with actual fraud indicators. We also provide additional guidance and recommended practices for Ohio's smaller governments, as they generally lack the necessary resources to devote to a formal antifraud program. Uniquely, this edition features an actual case of fraud that occurred in a small Ohio village, as well as the subsequent special audit that was initiated by this office. I believe the case epitomizes the vulnerability of smaller governments to fraud, yet further substantiates the need for all public organizations to be proactive in managing their fraud risks and strengthening their internal controls. Finally, we are introducing a new section to *Best Practices*, entitled The Tips Page, which provides tips on a variety of topics within government accounting and finance.

As you work to implement the recommendations and practices regarding fraud, remember that ignoring your fraud risks is like neglecting your car's regularly scheduled oil change. You may not experience immediate problems, but sooner or later you will be faced with costly repairs. Further, as governments work to strengthen their antifraud controls in accordance with *Best Practices*, the public can feel more confident that its tax dollars are being properly safeguarded.

As a reminder, you may report suspected incidents of fraud by calling **1-866-FRAUD-OH**, completing an online complaint form at www.auditor.state.oh.us, or mailing a written complaint to the Auditor of State's Office.

It is our hope that you find this issue as well as the last issue on governmental fraud valuable to your organization. As always, we look forward to any feedback you may have regarding the information presented in *Best Practices*.

Sincerely,

Betty Montgomery
Ohio Auditor of State

Fraud Indicators - "Red Flags"

Consider the following scenarios:

Like so many other prudent, responsible government officials in Ohio, you've read the last issue of *Best Practices* and have worked with your colleagues to implement its many recommendations designed to identify, assess, and mitigate fraud risks. If you haven't yet read the Winter 2006 issue of *Best Practices*, you may access it by clicking www.auditor.state.us/publications/. Specifically, your organization has established a formal fraud risk prevention program, incorporating such measures as standard operating procedures, an internal audit function, and an ethics policy. Further, your organization has implemented a risk assessment program and bolstered its internal controls in a number of areas that appear vulnerable to fraudulent activity. All in all, your organization's antifraud efforts seem to be working as planned, when suddenly your assessment activities reveal what appears to be an indication of fraud. In fact, you discover an unusual increase in adjustments and write-offs to customer utility accounts, which is a potential fraud indicator. At this point, without further investigation, management does not know whether fraud has actually occurred.

Compared to fraud risk indicators (which you may recall from the last issue of *Best Practices*), actual fraud indicators represent instances where fraud may have occurred, as opposed to situations or conditions in an organization's operations that lend themselves to an increased risk for fraud. To draw a further distinction between the two, fraud risk indicators help organizations develop preventative measures in areas that are at risk for fraud, while fraud indicators help organizations detect fraud after it has occurred. Other examples of fraud indicators or "red flags" and their corresponding area of operation include:

General Red Flags

- ✓ Significant lifestyle changes among employee(s): expensive cars, jewelry, homes, clothes, etc.
- ✓ Employee(s) with significant personal debt and credit problems
- ✓ Significant behavioral changes among employee(s) - possibly indicative of drug, alcohol or gambling problems, or fear of job loss
- ✓ Instances where employee(s) refuse to take vacation or sick leave or refuse to accept promotions
- ✓ Reluctance among employee(s) to provide information to auditors or investigators
- ✓ Excessive number of checking accounts maintained by entity
- ✓ Frequent changes in banking accounts
- ✓ Frequent requests for new external auditors
- ✓ Excessive number of year-end transactions or journal entry adjustments
- ✓ Unsupported transactions or journal entry adjustments
- ✓ Refusal by employee(s) to use serial numbered documents (e.g., receipts)
- ✓ Unexpected overdrafts or declines in cash balances
- ✓ Financial transactions that don't make sense - either common or business
- ✓ Service contracts for which there is no product
- ✓ Missing or altered documents (e.g., accounting records)
- ✓ Photocopied documents in place of originals
- ✓ Significant sums of money lent/borrowed among co-workers

- ✓ Visits by creditors or collectors at the workplace
- ✓ Evasive or unreasonable responses to questions
- ✓ Employee(s) with unusually large sums of money

