

POCKETED PAYMENTS:

Preventing the theft of incoming funds

Rogue employees have exploited weak internal controls to steal millions in customer payments from Ohio's local governments. Identifying and addressing vulnerabilities in the collection process is critical to ensuring fees and other funds make it to the bank.



Dave Yost
Ohio Auditor of State

Dave Yost
Ohio Auditor of State

88 E. Broad St.
Columbus, OH 43215
800-282-0370
614-466-4490
www.ohioauditor.gov

Cover photo illustration:
Photo by Ohio Auditor of
State's office



Dave Yost
Ohio Auditor of State

SPECIAL REPORT

A message from the Auditor



Every day in Ohio, thousands of taxpayers give cash to a government employee responsible for accepting payments for fines, fees, utilities, event tickets and many other things.

Those dollars too often end up in the pockets and bank accounts of the clerks accepting payment and not the schools, townships, libraries and other governmental entities where they belong. As Auditor of State, I see firsthand how frequently these dollars don't make it to their intended destination. The impact on Ohio's communities during the past 10 years has been significant: \$3.4 million in missing payments, much of it linked to theft.

Our review showed that time and again, rogue employees have successfully robbed governments because they were entrusted with total, unchecked control over fiscal operations. It's time for more administrators to take up shields and involve themselves in the defense of their financial resources.

Because of the magnitude of the losses, and because drastically reducing this type of theft is eminently achievable, my team assembled this report to draw attention to the problem and provide recommendations for closing the loopholes that allow for this type of theft to occur.

The key to protecting payments from being pocketed is to establish checks and balances on the money and to establish clear processes for how payments will be received and documented. And Ohioans can help by demanding a receipt for any cash payment they make to a local government.

It is, after all, your money.

Sincerely,

A handwritten signature in blue ink that reads "Dave Yost".

Dave Yost

Introduction

The bridge between a customer’s payment of a government fee and the money being deposited into a government bank account too often is left unguarded. With revenue being the lifeblood of any government, public officials cannot afford to overlook vulnerabilities in the handling of incoming funds.

Most employees on the fiscal side of operations are honest, hard-working individuals. However, a small percentage of deceitful workers have exploited this process for their own benefit. They succeed temporarily because of their access to the system and knowledge of its inner workings – but also because no one is watching.



In the past decade, auditors have identified more than \$3.4 million¹ worth of incoming payments that never made it into the government accounts. The missing money involved at least 77 local governments and school districts. While not all of these cases were definitively criminal, 53 employees at these entities were convicted of theft.

“For an unscrupulous employee, nothing can be more tempting than a continuous stream of cash passing through their fingers,” Auditor Yost said. “The risks are apparent, and it’s up to Ohio’s local government officials to take the necessary precautions to avoid falling victim.”

Local government administrators often are exceptionally knowledgeable about the successful operations of their entities, but many lack the same degree of expertise when it comes to financial processes. As a result, some officials feel more comfortable assigning full control of these duties to fiscal personnel,

¹ This total is based on figures listed in audit summaries of findings for recovery. Because it is not a requirement that summaries note when the theft or loss of funds involves incoming payments, this total may not be comprehensive.



who are then subjected to little oversight. This is an environment ripe for theft.

Before local government leaders can shut the window of opportunity on thieves, they must first understand the safest procedures for processing incoming funds. This report provides an overview of these steps and uses real-world examples to highlight weaknesses and ways to address them.

Knowledge is essential to prevent fraud. It is important that local government leaders remember they have a right – and duty – to ask questions of fiscal personnel whenever confusion or concerns arise. If further guidance is necessary, the Auditor of State’s office stands ready to help.

The thief behind the counter

The Auditor of State's office has linked 20 of the 77 instances of missing payments in the past decade to utility transactions. More are under review.



As of the release of this report, 15 convictions have resulted from those 20 cases. Each of the confirmed thefts was committed by one or more employees involved in the handling of incoming funds, usually a utility clerk or fiscal officer.

Still, the theft of incoming funds is not limited to utility departments. Auditors also have tied a substantial number of similar incidents to employees at other governments and school districts, such as court clerks, secretaries and school lunchroom employees. Regardless of the entity involved, this type of theft is most commonly committed by cashier-level employees who deal directly with customers over the counter.

In some situations, thousands of dollars can pass through the hands of one of these employees on any given day, creating the opportunity for theft.

"The nature of these jobs requires some employees to confront temptation on a daily basis," Auditor Yost said. "Weak oversight can help turn temptation into intent, so the obvious solution is to nip this in the bud with solid internal controls."

The majority of culprits also share a common characteristic of knowing the strengths and weaknesses of their systems better than anyone else in their organization. Accordingly, their level of familiarity helps them recognize flaws and craft schemes to exploit them.

These employees are usually mindful of the review systems in place and can maneuver around them. Thieves tend to target cash because it is more difficult to trace than other forms of payment such as checks and credit cards.

To view an interactive map of all the entities for which the Auditor's office has issued findings for recovery, go to the Auditor's website at:

www.ohioauditor.gov/fraud/pocketed_payments_map.html



They are rarely impulsive, often spending a great deal of time developing a plan to cover their tracks, experts say. Historically, they test the waters by stealing a few dollars here and there to see what they can get away with. If their theft passes through the government's internal control unnoticed, employees tend to up the ante.

The motivation for these individuals varies from case to case, but often involves a desire to enhance their lifestyle by living beyond their means. In other cases, thieves steal to feed vices such as a gambling or drug addiction. Still, others succumb to pressure to pay off expensive bills or to make ends meet.



No government is immune to theft

Members of the Auditor of State’s office have helped investigate stolen revenue at almost every level of local government in Ohio.

