Fraud and Understanding Fraud Basics

MACC
MID AMERICA COMPUTER CORP

2017 MACC Expo

Charles A. Albert, CPA/CFE
Curtis Blakely and Co, PC, CPAs

Curtis Blakely & Co., PC
Certified Public Accountants & Consultants

Qualifications

- Curtis Blakely And Co, CPAs, PC has been serving the utility industry for over 50 years.
- We audit over 100 companies including their subsidiaries.
- RUS Approved Accounting Firm
- CBCo has clients in Arizona, New Mexico, Texas, Louisiana, Oregon, Oklahoma, Florida, Colorado, California as well as Mexico.
- Two individuals hold their Certified Fraud Examiner (CFE) certification – Charles Albert, CPA-CFE, and Tessa Fowler, CPA-CFE
- In addition to audit services, we perform monthly accounting assistance for numerous telecommunications firms (act as contract controller in some cases). We know the “nuts and bolts” of telcom accounting.
- We have noticed an increase over the past several years in fraudulent activity, and participated in numerous fraud investigations.

So what exactly is Fraud?

Fraud (Definition)

Black's Law Dictionary states that fraud is "a generic term, embracing all multifarious means, which human ingenuity can devise, and which are resorted to by one individual to get advantage over another by false suggestions or by suppression of truth, and includes all surprise, trickery, cunning, dissembling, and any unfair way by which another is cheated."

The intentional (deliberate) deception resulting in injury to another person. It is a deliberate misrepresentation which causes another person to suffer damages, usually monetary damages.

Accounting Fraud

An employee who manipulates a company's accounts to cover up theft or uses the company's accounts payable and receivable to steal commits accounting fraud. Employees involved in accounting fraud schemes are generally those in positions that have access to a company's accounts with little or no oversight.

Accounting fraud includes:

Embezzlement (also called larceny) – Any fraud conducted by a person who controls the funds being used.

Accounts payable fraud

Fake supplier – An employee sets up a fake supplier and bills the company for good or services not provided.

Personal purchases – An employee uses company funds to pay for personal purchases and records the payments as legitimate business expenses in the accounting system.

Double-check fraud – An employee writes a check to pay an invoice then writes a second check to himself or herself and records the disbursement in the accounting system as a payment to the same supplier.

Accounts receivable fraud

Lapping – An employee covers up the theft of funds from customer 1's account by recording the payment by customer 2 to customer 1's account, then applies the payment by customer 3 to customer 2's account, and so on. The employee usually must falsify accounting records to conceal the lapping scheme.

Diversion – An employee keeps the funds from an account that has been written off by the company. These funds are often not tracked.

Fictitious accounts or sales – An employee creates fictitious accounts and sales to make the company appear more profitable to investors and creditors or to boost commissions that are based on accounts opened or sales volume.

Understanding The Financials

In order to detect fraud, it is beneficial to have a background of accounting and understand the flow of information which the end result is the financial statements and other information monthly.

- Luca Pacioli gave us debits and credits in 1494. Some of us learned the “old fashioned” way – a ledger. This taught the user the true flow of the accounting process…..
- Often bookkeeping seems completely automated. The transactions flow where they need to, generating monthly reports, supporting schedules, financial statements, invoices, payroll and other accounting information.
- An employee may only see one area of the company’s accounting activities and not be aware of what function they play in the overall financial functions of the organization.
- Without an understanding of the transaction flow and the “big picture” by knowledgeable personnel and management, a fraudster may be able to hide his fraud with relative ease.

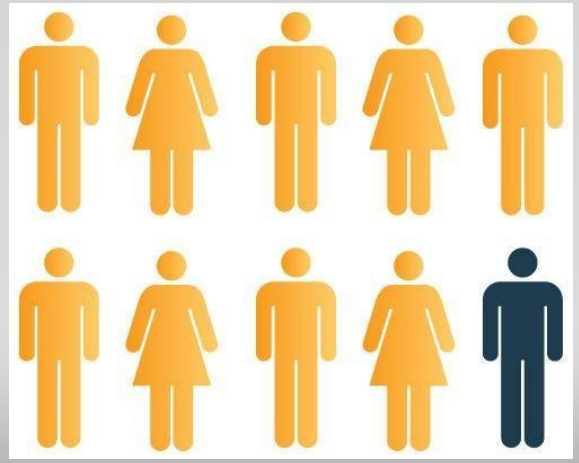
Who Commits Fraud?