Red Flags in Purchasing and Disbursement

- ✓ Increased number of complaints received by the entity about products or service
- ✓ Acceptance of gratuities or significant “promotional” items by employee(s)
- ✓ Frequent use of handwritten endorsements vs. stamped endorsements
- ✓ Prepayment of goods or services
- ✓ Frequent use of sole source procurement contracts
- ✓ Pressure to expedite payments
- ✓ Inordinate volume of “manual” checks
- ✓ Lack of physical security over assets/inventory
- ✓ Payments to vendors that aren’t on an approved vendor list
- ✓ High volume of purchases from new vendors
- ✓ Purchases that bypass the normal procurement procedures
- ✓ Vendors without physical addresses
- ✓ Vendor addresses matching employee addresses
- ✓ Purchasing agents that pick up vendor payments rather than have them mailed
- ✓ “Consulting” contracts for which there is no determinable end product
- ✓ Abnormal number of expense items, supplies, or reimbursement to employee(s)
- ✓ Significant deviations from specifications on delivered goods or services
- ✓ Handwritten/typed vs. computer generated invoices
- ✓ Cash payments when checks expected

Red Flags in Sales/Receipts/Accounts Receivable

- ✓ Excessive number of voided receipts, customer discounts, and/or returns
- ✓ Unauthorized voided receipts, customer discounts, and/or returns
- ✓ Unauthorized customer/taxpayer account adjustments or write-offs
- ✓ Untimely deposits
- ✓ Unauthorized bank accounts
- ✓ Frequent use of handwritten vs. stamped endorsements
- ✓ Sudden activity in a dormant banking account
- ✓ Taxpayer/Customer complaints that they are receiving non-payment notices
- ✓ Discrepancies between bank deposits and postings
- ✓ Excessive or unjustified cash transactions
- ✓ Large number of write-offs of taxpayer/customer accounts
- ✓ Significant and/or frequent cash register shortages and overages
- ✓ Increase in past due accounts
- ✓ No collection efforts on past-due or written-off accounts
- ✓ Cash payments when checks expected

Red Flags in Payroll

- ✓ Inconsistent overtime hours for a cost center
- ✓ Overtime charged during a slack period
- ✓ Overtime charged for employee(s) who would not normally receive overtime pay
- ✓ Budget variations for payroll by cost center
- ✓ Employee(s) with duplicate Social Security numbers, names, and addresses
- ✓ Employee(s) with few or no payroll deductions

Reactions to Fraud Indicators

Once the organization is confronted with a fraud indicator, the next step is to develop a strategy for determining whether fraud has, in fact, occurred. As a general consideration, the steps taken to investigate potential fraud should occur from the "outside-in." In other words, management should begin by gathering information from other sources before confronting the alleged fraudster. This approach is recommended so as not to alert the alleged fraudster to the investigation and to protect the parties involved against unproven allegations.

To begin the investigation, management should gain a thorough understanding of the process surrounding the fraud indicator. Not only should management evaluate any relevant policies and procedures, management should also interview personnel to assess adherence to the policies and procedures. Further, management should gather any corroborating documentation related to the suspicious activity. Sources of corroborating documentation may include other departments, external third-parties (e.g., vendors or other governmental entities), and various information systems. At this point, management should be able to make a preliminary assessment as to whether fraud has taken place. Additionally, early on in the investigation, management should consult with the organization's legal counsel and human resources department to address any legal or other liability issues. Once the allegation is substantiated, management should then determine whether to contact the appropriate law enforcement agency and/or the Auditor of State.

Using our previous example where management discovered an unusual increase in adjustments and write-offs to customer utility accounts, management should consider the following steps to further investigate the fraud indicator:

- Evaluate any available documentation supporting account adjustments or write-offs.
- Compare the current billing period to prior billing periods to determine if write-offs and adjustments are abnormally high or in line with prior periods.
- Select a sample of written-off and adjusted accounts and recalculate the billings based on actual usage levels.
- Confirm amounts paid with utility customers.
- Reconcile amounts paid by customers with amounts posted to their utility accounts.
- Compare money collected and deposited to customer receipts.

If the results of performing the above steps indicate alleged fraud, management should consult the organization's legal counsel to determine the best course of action, which may include contacting the appropriate law enforcement agency and confronting the alleged fraudster.

Fraud and Small Governments

As the Association of Certified Fraud Examiners (ACFE) survey revealed in the last issue of *Best Practices*, small organizations (those with fewer than 100 employees) are particularly vulnerable to fraud, primarily because they lack the resources that are necessary to sufficiently control their risk for fraud. For instance, they may not employ enough fiscal personnel to ensure segregation of duties among the government's receipt and deposit processes. With the same person responsible for both receipting and depositing monies, the government's risk for fraud increases as that individual is better situated to take the funds before they are properly recorded and deposited into the government's account.