The irrefutable conclusion from past audit work is that no government is immune to this type of theft. Some governments, however, are more vulnerable than others because of deficiencies in finances, staffing and training.

“Governments operating on a shoestring budget don’t have the luxury of a large staff to divvy up financial responsibilities,” Auditor Yost said. “Administrators in these situations need to take on a greater watchdog role to promote integrity and accountability on the cash side of operations.”

Villages, which commonly have only one or two fiscal employees, account for 22 of the 77 (29%) entities where auditors have identified stolen or misplaced payments in the past decade. Villages also see a high volume of utility payments, which is the most frequently targeted form of incoming revenue.

For small communities such as villages, finding someone with the expertise and desire to serve as a fiscal officer can prove challenging. In some situations, these governments end up with someone who is well intentioned but lacks the knowledge to do the job properly.

On the other hand, in a worst-case scenario, communities unknowingly have chosen ill-intentioned individuals who are skilled enough to cause harm and hide their misdeeds from others. The damage often occurs when they are given free reign over financial operations with little oversight from administrators such as village council members.

Second to villages, school districts have suffered at least 15 cases of stolen or missing revenue. Most

Entities with findings since 2007

Villages	22
School districts	15
Courts	8
Counties	7
Cities	6
Agricultural societies	3
Libraries	3
Health department	2
Sheriff’s departments	2
Townships	2
County treasurer’s office	2
Ambulance district	1
Charter school	1
Environmental services department	1
Park district	1
Water and sewer district	1

districts have a large number of cash collection points for students and parents to pay for field trips, dress down days, lunches, extracurricular activities and athletic event tickets – all of which have been targeted by thieves.

Unique to school districts, many of these collection points are usually manned by non-fiscal staff, such as teachers, secretaries and principals. In some cases, teachers in every classroom are expected to collect payments from students and prepare the funds for deposit.

Tracking these funds can be difficult for one school building, let alone for the multiple schools that can make up a district. Perceiving this weakness as an opportunity for theft, some employees have made off with tens of thousands of dollars before being caught.

Among the other entities with more than two cases of missing revenue are courts (8), counties (7), cities (6), agricultural societies (3) and libraries (3). Regardless of the type of government, all theft prevention comes down to sound internal controls.



Many methods, same result

Auditors and investigators over the years have exposed a wide range of tactics employed by dishonest workers to swipe incoming funds. Every approach varies to some degree, but most share a common element: the perpetrator devises a plan to conceal his or her misdeeds after the dollars vanish.

Auditors are frequently tasked with unraveling complex schemes that require careful planning and maneuvering on the part of the perpetrator to avoid detection. What follows are some of the most common schemes reported in past audits, accompanied by safeguards local governments can institute to defend against adjusting journal entry, void and check-substitution schemes.





Adjusting Journal Entry Scheme

OVERVIEW

Certain situations require changes to the balance on a customer's account to correct billing errors such as inaccurate meter readings or erroneous late fees. Employees typically remedy these mistakes by creating entries in the entity's billing system, called non-cash adjustments, which either increase or decrease the account balance to the proper amount owed.

In an adjusting journal entry scheme, an employee who receives a customer's payment does not record the transaction as a payment in the billing system. Instead, the employee pockets the cash and creates a fraudulent adjustment to lower the customer's account balance back to zero. In some cases, employees are more discreet and steal only part of a customer's payment, adjusting the account balance only enough to offset the stolen amount.

The use of this scheme ensures the entity's cash journal balances at the end of the day and leaves little, if any, trace of the transaction to the untrained eye. The tactic also prevents the victimized customer from receiving a delinquent payment letter because his or her account balance shows no amount owed.

VILLAGE OF RIPLEY

Citizens of the Village of Ripley probably never considered the possibility their utility payments were heading straight into the pockets of the village's utility clerk, Katherine Lang.

Capitalizing on the village's weak internal controls, Lang evaded detection by employing an adjusting journal entry scheme. By the time the jig was up, she had drained nearly \$1 million from the small community of roughly 1,750 people in southeast Brown County.

Village officials became suspicious of Lang's work after a review of utility account adjustments revealed various unusual, unexplained adjustments to utility customer accounts – a red flag for theft.

Lang was in charge of the entire utility payment collection process, which included creating customer accounts, collecting and posting payments, and making deposits. Another red flag for village officials was the fact that she stored the adjustment records in a locked drawer in her desk, accessible only to her.

The village notified the Auditor of State's office, which launched a special audit into the matter. During a thorough examination of the village's records, auditors determined that Lang covered up \$683,390 of her \$952,618 theft by creating 556 account adjustments in the village's billing system. None of the adjustments were authorized by village officials or supported by documentation.

Lang was indicted in 2010 on three counts of theft in office and seven counts of tampering with records. She pleaded guilty the following year to the trio of theft in office counts in exchange for the state's dismissal of the remaining seven charges. The court sentenced Lang to 13 years in prison, which she is currently serving, and ordered her to pay nearly \$1.1 million in restitution and audit costs.

FROM THE VILLAGE OF RIPLEY AUDIT

“Documentation maintained should explain the reason for the adjustment and reflect supervisory approval prior to posting the adjustment to the utility system.”



123rf.com

PREVENTION

One of the simplest, most common-sense safeguards local governments can implement to defend against this scheme is a routine review of adjustment reports. Most modern billing systems are capable of automatically generating these reports, which list every adjustment entered into the system.

This review practice, which led to Lang's downfall, allows an entity's oversight authority (often members of a board or council) to easily spot suspicious entries that may be an indication of theft. Excessive adjustments are a red flag, as are adjustments that lack corresponding supervisor approval or valid explanations for the adjustments.

