Cash Receipting: Fraud Prevention and Internal Controls

WACO Annual Conference

October 3, 2018

Table of Contents

Fraud Statistics and Overview

Occupational fraud and abuse

The Association of Certified Fraud Examiners' 2018 *Report to the Nations on Occupational Fraud and Abuse* included a study that examined occupational losses to determine how they occurred, were detected and how much was lost. In the 2,690 cases studied, typical losses were pegged at 5 percent of yearly revenue, and the average loss per case was $2.7 million.

Anti-fraud controls

The most prominent weaknesses leading to frauds were **lack of internal controls and management review**. Anti-fraud controls are associated with:

- Quicker detection
- Reduced losses

In organizations that had specific anti-fraud controls in place, fraud losses were detected up to 58 percent more quickly and were as much as 56 percent smaller.

Fraud detection

Tips are consistently the most common detection method by a significant margin at 40%. Over half of the tips come from employees (53%) followed by customers at 21%. Other detection methods include internal audit at 15% and management review at 13%.

Smaller organizations (<100 employees) typically have fewer anti-fraud controls than larger entities and require an increased level of trust in employees to do the right thing, leaving them more vulnerable to fraud. Also, they are more likely to rely on external audit as their primary anti-fraud control, which identifies frauds in less than 5% of the cases.

$7.1 billion

losses (2,690 cases studied)

5%

estimated portion of yearly revenue lost to fraud

Perpetrators

96%

no previous conviction

43%

living beyond means

25%

accounting/finance/ purchasing

69%

male

Importance of Internal Controls

Anti-fraud controls

The most prominent weaknesses leading to frauds are **lack of internal controls and management review**. Anti-fraud controls are associated with more than *half* of asset misappropriation schemes.

What are internal controls?

- A process designed to give reasonable assurance of:
  - Effective and efficient operations
  - Compliance with applicable laws and regulations
  - Reliable financial reporting
- *An important factor in preventing and detecting fraud*

Who is responsible for internal controls?

Management is in the best position to establish and maintain internal controls and is held primarily accountable for their proper functioning.

Why are internal controls important?

Fraud is facilitated by the combination of 3 factors:

- *Motivation* – a pressure or need for money
- *Rationalization* – the fraudster's ability to justify in his/her mind that their actions are OK
- *Opportunity* – the situation/environment that allows the fraud to occur (often weak/nonexistent internal controls)

Effective internal controls break the fraud triangle by **minimizing** the "opportunity" factor

- Clearly define the cash-handling process and develop expectations
- Develop forms and reports to validate and support transactions
- Observe and monitor activities
- Review documents

Effective internal controls:

- Protect employees
- Safeguard public resources
- Help prevent fraud

Effective internal controls **enable** you to:

- Identify a loss promptly
- Determine the entire amount lost
- Identify responsibility for the loss

30%

lack of internal controls

19%

override of internal controls

18%

lack of management review

10%

poor tone at the top

Common Cash Receipting Schemes

Larceny (theft of funds that are already recorded in the entity's accounting records)

- Reversing transactions
  - False voids or adjustments
  - "Negative" cash receipts
- Missing deposits
- Unauthorized access
  - Destroy or alter register tapes
  - Two sets of receipts

Skimming (the fraudster takes cash "off the top" of the daily receipts and never officially records the total or records a lower amount. Cash is taken before being recorded and deposited)

- Theft of cash receipts
  - Unrecorded receipts
  - Understated receipts
- Theft of cash on hand
- Substitute unexpected/other receipts
  - Write-off schemes
  - Lapping (a sophisticated skimming scheme where the fraudster steals a customer payment and covers the shortage with another customer's payment received at a later date)

Common weaknesses and warning signs

Fraudsters take advantage of situations that exist in their work environment (the opportunity side of the fraud triangle) to commit fraud. They also leave "clues" behind because a fraud involves not only committing the act itself, but also efforts to conceal the misdeeds. Understanding the methods fraudsters use to perpetrate and cover their crimes can help governments better design internal controls to limit the opportunity to commit fraud, and identify the warning signs.

The State Auditor's Office sees an average of 450 loss reports filed each year and investigates an average of 40 cases a year. Our Office has been compiling fraud statistics for 30 years and consistently, the following *red flags* are identified as the common internal control weaknesses and fraud warning signs.

- Highly trusted employess with limited oversight
- No segregation of duties
- Inadequate monitoring and review
- Lack of supporting records
- High volume of voids/adjustments
- High volume of system deletions/modifications
- Deposits not made daily or intact

Examples

- A county cashier recorded fake transactions in the accounting system to misappropriate at least $617,467.
- A city cashier at a community center, misappropriated at least $14,491 by canceling valid transactions and removing the cash.
- A port manager misappropriated at least $89,024 in cash receipts, concealing it by altering the system report before sending it to the accounting department.
- A school district employee misappropriated at least $20,463 by not depositing cash payments that were paid for District services. He also did not pay for services that he received.
- A fairgrounds manager did not properly deposit cash receipts of $16,382. In addition, $1,128 in warrants to replenish petty cash and credit card fees were not deposited.
- A senior center travel coordinator used $31,429 of revenue for personal travel costs.