5% **of the population will commit fraud regardless of the circumstances.**

85% **of the population will commit fraud given certain conditions. (Pressure, Opportunity and Rationalization)**

10% **of the population will not commit fraud under any circumstances.**

Based on studies, 90% of people will commit fraud given the right conditions.



Hopefully the other 9 are in the other sessions.

Interest Fraud Statistics

- The typical organization loses over 5% of its revenue to fraudulent activities annually.
- The median loss is $140,000.
- A typical fraud lasts 18 months before detection.
- The most frequent method to uncover fraud is by a tip.
- ***81%*** of the cases reported, the fraudster displayed one or more Behavioral Red Flags.

Auditor's Responsibility

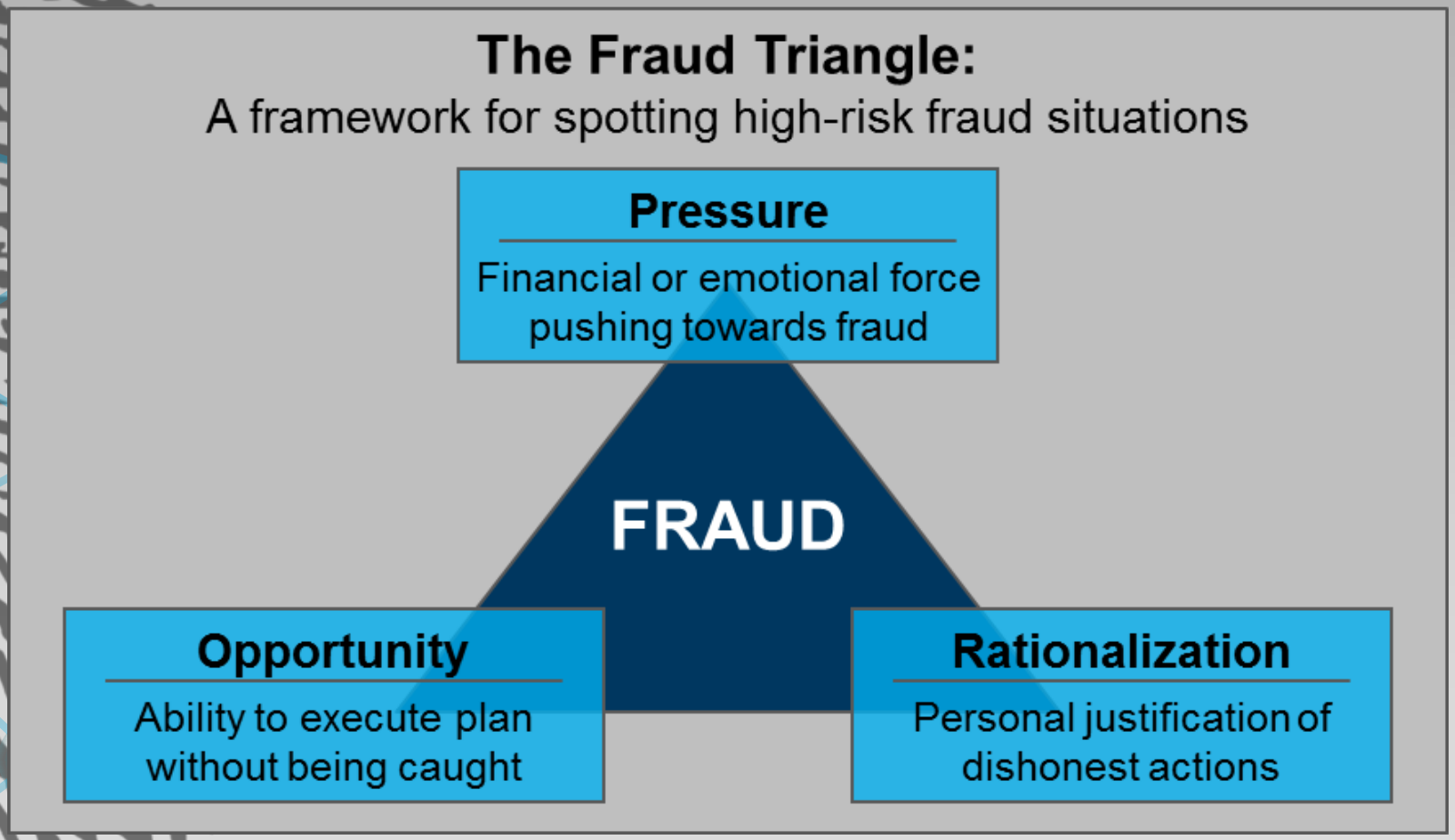
A financial statement audit is ***not*** designed to detect immaterial fraud. However, any fraud encountered during a financial statement audit should be reported to management or the board of directors.