To ensure this control is effective, local governments should require all employees to obtain supervisor approval prior to making an adjustment. Additionally, employees should retain detailed documentation to support the approval and the need for an adjustment.

"Thieves prefer to work in the shadows,"

Auditor Yost said. "When local governments demand a complete record of every transaction or adjustment, they force schemers to operate in the daylight, leaving a clear paper trail to their doorstep if they choose to strike."

When possible, governments also should split fiscal duties among employees, but should limit those authorized to enter account adjustments to a few individuals. Katherine Lang's complete control over the billing process was a key factor in her ability to evade detection.

For smaller governments where separation of duties may not be an option, requirements for employees to provide customers with receipts or signs posted that encourage customers to obtain receipts can serve as alternative deterrents.

A tempted employee will likely think twice about stealing a \$100 payment with a fraudulent adjustment if the customer expects a receipt and if the employee knows administrators check adjustment reports.



Void Scheme

OVERVIEW

Most people probably associate cash registers with the retail and food service industries, but they also are a common tool for many local governments. As many entities transition to web-based payment options, cash registers still prove useful for citizens who prefer to pay in person for utility payments, title and permit fees, and other public services.

Wherever cash registers are present, there also exists a need to cancel erroneous payments through voids. When this procedure goes unchecked, local government dollars are left vulnerable to thieves who characteristically seek opportunities for fast money and an easy way to sweep their crimes under the rug. For some of these criminals, a void scheme fits the bill.

The tactic works by manipulating an entity's paper trail to appear as if a customer's payment was refunded. After a customer makes a payment, the offending employee re-enters the billing system and voids the transaction. This maneuver shows the funds exiting the entity's system, allowing the employee to pocket the customer's payment with little evidence left on the government's side of the transaction.

However, this scheme is risky when it comes to the customer's side of the transaction because all it takes to blow the lid off the employee's ploy is one victimized customer who realizes his or her permit, title or utility payment is invalid despite having evidence in the form of a receipt. This was exactly the case during a recent audit of Montgomery County.



123rf.com

MONTGOMERY COUNTY

A concerned customer with a utility receipt was all it took to expose a deceitful employee who used a void scheme to steal thousands of dollars from Montgomery County.

"Incompetent oversight allowed the customers' trash fees to become this employee's treasure," Auditor Yost said in 2016, speaking of the now-convicted former customer service specialist who preyed on customer payments.

During a routine financial audit of Montgomery County for fiscal year 2014, auditors quickly spotted a discrepancy: incoming dollars from customer solid waste payments did not match the amounts transferred to the county treasurer's office.

Auditors brought the matter to the attention of the county and subsequently learned of a customer who received a water shut-off notice despite having a receipt to prove he paid his bill on time with cash.

The Auditor's office elevated the review to a special audit as investigators focused their attention on Rozalin Smith, the utility employee who collected the customer's payment – the same person

POCKETED PAYMENTS | THE SCHEMES



involved in the solid waste payment discrepancy.

Smith's responsibilities included receiving utility payments and crediting them to customer accounts. Auditors identified ten transactions totaling \$2,092 where Smith credited the funds to the customer's account before voiding the payments and keeping the cash for her personal use. She stole an additional \$12,987 through other means.

Following the initial customer complaint, the county pulled surveillance footage that showed Smith receiving the customer's payment and then voiding the transaction. When questioned, Smith

details for every void. Local governments can take full advantage of this feature by requiring employees to include with each void an explanation of why the cancellation was necessary, as well as documentation of the supervisor approval.

Using this report, a supervisor can simply scan the list of voids to verify that each entry matches up with a corresponding explanation and approval from management. A supervisor should follow up on any voids that lack the required supporting documentation.

As in the case of Montgomery County, a receipt



confessed to using a void scheme.

She pleaded guilty in December 2015 to one count of theft in office and was sentenced to five years of probation, 40 hours of community service and ordered to repay the stolen money.

PREVENTION

Of several ways to head off void schemes, perhaps the most effective defense is a requirement for employees to obtain prior approval from a supervisor for every voided payment. A smart thief will not create a fraudulent void if they are required to adhere to a strict review process right off the bat.

As a secondary control, entities using modern billing systems can generate reports that list the

is sometimes all it takes to stop a thief. It makes sense then to urge customers to obtain and save their receipts as proof of their payments. Entities can do this by first adopting policies requiring employees to provide each customer with a copy of their receipt.

Governments also can post signs that encourage customers to obtain and save receipts for every transaction. For example, a sign posted in an area where payments are collected could read: "Please save your receipt. This will help ensure your payment is properly credited to your account."

A dishonest employee will be far less likely to steal from an incoming payment if the customer's receipt makes it impossible to erase the paper trail.



Check-Substitution Scheme

OVERVIEW

Local governments occasionally receive atypical revenue in the form of mailed checks for rebates, insurance claims and other one-off payments. These unexpected checks are a welcome sight for thieves looking for fast money and an easy cover-up.

