Spring 5-16-2014

Small Business Occupational Fraud

Judy Dunne
La Salle University, dunnej1@student.lasalle.edu

Deterring Fraud in Small Business

Judith M. Dunne

La Salle University

ABSTRACT

Estimate show that businesses will lose approximately 5% of revenue annually to occupational fraud. A small business generating $5 million in annual revenue will be estimated to lose $250,000 annually to fraud. The small business owners, with only a few employees, do not have the luxury an internal audit department to keep fraud in check. The small business owners must rely on themselves to be the audit department and it has to happen in a cost effective manner. In order to combat the possibility of fraud, the small business owner must first be familiar with the concepts of the fraud models. The fraud triangle theory states that three elements, pressure, opportunity, and rationalization, must be present for fraud to occur. The small business owner can deter fraud by eliminating one of the elements. Opportunity can be weakened with the segregation of certain duties, requiring mandatory vacations, monthly account reconciliations and analysis. Capability, must be considered when evaluating how fraud could occur. Open communication and education of fraud awareness is also a vital tool in deterring fraud. Employees should be made aware that management is conscious of the possibility of occupational fraud and that such actions will not be tolerated. The small business owner does not need to spend a lot of money on fraud deterrence measures. Establishing firm policies, communicating with employees and creating internal controls are all cost effective deterrents to combat the opportunity and capability of occupational fraud.

Small businesses are unique because of their size. This enables them to adapt to customer requests, respond quickly to their competition and provide gainful employment. According to the United States Census Bureau Survey, small businesses (with less than 500 employees) provided employment for 59.8 million people and generated payrolls in excess of 2.2 billion dollars (see Table1). Firms employing 500 people or more provided employment for 60.7 million people and generated payrolls in excess of 2.8 billion dollars. Non-employer firms defined in this chart are businesses with no employees or payroll such as solo practitioners.

Table 1

U.S. Census Bureau Survey 2007				
U.S. Census Bureau Survey 2007	Firms and Establishments	Paid Employees	Annual Payroll	Sales or Receipts
All firms	57,170,715	120,604,265	5,026,778,232	30,738,533,467
Non-employer firms	21,708,021	n/a	n/a	991,791,563
Firms with 1 to 499 employees	12,577,567	59,866,924	2,204,837,721	11,380,080,684
Firms with 500 employees or more	1,177,106	60,737,341	2,821,940,511	18,366,661,220

Table1 Note: Data is combined for ease of reading. The full chart can be found in Appendix A

Although the data indicates that small businesses can compete with larger firms, it is also the small business' size that is one of the biggest downfalls. Small businesses are more susceptible to occupational fraud. According to the Association of Certified Fraud Examiners ("ACFE") 2010 Report to the Nations, small businesses are disproportionately victimized by occupational fraud because small organizations are typically lacking in anti-fraud controls compared to their larger counterparts. (Ratley, 2012) Some of their weaknesses against fraud are the lack of available resources or the lack of the basic understanding of the fraud models. Another weakness is the simple attitude that fraud could never occur at their business. Increasing the

small business owner's education and awareness of the two predominant fraud models, specifically the opportunity side of the fraud triangle and the capability side of the fraud diamond, will enable him/her to deter fraud without adding additional resources. Establishing firm policies, communicating with employees and developing consistent internal controls are cost effective deterrents for the small business owner to combat the opportunity and capability of occupational fraud.

The Reason Small Businesses Are Susceptible To Fraud.

In the article "*Fraud Awareness in Small Business"* published in The National Public Accountant, C. Lavery, D. Lindberg, and K. Razaki stated there are three reasons small businesses are considered to be the most vulnerable to fraud. First, the very size of a small business limits its ability to segregate duties or functions related to authorizing, record keeping and physically safeguarding assets. The opportunity to commit fraud is increased when internal controls are weakened by the lack of segregation. Second, smaller businesses often overlook the importance of routine accounting functions such as account reconciliations and specific account analyses. Third, the management and employees of the company may not have adequate fraud awareness. It is also very common for the management of smaller businesses to believe that the close relationships that exist among the employees will prevent fraud from being committed. These feelings of trust may in fact create the environment of opportunity to commit fraud.