Example: Auditor requests invoices exceeding their planning materiality threshold for Individually Significant Items (ISI) when reviewing the plant activity for the year. The audit planning materiality calculation determined that invoices over $10,000 should be selected. The fraudster wrote 4 checks to himself ranging from $3,000 – 7,500, coding the disbursements to other vendors and to several different plant accounts.

The auditor may not uncover these fraudulent disbursements by simply vouching items over scope. Cash disbursements testing and a sample may uncover one or more of the amounts.

In summary, it is NOT the CPA firms' responsibility to uncover fraud during the audit if it is immaterial to the financial statements taken as a whole.

Fraud Triangle



Pressure “Red Flags”

- Living beyond their means.
- Gambling/substance abuse problems.
- Overwhelming debt obligations.
- Job dissatisfaction/frustration.
- Other financial obligations (medical needs, added dependents)
- Legal problems.

Employee Fraud Detection Tips

Watch for the following red flags:

- Employees with a lavish lifestyle that doesn't match their salary
- Employees who don't take vacation
- Employees who routinely stay late and work on weekends
- Frequent tips or complaints about an employee
- Inventory shortages
- An employee who reluctant to share his or her job function
- Large number of write-offs in account receivable
- Employees who seem to feel the rules don't apply to them

The best way to detect employee fraud is through tips, which is why implementing a whistleblower hotline can be the best deterrent. The most common detection method is tips, with 39 percent of frauds being detected this way. Employees who know that there's a hotline and a company culture that encourages its use have more than just the bosses to be worried about. Every employee becomes the eyes and ears of the company.

Opportunity “Red Flags”

- Nonexistent or insufficient internal controls.
- Ineffective management or high turnover.
- Access to cash on hand or bank accounts.
- Unused PTO (Vacation, Sick)
- Friendly relationships with vendors/suppliers.
- Understaffing.
- History of Tolerating Fraud

Rationalization “Red Flags”

