

OUTSMART FRAUD

Strategic Internal Controls to Prevent Business Fraud



GrowthForceTM
put your numbers to work

OUTSMART BUSINESS FRAUD with Internal Controls

Using statistical data from the Association of Certified Fraud Examiner's 2016 "Report to the Nations on Occupational Fraud and Abuse," this whitepaper addresses the impact of fraud on businesses, exposes the most common schemes employed by fraudsters, and outlines the critical steps every business owner must take to deter employee theft.

Fraud Prevention Cannot Be Built On Trust

There are numerous reasons why organizations, particularly small businesses, lack a system of internal controls. A common culprit is limited resources, which can complicate even the simplest of safeguards, such as separation of duties.

While many growth-oriented businesses overlook the importance of implementing systems and strategies designed to reduce their risk, it's certainly a valuable investment when considering the impact of occupational fraud – the typical surveyed organization lost 5% of its annual revenue to fraud, at a median loss of \$150,000 per case.

In addition to mitigating fraud risks, proper internal controls ensure that the flow of information into an accounting system is valid, timely and classified in the right period. High standards net high quality information, from which businesses can make informed decisions and take strategic actions. The overall goal is to make it harder to steal and easier to uncover, however, no system has the power to prevent 100% of crime.

“...the typical surveyed organization lost 5% of its annual revenue to fraud, at a median loss of \$150,000 per case.”

FRAUD FACTS 2016

Report to the Nations

According to the most recent statistic from the Association of Certified Fraud Examiners, smaller organizations are most vulnerable to occupational fraud and continue to suffer the largest median losses. Typically, these organizations have fewer resources than their larger counterparts, often resulting in fewer and less-effective anti-fraud controls. As expected, small business losses have a greater impact on the organization's financial health than they would on larger organizations.

Here are some additional facts about business fraud:

THE TYPICAL SURVEYED ORGANIZATION LOST

5% OF ITS ANNUAL REVENUE TO FRAUD,

AT A MEDIAN LOSS OF

\$150,000

PER CASE.

MORE THAN

23%

OF FRAUD CASES EQUALED/ EXCEEDED

\$1MM IN LOSSES.

40-60%

OF BUSINESSES NEVER RECOVER ANY FRAUD-RELATED LOSSES.

MOST FRAUDSTERS ARE FIRST-TIME OFFENDERS WITH CLEAN RECORDS.

Fraud Scheme Rate, by Size of Victim Organization (1388 cases)

Scheme, Median Loss	<100 Employees	100+ Employees
Billing, \$100K	27.1%	20.9%
Check Tampering, \$158K	20.1%	8.4%
Skimming, \$53K	19.9%	8.9%
Expense Reimbursements, \$40K	16.7%	13.9%
Non-Cash, \$70K	18.8%	19.3%
Cash on Hand, \$25K	16.4%	10.3%
Payroll, \$90K	14.0%	6.3%
Cash Larceny, \$90K	13.5%	6.5%
Financial Statement Fraud, \$975K	12.1%	8.8%

\$3.7

TRILLION IS THE ESTIMATED ANNUAL GLOBAL LOSS DUE TO FRAUD, BASED ON 2011 GWP.

REPORTED CASES OF FRAUD LASTED A MEDIAN OF

18 MONTHS BEFORE DETECTION

EMPLOYEES WORKING IN ONE OF THE FOLLOWING SIX DEPARTMENTS COMMITTED

76% OF ALL FRAUD:

ACCOUNTING, OPERATIONS, SALES, EXECUTIVE/ UPPER MANAGEMENT, CUSTOMER SERVICES AND PURCHASING.

FRAUD IS MORE LIKELY TO BE DETECTED BY AN EMPLOYEE TIP.

1. BILLING FRAUD

\$150,000 median loss per case

The most popular method, billing fraud occurs when an employee submits personal, fake or inflated invoices for goods or services to the employer.

The employee may create a fictitious company and invoice the employer, or may generate new invoices or make multiple payments to a current, albeit non-accomplice vendor. Another billing fraud tactic is submitting bills for personal items purchased by the employee.

The best strategy for combatting billing fraud is to incorporate separation of duties for the various billing and bookkeeping functions. Authorization, record keeping and custody of related assets should be assigned to separate employees – simply put, the person writing the check should not be reconciling the accounts. For growing businesses, this separation may not be feasible, which is a common reason many businesses decide to outsource the bookkeeping and controller aspects of their business. The more eyes on the books, the less appealing your company is to potential fraudsters.

Outsmart Billing Fraud with Internal Controls

- Separate your accounting duties: accounts payable, accounts receivable and check writing/authorization
- Use purchase orders, or enact separate approval on invoices before handing them to the bookkeeper
- Separate bank reconciliation from bill payment
- Use an electronic bill payment system with built-in workflow
- Establish and review an approved vendor list
- Scan bill and link to each transaction inside QuickBooks

2. CHECK TAMPERING

\$158,000 median loss per case

When an employee intercepts, forges or alters a check drawn on your business account, that's check tampering.