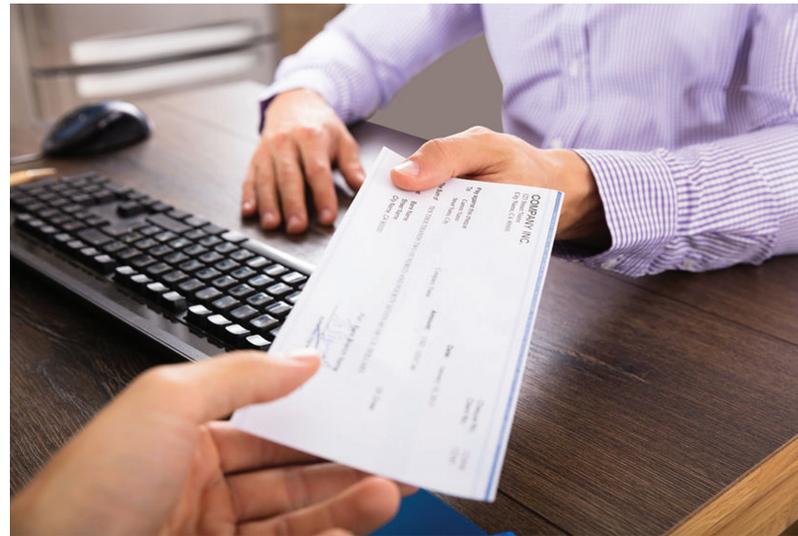
In a check-substitution scheme, an employee with access to the entity's mail stumbles upon one of these checks and sets it aside until it is time to strike. For example, say a scheming fiscal officer receives a letter that contains a \$100 rebate check for an equipment purchase. Instead of recording the check in the accounting system, the fiscal officer discretely slides the check into a desk drawer and waits for a few customers to make cash payments.

At this point, the perpetrator must wait for enough customer cash payments to accumulate to a sum that covers the check amount and avoids drawing attention.

Then, in an act of financial sleight of hand, the fiscal officer substitutes the rebate check for an equal value of \$100 in cash from the customer payments. This tactic ensures the sum of the revenue listed on the deposit slip agrees with the actual amount of cash and checks on hand, without raising suspicion to the fact that \$100 in cash was just stolen.

However, this trick does usually leave a noticeable trace for those who know where to look. Deposit slips list the makeup, or tender type, of each deposit by specifying the total amount of cash, as well as the amount and unique number of each check. The substitution of a check for cash creates inconsistencies between the breakdown listed on the deposit slip, the actual amount of cash and checks on hand, and the amounts recorded in the accounting system.

For example, a deposit slip that lists \$500 in cash will no longer match the actual amount of cash inside the bank bag if someone substitutes a \$100 check. While the overall amount recorded on the deposit slip is still accurate, only \$400



123rf.com

in cash is present in the bank bag. Additionally, the bank bag now contains an extra \$100 check that is absent from the deposit slip and the accounting system.

PIKE COUNTY CLERK OF COURTS

Irregularities between court collections and deposits sparked a special audit into the Pike County Clerk of Courts office, which uncovered a check-substitution scheme that successfully robbed the entity of more than \$1,700.

The Clerk of Courts office requested the Auditor's assistance with the matter in January 2014 after noticing deposit slips did not always agree with daily collection reports. The clerk's office had already placed Chief Deputy Clerk Darla Smith on administrative leave after suspecting her of wrongdoing. Shortly thereafter, employees discovered old checks on Smith's desk that she never deposited.

In addition to making bank deposits, Smith was solely responsible for processing all garnish-



ment (court-ordered wage withholdings) and sheriff foreclosure checks. She also was in charge of performing the office’s bank account reconciliations, which were not reviewed by anyone else.

“Unchecked authority combined with opportunity can often spell disaster,” Auditor Yost said at the conclusion of the audit. “The Pike County Clerk of Courts office should take steps to ensure that no one has this kind of free rein again.”

During a review of deposit records, auditors identified 369 bank deposits totaling \$568,066 made during a 375-day period. However, supporting collection documentation suggested the clerk’s office actually received \$572,665 during the period – a variance of \$4,599.

Upon further inspection, auditors identified three garnishment checks totaling \$1,470 that were deposited in the office’s bank account but were absent from collection records.

“We concluded the checks were substituted for cash (payments) collected and recorded but not deposited because the daily receipts recorded and deposited agreed in total but did not agree by tender type,” auditors wrote.

A fourth check made out to the court for \$235 also was substituted for cash. Smith used different tactics to steal thousands of dollars more from court collections. She pleaded guilty in 2015 to one count of theft in office and was sentenced to three years of probation and ordered to pay restitution and audit costs.

PREVENTION

An essential preventive measure to block check-substitution schemes is a thorough review of all deposits before taking the funds to the bank. Someone other than the employee(s) who collects payments should check the contents of the bank bag against the deposit slip to ensure

The substitution of a check for cash creates inconsistencies between the breakdown listed on the deposit slip, the actual amount of cash and checks on hand, and the amounts recorded in the accounting system.

there are no discrepancies in the amounts or tender types listed.

Whenever possible, responsibilities should be divided up among several employees to prevent a single individual from manipulating the entire process. In the case of Pike County, Darla Smith was able to successfully pull off her scheme because of her control over multiple steps in the process and because there was almost no oversight. Ideally, more than one employee should be involved in the preparation of deposits and

their trip to the bank.

Along with splitting duties, governments should consider requiring employees to take vacations and have other employees cover their tasks. Fraudsters often feel the need to work every day because their absence leaves them vulnerable to detection. This policy serves as a theft deterrent by requiring a potential thief to disrupt their daily work routine and have someone else temporarily assume his or her responsibilities.

Officials also should consider which employees have access to the mail and therefore have the ability to intercept a check. If possible, have more than one employee open the mail. Those who perform this task should not be responsible for taking funds to the bank because of the opportunity to tamper with deposits.

Additionally, governments should make deposits every day funds are collected to comply with state law. Doing so prevents large sums of cash from accumulating, making it harder for someone to substitute a check for cash without drawing attention.

Finally, governments should establish policies requiring employees to maintain supporting documentation for every deposit, including copies of deposit slips. This practice serves as a deterrent and enables supervisors and auditors to track the movement of funds if a theft is suspected.