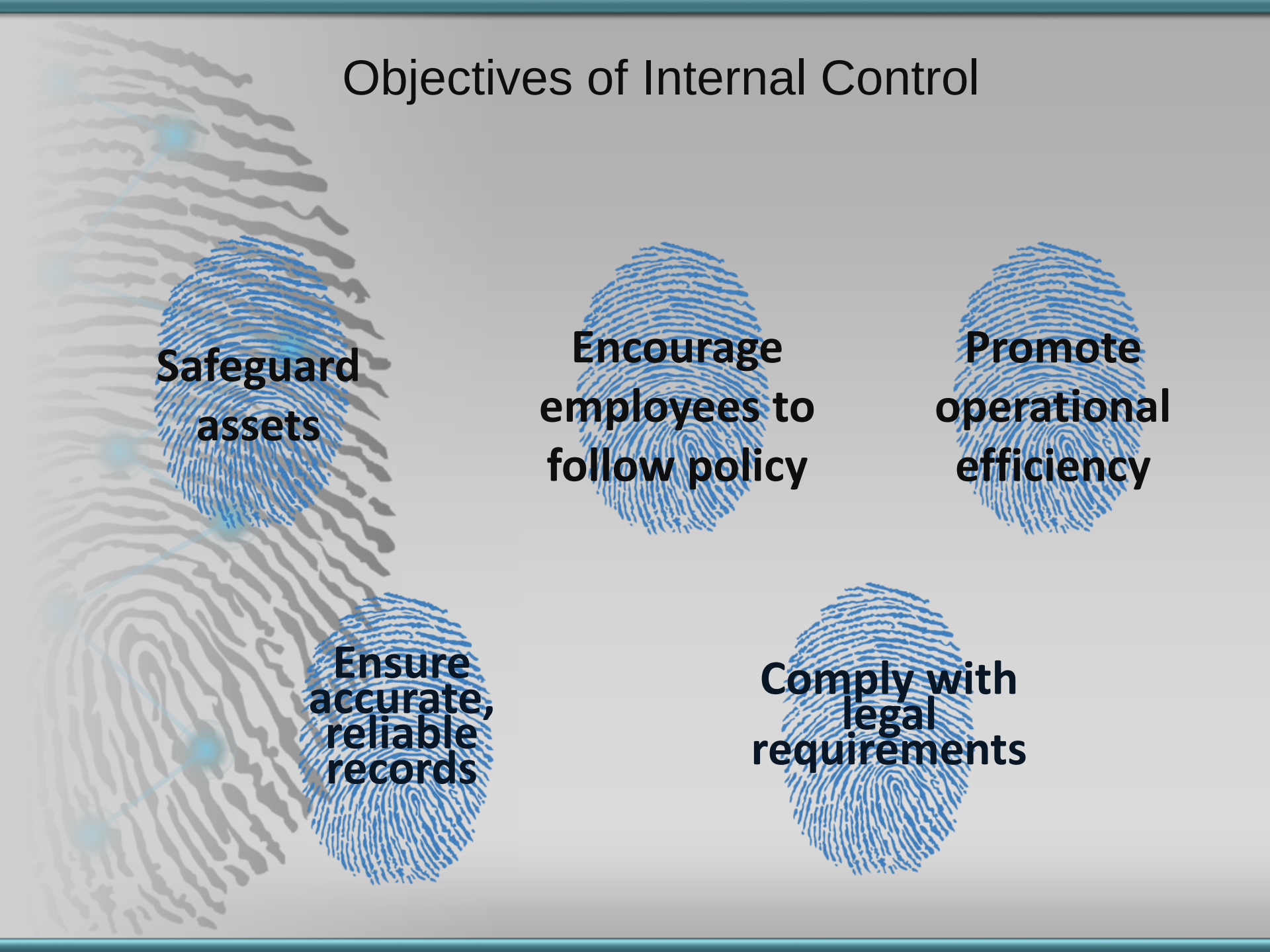
- “I’m just borrowing it. I’m going to pay it back.”
- “The Company has plenty. They won’t miss the money.”
- “I don’t get paid what I am worth. This just makes up for it.”
- “If the Company doesn’t even know I’m doing it, they deserve to lose the money.”
- “Everyone else does it.”
- “The GM bragged about how he used the points on the company card to go on vacation.”

Rationalization is a process of not perceiving reality, but of attempting to make reality fit one’s emotions. ~Ayn Rand

Fraud Prevention

- **Hotline (Tip)** — 39% of fraud cases in the US were discovered based on a tip. [ACFE 2016 Report to the Nations]
- **Fraud Policy** — Policy should apply to all directors, management, employees, vendors, etc. Policy should be reviewed and updated regularly. See ACFE website for example policy.
- **Tone at the Top** — Environment in which management behaves ethically, treats employees equally, zero tolerance for fraud.
- **Training** — Lack of proper training creates opportunities to commit fraud as well as reduces the ability to recognize it.
- **Internal Controls** — Will not guarantee protection against fraud, but is critical in deterring fraud as well as an aid to reveal fraud.

Objectives of Internal Control



Review Your Internal Controls Over Cash

- Cash Receipts
- Cash Disbursements
- Recording
- Reconciliation

Internal Controls – Cash

Segregation of Duties

The foundation of a good internal control system is segregation of duties. The duties of authorization (signing a check or releasing a wire transfer), custody (having access to the blank check stock or the ability to establish a wire transfer), and recordkeeping (ability to record the transaction in the accounting system) should be separated so that one individual cannot complete a transaction from start to finish. The concept behind segregation of duties is that in order to misappropriate cash, individuals would have to collude, rather than one individual acting alone.

For many businesses, proper segregation of duties can be difficult to achieve. In these instances, company owners may want to consider the bank statements delivered to them unopened. The owners should then review the bank statements and the check images for any transactions that appear unusual, and follow up on these transactions to obtain an understanding of them.