Altered Checks – changes the payee to misappropriate the funds

Forged Checks – forges signature or the payee endorsement

Concealed Checks – submits fraudulent check for signature in a batch, and authorized signer neglectfully signs and returns

Authorize Maker – authorized check signer also has access to checks, and misappropriates funds

To combat tampering, check cutting and preparation duties must be separated from check signing responsibilities. It's also imperative that an independent eye, like the owner, manager or outsourced controller, review statements for discrepancies before remitting to the bookkeeper. Businesses should consider outsourcing bank reconciliation if staffing restrictions prevent acceptable separation of duties.

Outsmart Check Tampering with Internal Controls

- Owner/manager reviews unopened bank statement, electronic payments and cancelled checks for authorized payee, signature
- Set up bank accounts for daily transaction download
- Compare payee in accounting system to checks
- Restrict access – data entry staff should not reconcile bank statement
- Switch to electronic checks and/or limit access to paper check
- Rotate employee responsibilities and perform audits
- Review audit trail report for changed payee
- Review budget vs. actual report for unexpected expenses
- Set up positive pay and ACH filters

#3. SKIMMING

\$53,000 median loss per case

Skimming is the theft of unrecorded cash sales and cash receipts before they're recorded on the books.

Instead of applying a customer's payment to the A/R balance, the skimming employee steals the funds and conceals the theft by creating a bad debt or credit memo and applying it to the A/R balance so the customer doesn't appear past due. A less complicated form of skimming is when a store clerk pretends to ring up a transaction, but keeps the cash instead. This can easily be overlooked as an inventory error or customer theft.

The only sure-fire way to prevent skimming is to eliminate cash coming into your office. This can be achieved by outsourcing your accounts receivable and having payments sent directly to your outsourced bookkeeping firm. Otherwise, in cash-rich businesses, good inventory, separation of duties, supervision, and rotating responsibilities are helpful strategies.

Outsmart Skimming Fraud with Internal Controls

- Eliminate cash coming to your office. You may use a lock box; make ACH/EFT payments or have payments sent directly to an outsourced bookkeeping firm.
- Require supervisory approval for A/R write-offs
- If separation of duties is not possible, then create memorized report of credit memos and postings to bad debt account
- Review of audit trail report and require management approval of customer credits and write-offs

4. PAYROLL FRAUD

\$90,000 median loss per case

While a less common scheme, payroll fraud is any scheme in which an employee causes the employer to issue payment based on false compensation claims.

Payroll fraud does affect smaller businesses (14%) at a larger rate than bigger organizations (6.3%), typically because smaller businesses have fewer controls and lack the necessary separation of duties. An employee may inflate hours or overtime on their time sheet, or an employee with payroll access might manipulate wages or issue payment to fictitious employees.

While the size of the organization is certainly a factor if payroll is done in house, this type of fraud can impact both small and large businesses when it comes to employees tracking and logging their hours worked. Therefore, extra attention must be paid towards establishing a system of review to reduce the likelihood for false compensation claims.

Outsmart Payroll Fraud with Internal Controls

- Outsource payroll and require owner/manager approval on payroll changes
- Separate duties: create, review/approve/sign payroll
- Encourage direct deposit or pay cards (no checks to steal)
- Separate bank reconciliation from payroll processing
- Set up positive pay for payroll
- Set ACH filter
- Set up user rights to restrict ability to edit payroll transactions
- Review payroll change reports; gross wages, W-2s
- Background checks

NEXT STEPS

Getting Started

A system of internal controls for fraud prevention is only valuable if it is universally known, universally understood and universally endorsed. Tribal knowledge is not sufficient for ensuring all employees understand policies and procedures. Once a system is adopted, it must be documented in the employee handbook, incorporated into training through standardized procedure manuals, and reinforced through continuing education and appropriate modeling by management. A Fraud Prevention Checklist is a good tool to measure the effectiveness or weaknesses of your current prevention strategies.

Initial Assessment – Questions To Ask

- Do employees understand what constitutes fraud?
- Is it in the employee manual and incorporated into training?
- Does management set the right tone (zero tolerance)?
- Do employees believe they can speak freely?
- Do employees know the proper channels for reporting?
- Are performance goals realistic?
- Are anonymous surveys conducted to assess morale?

Statistical Information Source

2016 Report to the Nations
on Occupational Fraud and
Abuse

<http://www.acfe.com/rtnn.aspx>

Additional Resources

Separation of Duties – 2, 3, or
4 Person Offices

[http://growthforce.com/
presentations/Segregation-of-
Duties.pdf](http://growthforce.com/presentations/Segregation-of-Duties.pdf)

How to Reduce the Risk of Fraud – 5 Simple Steps

[http://growthforce.com/
presentations/5-Steps-to-
Reduce-Fraud.pdf](http://growthforce.com/presentations/5-Steps-to-Reduce-Fraud.pdf)



How to Reach GrowthForce

**Please email info@growthforce.com
or call 281-358-2007.**

GrowthForce would be happy to review your current use of internal controls and make recommendations on how you can improve your business decision-making capability while reducing your risk for fraud.