Fairview Park City School District

Suspicious behavior from a Cuyahoga County high school principal sparked an internal investigation and special audit, which revealed a theft of more than \$59,000 from school proceeds.

Fairview High School principal Kevin Liptrap handled the deposit of revenue from athletic event ticket sales and other student activities, but he persistently failed to submit required supporting documentation to the district treasurer. When questioned by district officials, Liptrap was reluctant to cooperate and unable to provide the records.

Another puzzling question was why Liptrap, who previously served as district athletic director, continued to handle athletic event admissions after his promotion to principal when the responsibility should have gone to the new athletic director.

Upon further inspection, the district noticed a continuous



decline in cash collections over the prior four years. During a special audit into the matter, the Auditor of State's office discovered that Liptrap took \$51,579 worth of check payments for student participation fees and substituted the checks in deposits to hide his theft of cash ticket revenue. (This tactic, called a check-substitution scheme, is explained on Page 12 of this report.)

The audit also revealed that no deposits were made for 93 ticketed athletic events. Auditors determined that at least \$6,168 in revenue was unaccounted for from 48 of those events, but incomplete records prevented auditors from tracking proceeds from the remaining 45 events.

Liptrap confessed to investigators in 2010 that he stole the funds from the district. In 2012, he pleaded guilty to a charge of theft in office and was sentenced to five years of probation, 90 days in a halfway house and was ordered to pay \$122,142 in restitution and fees, including audit costs.



City of Marion

A former utility department supervisor drained tens of thousands of dollars from the City of Marion (Marion County), using her position of authority to camouflage her misdeeds for more than 3½ years.

From 2011 through most of 2014, Brenda Nwsosu pocketed \$17,375 from 71 customer payments. Nwsosu's level of access, along with a weak system of internal controls, provided the opportunity for her to manipulate account balances so it appeared as if all was normal.

She neglected to credit another \$16,901 in proceeds from 25 incoming checks to the appropriate accounts, instead posting the funds to



unrelated accounts to hide that she was stealing cash.

"You can only cover up your tracks for so long," Auditor Yost said in 2016. "Sooner or later, a vigilant citizen or public employee will pick up on the trail."

Nwsosu pleaded guilty to theft in office in April 2015 and was sentenced to 18 months in prison and ordered to pay \$34,276 in restitution.

Since the theft was detected, the city has implemented several fraud-prevention practices including unannounced audits of cash drawers and improved anti-fraud education for employees.

Village of Arlington Heights Mayor's Court

A mother-daughter duo siphoned off more than \$260,000 from the Arlington Heights Mayor's Court (Hamilton County) and masked their misdeeds with sophisticated tactics.

Court Clerk Donna Covert and her daughter Deputy Court Clerk Laura Jarvis staffed the counter at the Arlington Heights Mayor's Court, where they processed payments for fines, court costs and bonds. Covert served as her daughter's supervisor.

After noticing a shortage between court collections and deposits, the village requested assistance from the Auditor of State's office in 2010. A special audit determined that \$262,297 worth of incoming funds never made it to the court's bank account.

Auditors zeroed in on the pair of clerks and obtained access to their personal bank account records to check for



unusual activity. The review discovered \$29,842 in cash deposited into Covert's bank account and another \$19,398 in cash deposited in Jarvis' account.

During interviews with investigators from the Auditor's office, the clerks admitted to stealing the money from the court and depositing some of it into their bank accounts.

The clerks used a variety of tactics to conceal their theft, including substituting checks for cash, failing to issue customer receipts and neglecting to record transactions in the court's billing system.

Pointing to a lax system of internal controls, Auditor Yost said the pair "took advantage of the situation, and in this case, taxpayers were the victims."

Covert pleaded guilty to one count of theft in office in 2013 and was sentenced to one year in prison. Jarvis pleaded guilty to theft in office in 2015 and was sentenced to nine months in prison. Both were ordered to repay the stolen money.



Hillsboro City School District

At the Hillsboro City School District in Highland County, an elementary school lunchroom employee doctored financial records to conceal her theft of \$6,548 in student lunch money.

Pam Ward, the school's head cook, was responsible for reviewing daily deposit reports and depositing the collected funds into the bank, along with a deposit slip from the school's billing system.

An audit of the district discovered that Ward deposited only \$38,406 of the \$44,954 the school took in from 71 days of sales during 2010. Auditors determined that 58 of the school's daily deposits did not agree with the revenue logged in the school's computer system.



A closer inspection of the records submitted by Ward to the treasurer revealed that reports were altered to agree with the amounts deposited into the bank. Also, the cash collection amounts reported to the Ohio Department of Education were inconsistent with district records and were understated to agree with the amounts that Ward deposited.

"Because of the actions of one, the Hillsboro City Schools are left with the tab for more than 2,900 student lunches," Auditor Yost said at the time.

Ward pleaded guilty in 2012 to one charge of theft and was sentenced to five years of probation and ordered to pay restitution to the school district.



Best Practices

It is unrealistic to believe a supervisor can look over the shoulder of every employee who processes incoming dollars. But a variety of proven internal controls exist to help governments of all sizes and budgets narrow the opportunity for theft.

Government leaders should periodically meet with fiscal personnel to assess their procedures. During this review, administrators should request a walkthrough of the process and determine whether employees adhere closely to the steps listed. This discussion also should include an explanation of each control mechanism in place to deter and detect theft.

With a better understanding of the environment, leaders can examine cash collection points, identify holes in the process and create stronger controls to plug them. After creating or updating a plan of action, administrators should cement the safeguards in a formal written policy. Each employee should be given a copy of the policy and be required to sign an attestation that they have read and understood it. Still, policies are useless if they are not enforced, so administrators should conduct routine checks to ensure employees are in compliance.