Designing Cash Handling Internal Controls

Management is in the best position to establish and maintain internal controls and is held primarily accountable for their proper functioning.

Break the system into:

- Locations
- Process segments

Evaluate and choose the type of control that will work best:

- Preventive
- Detective

Internal controls: The big picture

Effective internal controls break the fraud triangle by **minimizing** the "opportunity" factor.

- Clearly define the cash-handling process and develop expectations
- Develop forms and reports to validate and support transactions
- Observe and monitor activities
- Review documents

Cash handling controls: Define the process

- Written policies and procedures communicated directly from management
- Required training in cash receipting responsibilities
- Reasonable safeguards to secure areas where receipts are handled
- Require proper recording of transaction amounts, payment modes, dates and general ledger account
- Cash receipts must be deposited intact and promptly (daily if practical)
- Employees who handle receipts must be bonded

Safeguard and limit access to receipts awaiting deposit

- Is a safe or locking cabinet used to store deposits? How frequently is the safe combination changed?
- Use separate, secured cash drawers for each cashier
- Document all fund transfers between cash handlers
- Consider using locking bank bags
- Consider using video cameras in key locations

Segregate duties

One person should not control the entire accounting transaction (authorization, recording, reconciling and custody)

The following duties should be segregated:

- Cash receipts
- Cash counts
- Bank deposits
- Deposit/receipt reconciliation
- Bank reconciliations
- Deposit posting
- Cash disbursements

Mail receipts

- Mail is opened by someone independent of the cashier, accounts receivable bookkeeper or employees who may initiate or post journal entries
- Does the employee opening the mail:
  - Immediately restrictively endorse checks?
  - Prepare a list of money, checks and other receipts?
  - Forward receipts to the person preparing the bank deposit?
  - Forward the listing to the person responsible for authenticating the deposit to the amount recorded?

Billings and receivables

Billings/receivables employee should be restricted from:

- Posting account payments
- Preparing the bank deposit
- Access to the cash receipt books
- Access to customer collections

Cashier should be restricted from:

- Posting account write-offs and adjustments
- Access to customer statements
- Handling customer complaints

Cash handling controls: Develop expectations

Revenue

- What is the historical/typical revenue pattern?
- Perform a periodic "look back" of revenues. Does it make sense given your understanding of the operations?

Unanticipated revenue

Does the organization receipt/record infrequent revenue streams or "unanticipated" revenues (rebates, collection agency payment, grants, agreements with annual payment, one-time fees etc.)?

Cash handling controls: Forms, reports, support

Pre-numbered receipts: Are receipts used sequentially? Are all the receipt numbers accounted for?
Standardized forms: Do they capture the right information? Are they complete?
Bank reconciliations: Are they timely? Do reconciling items make sense? Is the right employee completing them?
Reports: Are they system generated?

Cash handling controls: Systems

Access

- Review user rights periodically
- Limit system permissions to only those needed to complete job tasks
- Give each employee unique user log-on ID and password
- Prohibit sharing of log-on IDs and passwords
- Automate log-offs for inactivity
- Decide what functions are allowed in "administrator" rights

Operations

- Is the system set up to use all security options?
- Can transactions be pre- or post-dated outside the current period?
- Does the system batch transactions, allowing changes until the end of day?
- Can receipts be kept in unreconciled/batch mode instead of finalizing them?
- How do system modules interface?

System reports

- Monitor audit trail/transaction logs
- How do voids and adjustments appear in the reports?
- Are you reviewing a "final" report?
- Know which module generates which reports
- Are reports ad hoc or user defined?

Cash handling controls: Observe, monitor, review

Beware of the "trusted employee" trap

- "Trusted employees" still need oversight
- Sometimes good people do bad things
- Two phrases we often hear:
  - "I trusted him/her"
  - "We never thought it would happen to us"

Actions to take

- **Compare bank deposits to receipt records.** Do the payment modes agree?
- **Develop deposit composition expectations.** Does the total deposit make sense?
- **Create and review error reports.** Do you create and review audit logs, voids and adjustment reports, and exception reports?
- **Perform surprise cash counts**

Voids

- Does the amount of void activity make sense?
- Are voids and adjustments authorized, supported, reasonable and legitimate?
- Are actual voids recorded in the system compared with those approved?