Because small governments lack the necessary resources to implement sufficient controls, it is critical for their governing boards and fiscal officers to actively monitor areas that are particularly vulnerable to fraud. Further, they should be cognizant of fraud indicators so frauds are detected before they cause significant loss to the organization.

Although smaller governments generally do not have staff dedicated specifically to do internal audits, there are a number of risk assessment activities and other fraud prevention techniques that can be completed by the government's governing board, fiscal officer, and other fiscal personnel. Below are some of the more common fraud prevention techniques used by small governments and their associated risk areas:

Receipts

- Issue all receipts sequentially so missing receipts can be more easily identified.
- Use a duplicate or triplicate receipt book to ensure corroborative documentation exists for monies received by the government.
- Periodically total receipts for a selected period and compare the amount collected to the amount deposited to identify discrepancies.
- Review any voided receipts to ensure there is sufficient reasoning and support for the void. Typically, if a receipt is voided, there should be a reason documented on the receipt, and a subsequent receipt should be issued for that payment.

Expenditures

- Issue all checks sequentially so missing checks can be easily identified.
- Ensure that checks are signed by someone other than the preparer. If one person performs both functions, he or she could more easily divert public funds to his or her personal account.
- Require the individual who signs the checks to review invoices and other documentation to verify the amount of the purchases and to ensure that the purchases are for government business.¹
- Periodically review checks and related endorsements for irregularities, including the

¹ For those villages with combined clerk/treasurer positions, the mayor or council president should sign the checks, while someone independent of the check preparer should review the supporting documentation.

use of varying font types on checks and forged endorsement signatures.

- Refrain from providing employees with blank, endorsed checks as this increases the risk that a portion of the purchase could be used for personal items.
- Avoid the use of erasable ink as the name of the payee may be altered for fraudulent reasons.

Payroll

- Regularly compare staff rosters with payroll registers to identify potential ghost employees through whom fraudsters may receive additional pay.
- Periodically compare employee hourly rates per the payroll register to the approved hourly rate to ensure rates have not been erroneously, or worse, fraudulently inflated.
- Review time cards for approval prior to payment to help protect the government from paying for work not performed.
- Ensure policies are in place governing overtime compensation and leave.

Petty Cash Funds

- Establish the amount of the petty cash fund and guidelines for its use. Generally, the fund should be used for small emergency purchases for which there is not enough time to use the government's normal purchasing process.
- Require those using the petty cash fund to attach the receipts to the reimbursement voucher to ensure purchases were for government business.
- Periodically review receipts to ensure the purchases are for a proper public purpose (see AOS Technical Bulletins 2003-005 and 2004-002 available at www.auditor.state.oh.us under Publications).
- Periodically compare the petty cash fund balance with the amount of receipts supporting the checks issued to replenish the fund. Identified shortages could be an indication of fraud.

Procurement/Credit Cards

- Establish a thorough policy governing card usage and the processes used to ensure proper use of the card.
- Implement limits and other restrictions through the credit card company on the amount and type of purchases that can be made using the card.
- Review purchases along with receipts and invoices to ensure they are related to official government business.
- Require employees to sign an agreement stating they will not use the card for personal purchases.
- For an extensive discussion on procurement/credit cards including recommended controls and usage policies, please see the Winter 2004 issue of this newsletter at www.auditor.state.oh.us/Publications/.

Other Preventive Techniques

- Ensure the governing board is involved in the organization's finances. The mere involvement of the board can help deter employees from committing fraud in the first place.
- Document job duties for each employee to define work processes and standards for performance. Once job duties are formally defined, management can more easily identify areas that are at risk for fraud.
- Review monthly bank account reconciliations. Any unusual adjustments should include supporting documentation; otherwise, such adjustments are "red flags" for potential fraud.
- Segregate critical fiscal duties among staff to ensure one person does not have sole responsibility where checks and balances are necessary. Such duties include receipting and depositing public funds, preparing and signing checks, submitting and approving payroll, etc. When segregating these duties is not possible, the governing board should conduct surprise reviews on the activities of those individuals to help detect irregularities.

