



# **SAFEGUARDING YOUR CASH ASSETS**

By Patricia A. Patrick, CPA, CFE,  
CGFM, Associate Professor of  
Accounting, Shippensburg University

*Understanding misappropriation schemes and what  
can be done to effect internal controls*

**H**ave you ever wondered why cash is so vulnerable to theft? Cash is easily transferable from owner to owner, highly portable and liquid. Cash, checks and currency are easily converted to cash and payable to bearer. Cash does not contain any distinguishing marks identifying the owner, unless the owner marks the bills in advance. These features make cash the primary target of employee theft and one of a municipality's most vulnerable assets.

Cash can be misappropriated via skimming or larceny, this article explains several skimming and larceny schemes. It then describes the way a municipality can implement effective internal controls over cash receipts, cash disbursements, municipal credit cards and petty cash funds, as these are some of the more common ways cash is misappropriated. Cash is vulnerable to theft, but municipalities can implement basic controls to safeguard it.

#### **The Misappropriation of Cash**

As noted above, cash is a very vulnerable asset. It can be misappropriated through skimming or larceny. Skimming is when incoming cash is stolen before it is entered into a municipality's books. Larceny is when cash that has been recorded is taken by a perpetrator.

**Skimming.** Skimming can occur anywhere cash enters the municipality. Municipal employees who handle incoming cash are the most likely perpetrators of skimming schemes. This includes mailroom employees, as well as employees who handle cash sales and customer payments. The most basic skimming scheme occurs when an employee makes a cash sale and pockets the cash without recording the sale. Skimming also occurs when an employee understates the amount of a legitimate sale or conducts unauthorized sales after hours or off-

the-premises. Employees that transact sales, fail to record the full amount of the sales and pocket the cash are committing skimming.

Skimming can also be perpetrated by stealing the payments of customers. Municipalities bill customers for a variety of services and those customers remit payments. If an employee steals the incoming cash before it is recorded on the municipality's books it is a skimming scheme referred to as "lapping." Lapping is when an employee steals the incoming cash from Customer A and applies the subsequent cash payment of Customer B to Customer A's account. Lapping is a complex scheme designed to conceal the theft of customer payments by applying the cash payments of one customer to the accounts of other customers. Lapping schemes must be continuously carried out to avoid detection.

Skimming is best prevented by heightening managerial oversight at the point in which the cash enters the municipality. Managers can physically watch employees open the mail or install surveillance cameras to serve the same purpose. The "perception of detection" is an effective deterrent of skimming. It is very difficult to detect skimming without turning an inside witness or catching the perpetrator in the act. This makes tips by an eye-witness an effective way to detect skimming. The best way to detect lapping is to compare the name on the customer account where the cash receipt is posted with the name on the customer check evidencing payment. A mismatch between the name of the customer that sent the payment and the account to which the cash receipt was posted is an indication of lapping.

**Larceny.** Larceny is when cash that has already been recorded on the victim-organization's books is stolen. Larceny occurs when an employee intentionally takes cash that belongs to the municipality. The primary

difference between skimming and larceny is that larceny is the theft of cash that has already been recorded in the municipality's general ledger, and skimmed cash has yet to be recorded. Another word for larceny is simple theft. Larceny usually involves the simple theft of unguarded cash sitting on a table. To legally prove larceny the municipality must prove four elements: 1) the employee took the cash; 2) the cash belonged to the municipality; 3) the cash was taken without the municipality's consent; and 4) the employee intended to convert the cash to his own use. Proving larceny may not be so simple. It may be easier to safeguard from larceny by implementing good internal controls.

#### **Internal Controls Over Cash**

Good internal controls over cash usually involve implementing internal controls over cash receipts, cash disbursements, municipal credit cards and petty cash funds.

**Cash receipts.** Municipalities can protect cash receipts by employing a few simple steps. The first and most important step is to require two employees to be present when opening the incoming mail. Requiring someone to witness the opening of the mail prevents the skimming of cash receipts. Once the mail is open, one of the employees should make a list of all the cash and checks received in the mail, along with the identity of the party remitting the payment and the purpose of the payment. These facts are usually documented by the remittance advice (e.g., the tear-off portion of the invoice enclosed with the receipt). Municipalities should photocopy checks when remittance advices are not included with the receipts. The checks should be immediately endorsed on the back "for deposit only" with the municipality's account number. The employee who prepares the list of cash receipts should give the list to a



**MISAPPROPRIATION IS NOT APPROPRIATE** Skimming and larceny schemes are common ways for people to steal cash

second employee, who will prepare the deposit ticket. The second employee will also deposit the cash daily and intact. The second employee will then give the bank-validated deposit ticket and the list of cash receipts to a third employee, who will ensure that the totals match. The third employee will then record the cash receipts to the general ledger. On a monthly basis the second employee will reconcile the bank statements, and the third employee will reconcile the accounts receivable/payable control accounts to the subsidiary ledgers. It is also advisable to bond the employees that handle cash. This will enable the municipality to recover their losses in the event of a theft.

**Cash disbursements.** The most effective control over cash disbursements is the use of a voucher system. A voucher system is series of documents showing that purchases are properly approved and documented before they are entered into the accounting system and paid. The first step toward making a purchase in a voucher system is to complete a Purchase Requisition. A Purchase Requisition is an internal document prepared by the person making the purchase request. It describes the item to be purchased. If the purchase requisition is approved (signed), a serially numbered purchase

order (PO) will be issued, indicating the item to be purchased, the authorized vendor and the purchase price. Once a signed the PO is presented to the vendor and the item is purchased, the vendor will send the municipality an invoice. If the item is shipped the municipality will complete a receiving report. Someone at the municipality should review the receiving report to ensure the items ordered are the items received. If someone from the municipality picks up the item, that person will sign a bill of lading. When all the documents are completed, the purchase requisition, PO, receiving report (or bill of lading) and vendor invoice can be matched. If the information on all the documents is consistent the liability can be entered into accounts payable. If it is not, the discrepancies should be investigated. Once entered into accounts payable, all purchases should be paid by check. Recurring or large purchases should never be paid with cash. Likewise, municipalities should strictly prohibit ATM withdraws. Municipalities that follow the above recommendations will ensure that purchases are properly authorized. This, in turn, provides strong internal controls over cash disbursements.