Best Practices

The following are descriptions of the general steps fiscal personnel should take when receiving incoming payments and preparing the funds for deposit. These steps may vary slightly depending on the size and type of entity. Also included are explanations of common vulnerabilities found in past audits, as well as safeguards to help local governments reinforce these weaknesses.

It's critical to remember that no lone employee should perform these steps from start to finish. Whenever possible, duties should be divided up among multiple employees to deter potential thieves.

1

Collect payment and issue a duplicate receipt to the customer

2

Secure the funds

3

Post the payment to the billing and accounting systems

4

Reconcile, or balance, the money on hand with documented amount

5

Prepare a deposit slip and deposit funds with the bank daily

STEP 1: Collect payment and issue a duplicate receipt to the customer

IN PRACTICE

When a clerk or other fiscal employee initiates a transaction with a customer, the employee should verify that the sum of the incoming cash or check agrees with the total amount owed by the customer. The employee then should issue a duplicate receipt to the customer and maintain the entity's copy with its records.

WEAKNESSES

Potential weaknesses arise in the handling of duplicate receipts, which are an essential component of supporting documentation for local governments and their clients. Given their importance, dishonest employees may seek opportunities to omit duplicate receipts from an entity's records to eliminate a paper trail. Others may avoid issuing receipts at all.

Another danger exists for governments that still issue manual, hand-written receipts. This practice is risky because thieves can remove or destroy sections of receipts to conceal theft. Regardless of whether a receipt system is automated or manual, pre-numbered receipts should be used.

SAFEGUARDS

Local governments should adopt policies requiring fiscal personnel to provide original receipts to customers and maintain the duplicate of each one in the entity's records. Duplicate receipts also should make note of the tender type – cash or check – presented for payment. All other supporting documentation for the transaction should be archived as well.

Auditors also recommend local governments implement unannounced cash counts to their systems of internal controls. The surprise nature of these reviews makes them effective in deterring would-be thieves.

Additionally, entities can post signs in areas where payments are collected that encourage customers to obtain receipts. Also, local governments that still issue manual receipts should transition to automated receipt systems – when financially viable – to reduce the risk of fraud.



Best Practices

- 1

Collect payment and issue a duplicate receipt to the customer
- 2

Secure the funds
- 3

Post the payment to the billing and accounting systems
- 4

Reconcile, or balance, the money on hand with the documented amount
- 5

Prepare a deposit slip and deposit funds with the bank daily

STEP 2: Secure the funds

IN PRACTICE

After the transaction is complete, an employee should secure the incoming cash or check in a cash register or cash box and ensure it is locked when left unattended. Next, the money should be moved to a locked safe and inserted into a bank bag prior to deposit.

WEAKNESSES

A failure to secure incoming funds creates a major vulnerability. Audits have found that some fiscal employees do not use lockable containers or bank bags, but instead stick the money in unsecure locations such as desk drawers. Doing so exposes the dollars to easy theft and makes it difficult to trace the funds if they go missing.

SAFEGUARDS

Local governments should designate secure storage locations for incoming funds, such as locked cash boxes and safes, where employees can store payments prior to deposit. A supervisor should restrict access to this location to a limited number of employees and monitor it with an access log or security camera. This serves as a deterrent to would-be thieves and aids in tracing funds if they go missing.

An additional step local governments can take to protect themselves against losses is to require surety bonds for cashiers and anyone else involved in this process. In the event of a theft, a surety bond can facilitate compensation for the financial damages experienced by the entity.

STEP 3: Post the payment to the billing and accounting systems

IN PRACTICE

After securing the funds, an employee should update the entity's billing and accounting systems to reflect the incoming payment. This is accomplished by locating the customer's account in the billing system and updating the balance accordingly. A corresponding entry should be made in the accounting system to account for the revenue.

A billing system serves to track the status of all customer accounts for a specific billing activity, such as utility payments. An accounting system records financial information, including revenue, from all of a local government's activities and those of its subdivisions. These systems are sometimes linked, enabling updates to the billing system to transmit automatically to the accounting system.

WEAKNESSES

As discussed earlier in this report, dishonest employees have manipu-



Best Practices

1

Collect payment and issue a duplicate receipt to the customer

2

Secure the funds

3

Post the payment to the billing and accounting systems

4

Reconcile, or balance, the money on hand with the documented amount

5

Prepare a deposit slip and deposit funds with the bank daily

lated this step on numerous occasions to conceal theft. Without proper controls in place, devious employees can easily create fraudulent adjustments to customer account balances to make it appear as if a transaction never occurred. This enables the employee to pocket the money without raising any red flags.

SAFEGUARDS

Local governments should require supervisor approval for all changes to customer account balances. Additionally, employees should maintain supporting documentation of the approval, as well as an explanation of why the change was necessary.

Government leaders should seek training on the use of review features in their accounting systems and regularly check adjustments for suspicious activity that could be a sign of theft.

STEP 4: Reconcile, or balance, the money on hand with the documented amount

IN PRACTICE

Fiscal personnel should prepare a collection report each day that includes the total documented amount of money received from customers. At least one employee, but preferably more, should remove the cash and checks from the secure location and count it to verify that the total is in agreement with the logged amount. Any unexplained variations could be a sign of theft and should be investigated. Employees should maintain documentation of all daily reconciliations with the entity's financial records.