Village of Mechanicsburg

The following case is being provided to show readers how fraud impacts even the smallest level of government in Ohio. The case also illustrates the need for small governments to implement the prevention techniques discussed above to help reduce their risk for fraud.

In February 2004, the Auditor of States' Office (AOS) received a tip from a concerned employee from the Village of Mechanicsburg (Champaign County) alleging that the Village Clerk/Income Tax Administrator was misusing public funds. The tip was received through the AOS Fraud Hotline at **1-866-FRAUD-OH**, a component of the AOS's *Taxpayer Protection Initiative* (Visit www.auditor.state.oh.us for more information on this initiative).

The AOS Special Investigations Unit met with Mechanicsburg Police Chief, Tim Bostic, who indicated that he was aware of monies missing from the Village's Summer Celebration Account. Upon further review of this account, Bostic believed income tax monies were being used to replenish missing Summer Celebration funds. He also noticed that cash income tax collections were missing.

Following meetings with other Village officials and the Champaign County Prosecutor, the AOS initiated a special audit of the Village of Mechanicsburg for the period November 1, 2001 through April 16, 2004.

Income Tax Receipts

Susan Cantrell, who served as both Village Clerk Treasurer and Income Tax Administrator, was responsible for receipting, depositing, and recording income tax payments to taxpayer accounts; which as noted above, is a clear lack of proper segregation of duties. Ms. Cantrell prepared a triplicate receipt for each income tax-related payment received by the Village. The white copy of the receipt was given to the taxpayer making a payment in person. When the payment was not in person, all three copies were maintained by the Village. In explaining the income tax collection process, Ms. Cantrell indicated that she would often write the amount paid on the individual's tax return. Finally, she would total the receipts to ensure they reconciled with the daily receipt journal and deposit slip.

On the surface Ms. Cantrell's explanation of the income tax collection process seemed normal, although it lacked some obvious internal controls (e.g., segregation of duties for the receipt and deposit process). Nevertheless, the weight of the allegations and the Police Chief's findings certainly warranted a more in depth examination of past receipts, corresponding deposit slips, and income tax collections.

The auditors began by scanning the Village's receipt book for missing and/or voided income tax receipts. The auditors noted that numerous receipts were missing and several were voided by Ms. Cantrell (see **Exhibit A**).

Exhibit A

MECHANICSBURG, OHIO
DIVISION OF INCOME TAX

Official Receipt of Income Tax Paid N^o. 31215

PAYMENT ON

Year 2001 TAX \$ 375

Year 000-00-0000 PENALTY \$

Qtr. JOID INTEREST \$

NAME John Doe CASH TOTAL AMOUNT DUE \$ 375

ADDRESS 000 Smith Ln

Received by Mary Culp Date 10-24-02

TAX OFFICE	DATE	AMOUNT

During an interview, Ms. Cantrell indicated that many taxpayers opted to pay their taxes with cash. In the end, Ms. Cantrell admitted to destroying and/or voiding receipts issued for cash payments and taking the money instead of depositing it into the Village's bank account (i.e., skimming). When comparing the receipts with the corresponding deposit slip for particular dates, the auditors noted many deposit slips that did not include any cash. To further illustrate this scheme, **Exhibit B** compares a receipt tally and the corresponding deposit ticket for several income tax collections from November 2001. This example also illustrates how the auditors identified the amount of tax collections taken by Ms. Cantrell.

Auditors also identified instances in which the tax return reflected a payment received and the receipt book did not reflect a receipt issued to the taxpayer. There were other instances in which the taxpayer's copy of the receipt was missing, no replacement receipt was issued, the taxpayer's account either did not reflect a payment or did not exist, and the income tax payment was not deposited into the Village's bank account.

In the end, the auditors identified 66 receipts over the four-year period that were not deposited. A finding for recovery was issued against Ms. Cantrell for \$12,176 in income taxes collected but not deposited into the Village's bank account.

Unauthorized Withdrawals

The auditors also examined financial activity in the Village's Summer Celebration Account, which accounted for donations made by individuals for an annual fireworks celebration. Ms. Cantrell was responsible for depositing the donations. Further, both Ms. Cantrell and the Mayor were required to sign for any withdrawals. However, the Mayor told auditors that the only withdrawal should be for the fireworks display, which was typically made in two installments.