Internal Controls – Cash

Review Authorized Signors

Carefully consider who your authorized signors are (authorization of the transaction). Those individuals should not have access to the blank check stock (custody of the asset) nor the ability to enter the transaction into the accounting system (recording of the transaction). The use of a signature stamp, although efficient, may be problematic in that you must have separate controls to ensure that the stamp is not readily available for inappropriate use.

Internal Controls – Cash

Require Dual Signatures

Your company may also want to consider the use of dual signatures. A dual signature policy includes the establishment of a dollar threshold over which checks require two signatures. The utilization of dual signatures establishes an element of segregation of duties for disbursements over a specified threshold in that these disbursements require more than one individual to authorize the transaction.

Internal Controls – Cash

Review Electronic Fund Transfers and Other Activity

The use of wire transfers has increased significantly over the years, and segregation of duties around wire transfers is paramount. The responsibilities for establishing a wire transfer should be segregated from the responsibility of releasing the wire transfer. If this segregation is not possible, consideration should be given to using a call-back procedure, in which the financial institution will call a specified individual when a wire transfer is initiated. Most important, the call back cannot go to any individual who is able to initiate a wire transfer.

Internal Controls – Cash

Reconcile Bank Accounts Timely

The bank reconciliation should be completed in a timely manner by someone who is independent of the cash disbursement process. The bank reconciliation should also include a review of the bank statement and the check images that are returned with the bank statement for unusual transactions. Any unusual items should be investigated and evaluated when necessary.

Internal Controls – Cash Receipts

- Independent reconciliation of cash collected to amounts posted.
- Someone independent of cash receipts process should deliver deposit to the bank.
- Someone independent of cash receipts process should post receipts to the general ledger.
- Someone independent of cash receipts processing and recording should reconcile the bank statement.

Internal Controls – Cash Receipts

- Independent reconciliation of cash collected to amounts posted.

All Rpt Areas
CO # : [redacted]
OCN # : [redacted]

Batch Report - Applied
8/1/2017 - 8/1/2017, Sorted by Order Payments Entered, Exclude POS
[redacted]

Page 1 of 1
08/23/2017 6:49:41 PM
[redacted]

All Payment Methods Are Included
Included: Pre-Payment Deposits

Account Name	Acct No	Payment Method	Payment Method Number	Transaction ID	Pay Date	NSF	Pay Amount
Batch Name 080117							
		Cash	MG		08/01/2017		100.00
		Cash	MG		08/01/2017		101.17
	Pay Method Count:	**2**			**Pay Method Total:**		**201.17**
		Check	1307 MG		08/01/2017		103.15
		Check	1224 KB		08/01/2017		205.92
		Check	1602 MG		08/01/2017		110.00
	Pay Method Count:	**3**			**Pay Method**		**419.07**
		Money Order	17-628956858 MG		08/01/2017		100.00
	Pay Method Count:	**1**			**Pay Method Total:**		**100.00**
	Batch Payment Count:	**6**			**Batch Total:**		**720.24**
	Subtotal Payment Count:	**6**			**Subtotal of Regular Payment B**		**720.24**
	Grand Total Payment Count:	**6**			**Grand Total of Payments:**		**720.24**
	Grand Total Pre-Payment Count:	**0**			**Grand Total of Pre-Payments:**		**0.00**
	Grand Total Count:	**6**			**Report Grand Total:**		**720.24**

Internal Controls – Cash

Fraud Findings With Clients

Food Franchise Client: Controller of a client embezzled several hundred thousand due to lax controls over cash.

- Wire transfer to personal Paypal Account
- Wire transfer to pay personal American Express debt
- Controller had signature stamp for owner
- Owner was unfamiliar with Balance Sheet, concentrated on net income. The controller used prepaid accounts to hide the withdrawals

Utility Client: 2 employees embezzled almost $65,000 in less than a year with 2 separate schemes

- Manager's responsibility was to make deposits and reconcile bank statement. Cash deposits were stolen by Manager.
- CSR also skimmed deposits.
- Prior Manager stole amounts given as a deposit for new construction.

Internal Controls – Accounts Receivable

Segregation of Duties

The maintenance of the receivable accounts and related subsidiary ledgers should be separated, wherever practicable, from the functions of (1) establishing the charges to the receivables accounts, (2) recording cash receipts and preparing the deposits, and (3) approval of any adjustments or write-off to any receivable accounts.