WEAKNESSES

Thieves attempting to conceal theft have sometimes made this good control go bad by doctoring collection reports and other reconciliation forms to make the entity's books balance at the end of the day. In many of these cases, the perpetrator oversaw the entire collection and deposit process, and knew that no one was reviewing collection or reconciliation documents.

SAFEGUARDS

When possible, local governments should split this responsibility among multiple employees to dissuade those who may be tempted to forge collection or reconciliation records. This common-sense yet effective practice increases the likelihood of detecting honest mistakes and deceitful tricks.



Best Practices

1

Collect payment and issue a duplicate receipt to the customer

2

Secure the funds

3

Post the payment to the billing and accounting systems

4

Reconcile, or balance, the money on hand with the documented amount

5

Prepare a deposit slip and deposit funds with the bank daily

STEP 5: Prepare a deposit slip and deposit funds with the bank daily

IN PRACTICE

An employee should prepare a bank deposit slip specifying the sum of funds collected, as well as a breakdown of cash versus checks. The slip should include a listing of each check number and its amount. A copy of the deposit slip should be maintained with the entity's records.

A separate employee should transport the funds and deposit slip to the bank for deposit. Alternatively, some larger governments hire armored transport services to take the funds to the bank. This step should occur daily, as required by state law, with limited exceptions.

WEAKNESSES

Like reconciliation forms, deposit slips are susceptible to tampering where oversight is lax. Fiscal employees with control over all of these documents can easily doctor them to hide misdeeds if no one is watching.

This step also poses risks because the designated employee often has unchecked access to the money and is the last of the entity's employees to see the funds intact. Auditors have uncovered multiple cases where these employees deposit some, if not all, of the entity's collections into a personal bank account. Other times, employees have gone to the store instead of the bank and enjoyed a shopping spree at the expense of the government.

The timeline for deposit is another area for concern, as employees can intentionally delay deposits to make it increasingly difficult for supervisors to track the status of funds.

SAFEGUARDS

A critical control at this level is a requirement for employees to make timely deposits, ideally each day funds are received. Employees should maintain documentation of each deposit.

Local governments also should implement a review process to verify the accuracy of deposit slips before the funds are taken to the bank. Auditors recommend paying particular attention to the itemized list of checks. A discrepancy in the check listing could be an indication of a substitution scheme, which is explained on Page 12 of this report.

At the end of this process, a supervising authority should conduct a follow-up review to ensure the amounts deposited with the bank match the collection amounts listed on supporting documentation.

POCKETED PAYMENTS

Conclusion

Revenue fuels local government operations, but it also is a prime target for unscrupulous employees whose responsibilities include the collection, processing and deposit of incoming funds. Many of these employees possess the opportunity and knowledge to inflict financial harm if they succumb to the temptation that is often present on a daily basis. Local government leaders can minimize this risk by routinely evaluating their systems of internal controls and establishing additional defensive measures in policy whenever weaknesses come to light. For more information, or to report suspected fraud anonymously, visit FraudOhio.org.

POCKETED PAYMENTS | COLLECTED BUT NOT DEPOSITED

AUDITED ENTITY	COUNTY	UNDEPOSITED	CONVICTION	RELEASED	SUMMARY
Ashland County-City Health Dept.	Ashland	\$89,061	yes	2012	Assistant stole payments for health services
Ayersville Water and Sewer District	Defiance	\$61,593	no	2015	Missing utility payments; unexplained acct. adjustments
Bellaire Local School District	Belmont	\$1,800	no	2007	Missing student payments for cheerleading camp
Belmont County Juvenile Court	Belmont	\$19,910	yes	2009	Grant administrator stole restitution payments
Belmont Park District	Belmont	\$3,563	no	2015	Rental fees missing from deposits
Brown County Clerk of Courts	Brown	\$5,921	yes	2013	Clerk overcharged customers, skimmed excess amounts
Buckeye Local School District	Jefferson	\$45,271	yes	2007	High school secretary used check-substitution scheme
City of Franklin Municipal Court	Warren	\$2,203	no	2011	Multiple shortages in court collections and deposits
City of Marion	Marion	\$34,276	yes	2016	Utility supervisor stole cash with a check-substitution scheme
City of Martins Ferry	Belmont	\$32,414	yes	2014	Utility clerk stole from utility payments
City of Orrville	Wayne	\$9,021	yes	2010	Utility clerk used substitution scheme to steal cash
City of Springboro	Warren	\$2,088	no	2012	Payments missing from building and zoning department
City of Steubenville	Jefferson	\$3,538	no	2014	Missing income tax payments
City of Wellston	Jackson	\$2,702	no	2010	Utility payments were collected but not deposited
Clark County	Clark	\$8,368	no	2011	Missing concealed carry, background check payments
Claymont Public Library	Tuscarawas	\$1,775	yes	2010	Clerk treasurer stole from library payments
Clermont County General Health Dist.	Clermont	\$9,694	yes	2012	Secretary voided transactions to conceal theft of cash
Columbus City School District*	Franklin	\$53,106	yes	*	Student activity funds, ticket revenue not deposited
Coshocton County Sheriff's Office	Coshocton	\$31,290	yes	2013	Lieutenant stole from collection drawer
Defiance County	Defiance	\$17,222	yes	2011	Clerk used void scheme to steal from payments
Erie County Treasurer's Office	Erie	\$146,592	yes	2010	Deputy treasurer stole from collections
Fairfield County	Fairfield	\$855	yes	2016	Employee stole from cash collections stored in a vault
Fairview Park City School District	Cuyahoga	\$59,278	yes	2011	Principal/athletic director used check-substitution scheme
Franklin County Agricultural Society	Franklin	\$61,068	yes	2014	Treasurer stole from collections
Franklin Township	Richland	\$5,407	yes	2014	Fiscal officer stole from various collections
Hardin County Treasurer's Office	Hardin	\$22,302	yes	2008	Deputy treasurer used check-substitution scheme
Harrison County Juvenile Court	Harrison	\$4,915	yes	2011	Clerk stole from court payments
Hillsboro City School District	Highland	\$6,548	yes	2012	Head cook stole lunch money, changed records
Jersey Township	Licking	\$1,170	no	2017	Missing revenue from zoning, cemetery transactions
Kinsman Free Public Library	Trumbull	\$16,354	yes	2013	Fiscal officer stole library payments
Lucas County Clerk of Courts	Lucas	\$125,934	yes	2008	Bookkeeper stole from cash collections
Madison County	Madison	\$1,815	yes	2016	Probation officer stole from restitution payments
Montgomery County Environ. Serv.	Montgomery	\$15,079	yes	2016	Employee used void scheme to steal utility payments
North Union Local School District	Union	\$18,531	yes	2010	Secretary stole from student payments
Northwest Ambulance District	Ashtabula	\$735	no	2012	Missing membership, ambulance fees