The auditors found that Ms. Cantrell used the Summer Celebration Account to "launder" stolen money, which mainly included income tax payments and employer payroll tax withholdings. She would deposit payroll remittances² from employers or income tax payments under the guise of a donation. She would then forge the Mayor's signature when the bank required both signatures on the withdrawal slip. The laundered cash was then deposited into her personal account. **Exhibit C** shows an example of an unauthorized withdrawal from the Village's Summer Celebration Account, where Ms. Cantrell forged the Mayor's signature. **Exhibit C** also shows the corresponding deposit slip, where Ms. Cantrell's deposited the monies into her personal bank account.

Exhibit C

SAVINGS WITHDRAWAL must be presented by the savings customer in person or by mail.

MECHANICSBURG SUMMER CELEBRATION
196 E SANDUSKY ST.
MECHANICSBURG, OH 43044

56-352/441
DATE 7-18-03

One Thousand Two Hundred ⁰⁰/₁₀₀ Dollars \$ 1200.08

DEDUCT ABOVE SUM FROM MY SAVINGS ACCOUNT
ON DEPOSIT WITH:

 **The Citizens National Bank**
of Urbana
MECHANICSBURG, OHIO 43044

Austin Cantrell
John Beutz
ADDRESS

² Amounts employers withhold from an employee's compensation which is due to the taxing district (e.g., village).

SUSAN L. CANTRELL 04-99
 [REDACTED]
 [REDACTED]

CASH
 56-353441

DATE 7-18-03
 DEPOSITS MAY NOT BE AVAILABLE FOR IMMEDIATE WITHDRAWAL

DOCUMENT # 509
 TRANSIT # 207
 497201
 LESS CASH RECEIVED

Deposit

NET DEPOSIT \$

CHAMPAIGN NATIONAL BANK
 AND TRUST
 "CELEBRATING 150 OF YEARS OF SERVICE"
 1851-2001

DEPOSIT TICKET

650.
 550.08
 7/18/03
 1200.08
 100.
 1100.08
 110008

[REDACTED] [REDACTED]

The auditors identified \$38,352 in unauthorized withdrawals by Ms. Cantrell from the Summer Celebration Account. Of the \$38,352, the auditors identified 40 instances in which Ms. Cantrell deposited \$31,590 into her personal account. Furthermore, while reviewing activity in Ms. Cantrell's personal account, the auditors found that Ms. Cantrell had forged 20 Village checks totaling \$15,228 payable to various Village vendors. Ms. Cantrell deposited the forged checks directly into her personal account.

In the end, Ms. Cantrell confessed to making numerous withdrawals from the Village fireworks account and placing the funds in her own personal bank account. She also confessed to a number of other schemes to divert public funds for her own personal use. The investigation led to a 10-count indictment against Ms. Cantrell for defrauding the Village out of more than \$80,000. Ms. Cantrell pleaded guilty to 5 counts of theft in office, 3 counts of money laundering, and 2 counts of tampering with records. She was sentenced to 12 and one half years in prison. She was also fined \$1,000 and ordered to pay back all the funds she stole from the various Village accounts. When asked where the money went, Ms. Cantrell said, "I took money everyway I could from the Village. I just bought normal stuff, clothes, whatever. I don't gamble or anything." A review of the activity in Ms. Cantrell's account revealed that the stolen money was spent on Wal-Mart purchases, lottery and convenience store purchases, bingo, and bank overdraft charges.

Lessons Learned from Mechanicsburg

There are many lessons that can be learned from the case involving Ms. Cantrell and the Village of Mechanicsburg. The special audit noted several internal control weaknesses and made the following recommendations for improved fiscal oversight:

- Segregate duties for receipting, depositing, and posting taxpayer payments.
- Perform reviews of adjustments entered in the Village computer system for validity and accuracy.

- Perform reviews of receipts issued to the daily deposits to ensure all monies collected are deposited.
- Review voided receipts and carbon copies to ensure all copies are valid and accurate.
- Establish and implement a records retention policy to ensure Village records are properly maintained.
- Establish a special revenue fund to account for donations and related payments for the annual fireworks display and to close existing separate savings account, thereby eliminating the opportunity for unauthorized withdrawals.

The special audit further recommended that management should regularly review endorsements on checks returned by the bank to ensure they are valid and make sure checks prepared have an invoice to support the payment. The check should also be completed prior to signing. Finally, if a segregated account cannot be established, management should review the activity on a regular basis to identify unusual deposits or expenditures.