Internal Controls – Accounts Receivable

Significant areas that should have segregation of duties:

- Invoice Customers
- Collection of Accounts Receivable
- Posting Cash Receipts to General Ledger
- Review of Aged Customer Accounts Receivable
- Authorization of Write Offs
- Investigate Accounts Receivable Discrepancies
- Authorize Adjustments to Accounts
- Open mail
- Prepare Deposits
- Deposit Cash Receipts

Internal Controls – Accounts Receivable

Reconciliations

It is crucial that all accounts receivable accounts be reconciled between the subsidiary records and the general ledger in a timely manner (monthly).

- All charges, collections, and adjustments to the accounts pertaining to a fiscal month should be recorded for an appropriate cut-off at the end of the fiscal period. MACC's system will allow a company to tie out to the penny.

Internal Controls – Accounts Receivable

Adjustments

Adjustments should be reviewed and approved by an employee (preferably management) independent of billing and collections.

- Employee could adjust accounts for skimmed payments or for friends, family and others for their personal gain.
- Authorization of setting up adjustment codes (USP) should be limited.

Internal Controls – Accounts Receivable

Uncollectibles

Past due accounts should be reviewed monthly and follow-up collection efforts made.

- Review late accounts for employees. We recommend having a policy that employee accounts are reviewed monthly. A MACC custom report could assist with this review.
- Review for relatives and related parties of employees for material write-offs. This could be indicative of fraudulent activity. Policy prohibiting adjustments for family could be considered.

Internal Controls – Accounts Receivable

Fraud Findings With Clients

CSR cashed a check in the business office. The check was returned as NSF. The CSR was notified of the NSF check from the bank and accounting. The CSR accessed their own account and added the NSF check as an adjustment to their own bill, effectively borrowing funds from the company.

Internal Controls – Accounts Receivable

Fraud Findings With Clients

CSR would take payments on accounts and adjust the account for the payment, providing a receipt to the customer for the payment. She would steal the payment but manipulated the system by deleting the payment once the customer left, then using the adjustment screen to reduce the amount the customer owed. The owner/manager did not review adjustment printout available to him had he had sufficient knowledge of the software.

Internal Controls – Accounts Receivable

Fraud Findings With Clients

CSR would take payments on accounts and adjust the account for the payment, providing a receipt to the customer for the payment. She had a “dummy terminal” for cash payments that would provide the customer with a receipt. Batch totals from the dummy terminal were never provided to accounting to reconcile back to the daily deposit.

Accounts Receivable was never reconciled. We found the fraud during our annual audit procedures.

Internal Controls – Inventory

Implement Controls Over Inventory

MACC's MI module is a robust and powerful tool if used properly. We recommend it to all over our mutual clients and have assisted countless companies in using it to its full potential.

Internal Controls – Inventory

Inventory Organization and Managing Inventory

- Secure Inventory In Locked Facilities With Limited Access
- Implement MACC MI
- Consider Separate GL Accounts (Reg, NonReg, CWF, CO, Etc)
- Take a full physical inventory count
- Consider Consistency In Item Codes in MACC When Setting Up
- Review Materials Usage Reporting Procedures
- Review Inventory Reconciliation for Unusual Items, Obsolete Items, Unit Costs that Appear Excessive, Etc.
- If a Contractor Uses Your Inventory Adequate Controls Are Even More Critical (Use You Inventory for Others, Etc)
- Trace Materials Usage to “As Built” Sheets and Contractor Invoices.
- Match Purchase Order and Invoice. Review Approval.
- Require That All Inventory Be Signed Out By Those Responsible and Provide The Inventory Clerk With a Work Order or Similar Information.
- Use The “Smell Test”…. Does it Look Reasonable?

Internal Controls – Inventory

Fraud Findings With Clients

- Modems Were Purchased By The Company. Installer Realized That There Were No Controls For Monitoring Modem Installation. The Employee Provided Modems to Others Free of Charge.
- IT Manager Determined That There Were No Controls on PC Purchases Other Than Matching Purchase Order With Invoice. Dell Purchases Were Not Examined For Reasonableness. He Began Ordering PCs, TVs, Even Video Equipment Through the Dell Account and Sold Them to Others. [“Smell Test: Company Had 20 Employees, but Had Purchased 50 PCs…]
- Contractor had access to company inventory. He was short inventory on another company he worked for, and borrowed from another company.