POCKETED PAYMENTS | COLLECTED BUT NOT DEPOSITED

AUDITED ENTITY	COUNTY	UNDEPOSITED	CONVICTION	RELEASED	SUMMARY
Perrysburg Ex. Village School District	Wood	\$211,898	yes	2016	Clerk stole cash, checks from district
Pickaway County	Pickaway	\$18,659	yes	2008	Corporal stole concealed carry, background check payments
Pickerington Local School District	Fairfield	\$557	no	2017	Missing student payments, library fees
Pike County	Pike	\$1,280	no	2017	Collected cash child support payments not deposited
Pike County Clerk of Courts	Pike	\$6,840	yes	2014	Clerk used check-substitution scheme to steal cash
Putnam County Agricultural Society	Putnam	\$600	no	2017	Missing revenue from county fair tickets
Salem City School District	Columbiana	\$23,440	yes	2012	Secretary stole student tuition payments
Sandusky County Sheriff	Sandusky	\$25,500	yes	2008	Captain stole from cash collections
Southern Hills Career and Tech. Center	Brown	\$1,905	no	2008	Missing customer payment
Talawanda City School District	Butler	\$5,313	no	2017	Missing revenue from athletic event ticket sales
Village of Aberdeen	Brown	\$24,875	yes	2017	Fiscal officer stole utility, income tax payments
Village of Albany	Athens	\$200	no	2012	Missing utility payment
Village of Alger	Hardin	\$37,081	yes	2011	Fiscal officer stole from utility payments
Village of Arlington Hts. Mayor's Court	Hamilton	\$262,297	yes, 2	2013	Clerks used substitution scheme to steal court payments
Village of Barnesville	Belmont	\$1,050	yes	2016	Fiscal officer stole fees, income tax payments
Village of Bellaire	Belmont	\$18,125	yes	2012	Utility clerk stole from utility payments
Village of Bethel	Clermont	\$13,258	yes	2010	Clerk stole from cash payments
Village of Chauncey	Athens	\$471	no	2009	Missing utility payments
Village of Germantown	Montgomery	\$9,454	no	2011	Missing utility payments; unexplained account adjustments
Village of Golf Manor	Hamilton	\$21,190	yes	2010	Clerk stole court payments
Village of Gratis	Preble	\$60,714	yes	2011	Fiscal officer stole utility payments
Village of Leetonia	Columbiana	\$1,700	yes	2012	Water lab employee stole from collection
Village of Lithopolis	Fairfield	\$20,099	yes	2009	Clerk stole from check payments
Village of Lockland Mayor's Court	Hamilton	\$188,481	yes	2008	Clerk used void scheme
Village of Lynchburg	Highland	\$64,145	yes	2010	Clerk stole from utility payments
Village of North Baltimore	Wood	\$79,123	yes	2015	Utility clerk stole from cash payments
Village of Ripley	Brown	\$952,618	yes	2010	Utility clerk used adjusting journal entry scheme
Village of Roswell*	Tuscarawas	\$1,637	no	2011	Missing utility payments
Village of Rutland	Meigs	\$77,957	yes, 2	2014	Fiscal officer, water clerk stole village collections
Village of Smithfield*	Jefferson	\$58,294	yes	*	Missing utility, mayor's court collections
Village of South Amherst	Lorain	\$13,035	no	2012	Missing utility payments
Village of Utica	Licking	\$360	no	2011	Missing income tax payments
Village of Verona	Preble	\$36,096	yes	2014	Clerk stole utility, rental payments
Village of Wintersville	Jefferson	\$3,120	no	2015	Missing magistrate court funds
Vinton County Local School District	Vinton	\$24,865	expunged	2010	Missing student lunch payments
Warren City School District	Trumbull	\$46,422	no	2013	Missing ticket revenue
Warren County	Warren	\$75,661	yes	2011	Employee stole Medicaid spend-down payments
Warrensville Heights City School Dist.	Cuyahoga	\$13,657	no	2012	Missing student payments
Westerville School District Library	Franklin	\$26,062	yes	2015	Deputy fiscal officer stole cash payments
Westside Community School	Cuyahoga	\$32,393	yes	2016	Administrative assistant stole student payments
Wheelersburg Local School District	Scioto	\$30,867	no	2009	Missing payments to latchkey program
Wyandot County Agricultural Society	Wyandot	\$5,807	yes	2017	Secretary stole cash collection

* Findings in multiple audits



Dave Yost
Ohio Auditor of State

88 E. Broad St.
Columbus, OH 43215
800-282-0370
614-466-4490
www.ohioauditor.gov