A voucher system is the most effective way to control purchases and subsequent cash disbursements.

However, a voucher system cannot protect the municipality against all purchase-related fraud. Blank POs can be stolen, signed and used by rogue employees to make unauthorized purchases. Rogue employees can also alter or falsify otherwise authorized POs. Executed POs are legally binding documents between the municipality and vendor. Municipalities will be legally obligated to pay for purchases made with POs, whether they approved the POs or not. Therefore, PO custodians should keep blank, serially-numbered POs in locked cabinets and safeguard them with care. Custodians should also be able to account for the disposition of every PO in the numeric sequence at any point in time, as every blank and unfilled PO exposes the municipality to potential legal liability.

**Municipal credit cards.** It is not uncommon for municipalities to issue municipal credit cards to employees, who are then authorized to make work-related purchases on these cards while traveling or performing other work-related duties. Employees submit their receipts to an administrator who, on a monthly basis compares the receipts to the statements and determines that the purchase is for an allowable item. If everything is in order, the administrator pays the bill. Municipalities should have written policies and procedures that disallow the purchase of personal items and state that original receipts (not photocopies) must be submitted for reimbursement. Unlike the voucher system above, purchases made with municipal credit cards need not be approved in advance. Employees simply make purchases, sign their names and submit receipts. Unauthorized purchases are not identified until after the purchases are made and the statements are reviewed by the administrator. This makes purchases made with credit cards harder, but not impossible to control.

A key step in gaining control over credit card purchases is maintaining safe custody over credit cards and ensuring that only responsible employees are issued cards. Employees should be asked to periodically read and acknowledge the municipality's policies regarding cards. The policies should be very clear about the types of items that are disallowed, and how and when the cards may be used. Another step is through the thorough review of the monthly statements. The administrator charged with reviewing and paying the monthly credit card bills should review the statements for disallowable items and insist upon getting original receipts. Employees should be asked to explain the work-related purpose of each purchase and/or to produce the purchased items upon request, so they can be physically inspected.

Employees can perpetrate a variety of fraud schemes using credit cards. For example, rogue employees can steal and use the credit cards of authorized cardholders. Authorized cardholders can purchase items for credit just to return them later for cash. Municipalities can minimize credit card frauds by establishing spending limits, having statements sent directly to the administrator, having someone independent of those with signature authority on the account review the statements, investigating unexplained increases in purchasing levels, and denying reimbursements for purchases made in contravention to the municipality's policies. Municipal credit cards give employees flexibility in making work-related purchases, but municipalities can still exercise control over those purchases.

**Petty cash funds.** While most purchases should be made using the voucher system described above, most municipalities maintain a petty cash fund for small, non-recurring purchases. It is not uncommon or

unacceptable for municipalities to maintain a small amount of cash for miscellaneous expenditures such as postage and office supplies. Expenditures made from a petty cash fund are often necessary to facilitate operations. It is not a problem for municipalities to make nominal purchases with cash, as long as the purchases are supported with receipts. The issue is how to maintain control over a petty cash fund, given its vulnerability to theft.

Control can be achieved over a petty cash fund by conducting surprise cash counts. At any given time the cash in the fund and the receipts collected to support the purchases should equal the total amount of the petty cash fund. If municipal officials believe the petty cash custodian is "borrowing" money from the petty cash fund during his lunch break or over the weekend, then the surprise cash counts will come up short. Municipalities can mark the bills in the fund. Placing marked bills in the fund on a Friday afternoon and finding a different set of bills in the fund on Monday morning may indicate a borrowing scheme. Municipalities can also periodically select a sample of petty cash expenditures and review them for appropriateness, authorization and validity. It is not inappropriate to keep small amounts of cash on-hand to pay for nominal purchases, but it is important to safeguard the petty cash fund from theft.

#### **Conclusion**

Cash is a vulnerable asset. It is highly liquid, not easily identifiable and very portable. This makes cash a prime target for theft by skimming and larceny. Municipalities can safeguard their cash by implementing internal controls over cash receipts, cash disbursements, municipal credit cards and petty cash funds. Internal controls over cash receipts involve establishing a separation



**BRIGHT IDEAS** Your borough can implement internal controls to help ensure assets are safeguarded

of duties and charging various employees with tasks related to the processing of cash receipts. Controls over cash disbursements include using a voucher system and paying for purchases by check. Controls over municipal credit cards involve establishing policies regarding the use of credit cards and diligently reviewing activities to ensure that they comply with stated policies. Controls over the petty cash funds require frequent surprise cash counts and periodically setting traps for custodians. Cash is a very vulnerable asset, but it can be protected by following a few simple steps. **(B)**

#### **About the Author**

Patricia A. Patrick, CPA, CFE, CGFM is Associate Professor of Accounting at Shippensburg University where she teaches auditing and forensic accounting. Patricia earned a PhD in Public Administration from Penn State Harrisburg in 2007 and has published in the Journal of Public Budgeting, Financial Management and Accounting, the International Journal of Public Administration, the Journal of Ethnicity in Criminal Justice, the Journal of Criminal Justice, Security Journal and Security Management.