Internal Controls – Accounts Payable

Internal Controls – Accounts Payable

Cash Disbursements Best Practices

- Pay from original invoices. Invoice copies should be verified against records to prevent duplicate payments.
- Deface invoice upon payment.
- Require a W-9 from all vendors.
- Checks should not be returned to the person that prepared them.
- ACH payments should be recorded through the Accounts Payable module (not by JE).
- Dual signatures.

Internal Controls – Accounts Payable

Cash Disbursements Best Practices

- **Verification of charges to company credit cards. All charges should have a receipt. Charge should be reviewed for legitimate business purpose.**

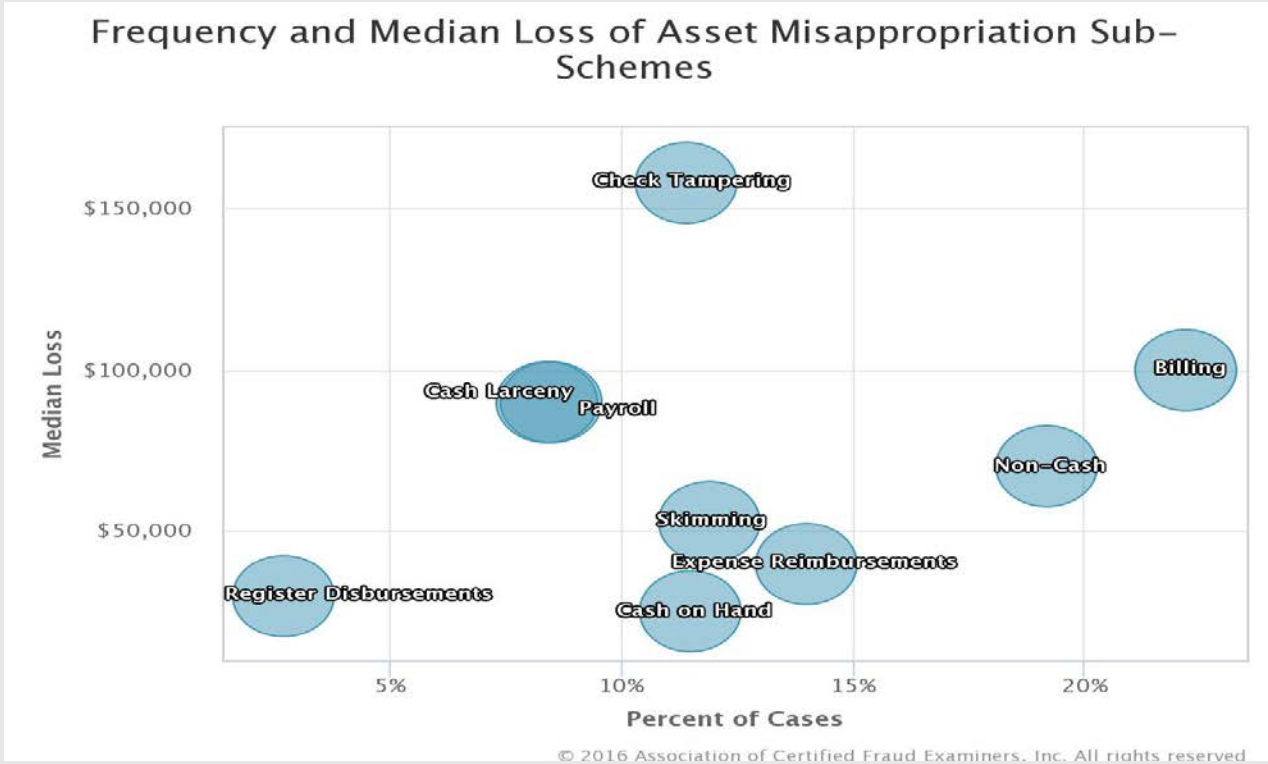
Fraud Finding With Client

Manager used corporate Home Depot card for legitimate business expenses as well as approximately $20,000 for personal charges. She purchased tools and appliances. She ordered a $1,000 safe and had it delivered to her home. She purchased over $6,000 in gift cards.