Ms. Cantrell was engaged in a number of fraud types as defined by the ACFE survey, which was featured in the last issue of *Best Practices*. She was skimming Village funds by taking income tax payments made in cash before they were formally recorded in the Village's books. She was involved in check tampering by forging the Mayor's signature and by forging checks to various vendors. Ms. Cantrell also went to great lengths to cover up her crime by laundering stolen money through a separate account and by making manual adjustments to a computer system designed to track income tax payments.

Further, the case echoes many of the aforementioned findings from the ACFE Survey. For example, the fraud occurred in a small organization – the Village of Mechanicsburg employs fewer than 100 employees. Also consistent with the ACFE findings, Ms. Cantrell was a first-time offender and her fraudulent activity was detected through a tip. As Village Clerk Treasurer and Income Tax Administrator, Ms. Cantrell had a significant level of authority within the Village, which enabled her to steal a relatively large amount of taxpayer dollars. With proper controls and other preventative measures in place, however, the Village may have been able to deter Ms. Cantrell from committing fraud in the first place. Even if they were ineffective as a deterrent, the controls would have likely enabled other Village officials to detect the fraud more expeditiously.

Words of Wisdom

The following quote was taken from President Ronald Reagan's farewell address as he spoke of the changing relations between the United States and the Soviet Union in a post Cold War environment.

"It's still trust, but verify. It's still play, but cut the cards. It's still watch closely. And don't be afraid to see what you see."

- President Ronald Reagan (1989)

In the context of workplace fraud, the quote nicely captures the attitude management must have for an organization to effectively provide services while protecting itself from fraud. Governments need to stay active and remain cognizant of those areas that pose the greatest risk. If an organization's fraud awareness and prevention programs are perceived to be active and known to everyone in the organization, it is less likely someone will be bold enough to test the system and commit fraud.

The Tips Page

Use of Estate Tax

- Local governments often receive estate tax revenue that may include estimated tax payments. Governments should use caution when appropriating and expending these monies because portions may need to be refunded when estates are ultimately settled. The AOS recommends that local governments appropriate estate taxes based on historical averages (or some other conservative approach), due to the unreliable and unpredictable nature of this revenue source.

Taxable Fringe Benefits

- Governments often afford their employees fringe benefits in addition to their salaries/wages. For example, a government may allow an employee to use a government-owned vehicle or cell phone for personal use, which is considered a taxable fringe benefit (with some exceptions). Many of these fringe benefits are considered taxable by the Internal Revenue Service (IRS). As such, government fiscal officers should be aware of the IRS regulations surrounding taxable fringe benefits when preparing employee W-2 forms. The IRS has developed a helpful guide to assist employers in determining the taxability of various fringe benefits. To access the guide, visit http://www.irs.gov/pub/irs-tege/fringe_bnft_flgsg.pdf.

Additionally, Tracy Jemison (Geauga County Auditor) and Jackie McKee (Holmes County Auditor) developed affidavit forms that enable employees to report their taxable benefits as they relate to personal cellular phone and vehicle use, as well as clothing and meal allowances. If you would like to develop similar affidavit forms to facilitate the employee reporting process, you may access the Holmes County forms by visiting www.auditor.state.oh.us/publications/bestpractices/holmes.pdf (**Note:** The AOS strongly recommends that governments consult their legal counsel should they choose to develop such affidavits.)

Office of Township Clerk – Renamed; Duties Remain Same

- In accordance with SB 107, which was signed into law on September 15, 2005, the office of township “clerk” is to be referred to as township “fiscal officer.” This change takes effect on December 20, 2005. However, there was no change in duties for the newly named position of township fiscal officer from those statutory duties of township clerk.

Coming Up in the Next Issue of

BEST Practices

In the next issue of *Best Practices*, we will provide guidance on disaster recovery planning and how governments can best prepare themselves in the event that a catastrophic loss disables operations. We will also provide guidance on how governments should prepare their federal schedules.

If you like this publication and if you think it will be of help to you, please contact us at (800) 282-0370 or email bestpractices@auditor.state.oh.us and let us know. If there are other areas in the audit arena you wish us to highlight or if you have any comments, concerns, or questions, please let us know. Your opinions are very important to us.



**AUDITOR OF STATE
BETTY MONTGOMERY
88E. BROAD ST., 5TH FLOOR
COLUMBUS, OH 43215**