Customers, accounts, refunds

- Customer bills should detail the prior balance, payments, adjustments and the current amount due
- Monitor customer complaints
- Review employee account activity
- Review deposit refunds

Look for red flags

- Deposits not made daily or intact
- Cash deposits that differ from normal patterns
- Unusual over/short receipting activity
- Unusual void activity by employee or department
- Negative cash receipts
- Unusual/ unexpected journal entries

Best Practice Tips

Develop a monthly revenue/receipting calendar

Use your annual budget to get a better handle on the anticipated timing of receipts. Receipts that are not monthly routine deposits are more susceptible to fraud. Your calendar can be high level or detailed, organization wide or for a single department.

Calendar may include

- Quarterly, semi-annual or annual contracts and agreements
- Monthly revenues that generate different cashflows
- Seasonal operations (pools, parks, etc.)

Identify revenue/receipting effects for operational changes

Many times the focus is on making the change happen but anticipate the revenues changes and be sure they happen. Examples include:

- Planning a surplus sale
- Adding new programs
- New fees for existing services
- Board approved rate increases
- One-time fees

Have employees certify they read policies, understand them and were provided training

This demonstrates to employees that management takes controls seriously and places high importance on following the established process. It also provides evidence should fraud happen to you. You could even have employees update their review and take refresher training annually.

Ask your software vendor about known system weaknesses

- Do you have the most current version of the software?
- Are your software preferences and permissions affording you the best use of software security options?
- Can receipts be post-dated, reprinted, or entered and remain un-finalized at end of day?
- How do modules interface when adjustments are made?

Ensure system reports are generated by the person performing the review and monitoring

If the reviewer understands the system, this best practice eliminates the complexities regarding ways system reports can be manipulated.

Spot check deposits to customer accounts to ensure they are posted to the correct account promptly and in full

Employees feel there is less "opportunity" if they know someone is looking. Getting into the details occasionally will confirm your understanding that the process, forms, reports and support are being used and the controls are operating as intended.

Occasionally prepare a bank deposit or bank reconciliation

Gather up all the documents the cashier or clerk would use and actually go through the process. Take it to the next level and take the deposit to the bank. You might learn valuable information about the process from that third party. If you decide to incorporate spot checks in your control system, these should occur randomly – NOT on a regular schedule.

What to Do if Fraud Happens to You

Report immediately

Immediate reporting is a statutory requirement (RCW 43.09.185).

- Fill out a report online at www.sao.wa.gov. (It takes only a few minutes!)
  Go to Investigations > Fraud Program > Report a Fraud

Not required to report in cases of:

- Normal "over and short" situations
- Reasonable inventory shortages
- Breaking and entering, or vandalism

What to do

- Protect accounting records from loss or destruction
- Remove access to financial system, bank account and credit cards
- Consider filing a police report (consult us on timing)
- Notify others who need to know about the loss
- Ensure personnel action is taken for violating policies and procedures, NOT for misappropriating public funds

What NOT to do

- **DO NOT** enter into a restitution agreement with an employee (written approval from both Auditor and Attorney General required by RCW 43.09.260)
- **DO NOT** agree to let employee repay to "make it go away"
- **DO NOT** try to be the investigator. But do start a record and timeline: how it came to your attention, records of conversations, etc.
- **DO NOT** physically prevent an employee from leaving the room or leaving the building

Bonus Material: Continuous Improvement

When is process too much process?

- Complexity results in errors
- Complicated and routinely circumvented
- Produces duplicate data or data that is not used

Processes should be:

- **Standardized**, especially at touch points
- **Clear** in staff roles and responsibilities
- **Simple** to understand for staff, mgmt., & auditors
- **Focused** on the next customer receiving output from each previous step
- **Examined** across the entire system
- **Reviewed and updated/adjusted** to address changes to the system and the environment (PDCA)

What to do

Streamline, simplify and standardize system-wide

When is documentation too much documentation?

- Form layout is not user friendly
- Forms record information that is not used
- Excessive email or electronic files are produced
- Memos and reports are complicated or not used
- Documents are copied and copies are never used

Documentation should be:

- **Created** from the customer's perspective
- **Consistent** in format and verbiage
- **Single-sourced**
- **Clearly labeled and dated**
- **Created** for a specific purpose and audience

What to do

Keep it clear, consistent and user-focused

When is monitoring too much monitoring?

- Reviews/approvals without an "opportunity" focus
- Redundant reviews or approvals that do not improve accuracy or quality
- Excess paperwork handling and shuffling
- Assignments that do not fit employee skills/talents
- Unbalanced workloads

Monitoring should be:

- **Purpose focused** and performed with intention
- **Focused** on the specific role and responsibility of each person – keep work close to the source
- **Embraced** and comforting for the truly trusted employees

What to do

Keep it focused, followed up and fully embraced as part of culture