Internal Controls – Accounts Payable

Cash Disbursements Best Practices

- Obtain original bank statements. Review statements AND contents. Many fraud schemes are a perpetuated by the use of check tampering.



Internal Controls – Accounts Payable

Cash Disbursements Segregation of Duties

- Invoice approval should be performed by someone that does not prepare the disbursements.
- Check signer should be independent of approval and disbursement process.
- Bank reconciliations should be performed by someone independent of check and ACH processing.
- Ensure software permissions are appropriate. As employees promote, terminate or change departments, access should be terminated immediately.

Internal Controls – Accounts Payable

Recent Accounts Payable Fraud Case

Mahopac Volunteer Fire Department

- Treasurer embezzled 5.7 million
- Wrote 275 checks to himself and businesses he owned.
- Concealed by entering checks into ledger under a valid vendor.
- Lavish lifestyle – 55’ yacht, vacation home in Florida, antique fire truck, luxury cars and vacations, $39,000 on jewelry and other purchases.

Corporate Credit Cards

A common fraud risk is an employee using a corporate credit card for personal gain instead of legitimate corporate purchases or travel and entertainment expenses.

Fraud tests can detect credit cards being used to acquire goods and services from vendors with suspect merchant codes (e.g., home supplies, personal entertainment, etc.) and corporate cards being used by employees on weekends or while the employee is on vacation. Additionally, tests can determine whether fuel is purchased in unusually large quantities, mileage charges are made in the same period as rental-car charges, and corporate-card transactions are approved by the card holder.

Recent Fraud Case

Client owned a car lot and a “cash for your title” style loan company. He would sell vehicles, finance, and loan up to $500 on a vehicle if a customer owned the vehicle and could provide a title.

While his office was at the same location, he was often away working on his numerous other business operations for several hours, and had one employee he trusted to make loans, take payments, prepare bank deposit, etc.

Recipe for disaster (Fraud Triangle)

Pressure: Financial Struggles, Family Issues

Opportunity: 90% of the transactions went through her, she was alone with access to cash and the system used to track it.

Rationalization: She felt she was underpaid, overworked. She felt her employer was not doing any “work” to earn the money, that she was doing the majority of the work.

Employee began taking “personal loans” by keeping the payments made by others and posting them later. (Skimming)

She began to get behind on the payments, so she then would apply one customer’s payment to another customer’s account (Lapping)

She then determined a method to post the payment to the customer account and provide the customer with a receipt, then delete the payment in the system which would allow her bank deposit “tie” to the payments made from the system. She would then credit the customer for the payment on the adjustments screen. The adjustments report was not reviewed by management.

The employee began reviewing old customer files that were paid in full and would call to see if they needed a loan. If they said no, she would take out a loan in their name, as they were already customers in the system. She would take the cash for the fictitious loans and retain a portion, pay on some other loans she was manipulating.

The owner noticed a discrepancy when he reviewed a bank deposit, and asked her about it.

She said she must have made an error, or the mechanic stole it (he had no access), then recanted and said she lost a portion of the deposit.

The owner retained her instead of terminating her, as she had been with him for 12 years.

A previous customer came to inquire about a loan, and the owner looked at the system and saw that the customer had an existing loan.

The owner confronted the manager. She was belligerent, said she would not tolerate his accusation and left.

He contacted CBCO, and we reviewed 18 months of data we were able to extract.

Estimated loss just for 18 months was over $90,000.

She has been indicted and the trial will begin soon.

Additional Information

Typically an employee will know if another is stealing. Consider a tip line or a locked drop box where comments can be made anonymously.

Surprise cash counts can help find fraud. Look for checks written by the cashier or other abnormal items.

Fully utilize the tools you have.

Look for odd behavior, changes in lifestyle, discussions on money problems, lavish purchases, odd hours, refusal to train others to assist with duties, lack of vacation days, insistence on being the only one who has access to the bank statement, bullying, etc.

Questions?

If you need any assistance of have any questions, we are always available to help.

Curtis Blakely and Co, PC, CPAs

Charley Albert, CPA/CFE/Shareholder

(903) 758-0734

calbert@cbandco.com