There is no state or federal legislation that requires a privately held small business to combat fraud. The anti-fraud legislations only apply to publically traded companies. A small business may be required by a commercial lender to produce audited financial statements as part of their loan agreement. If a small business is required to produce such statements, an independent certified public accountant would be required to conduct an audit of the statements in accordance with Generally Accepted Auditing Standards and specifically Statement on

Auditing Standards No. 99: Consideration of Fraud ("SAS 99"). SAS 99 is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants and became effective for audits of financial statements produced after December 15, 2002. (AICPA, 2002) SAS 99 requires auditors to consider fraud and identify risks of material misstatement due to fraud. SAS 99 does not require a full fraud audit of the business; it is a guideline for auditors when rendering an opinion on the factual accuracy of the financial statements. In the process of conducting such an audit occupational fraud may be discovered; however if a small business is not required by a lender to produce audited financial statements, the burden of combating fraud falls to the small business only.

Cost of Fraud to the small business owner

The ACFE has produced a biennial survey since 2002 entitled "Report to the Nations on Occupational Fraud and Abuse" that is based on actual cases reported by Certified Fraud Examiners ("CFE") throughout the world. The 2012 report reflects data from 1,388 occupational fraud cases that were reported by the CFE's that investigated them. The 2010 report reflects data from 1,843 cases. Participants of the survey estimate that the typical organization will lose 5% of revenue to fraud each year. Applied to the 2011 Gross World Product, 5% loss translates to potential annual fraud loss of $3.5 trillion. (Ratley, 2012) The median loss caused by fraud in the 2012 survey was $140,000 and the fraud lasted approximately 18 months before detection.

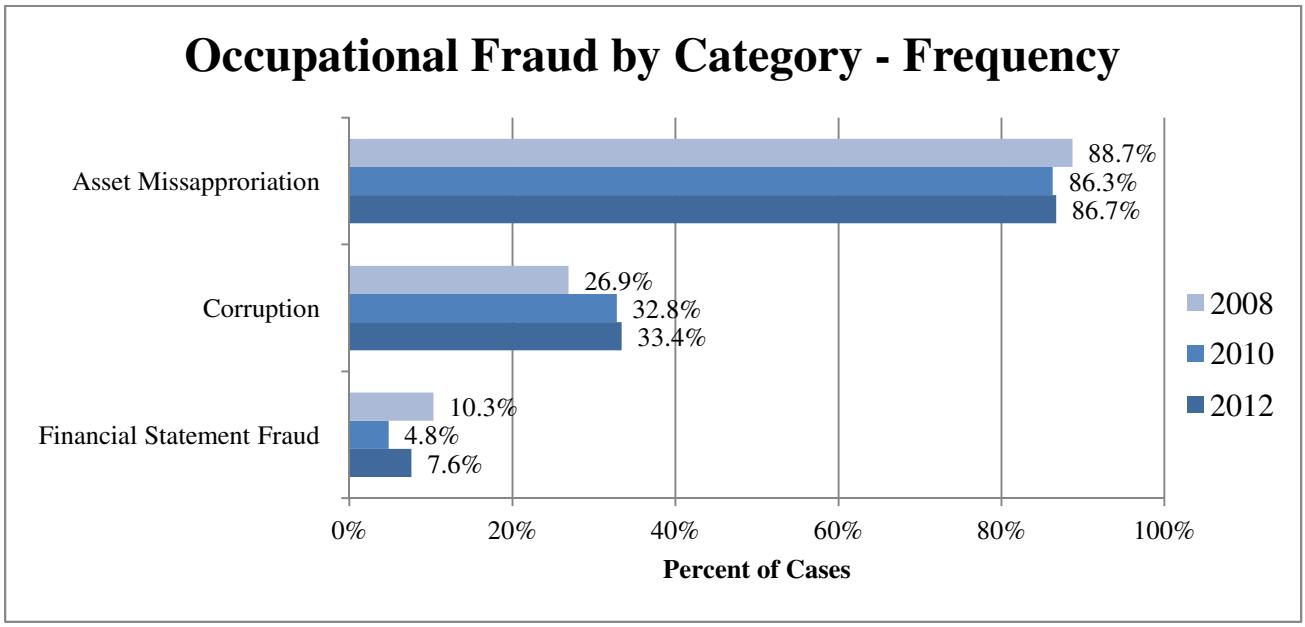
The ACFE research indicates that occupational fraud falls into three categories:

1. Asset misappropriation schemes: An employee steals or misuses the company resources (e.g. theft of cash, false billing schemes or inflated expense reports.)

2. Corruption schemes in which an employee misuses his/her position within a business transaction in order to gain a direct or indirect personal benefit (e.g. bribery or conflicts of interest.)
3. Financial statement fraud: An employee intentionally causes a misstatement or omission of material information in the business financial reports (e.g. recording fictitious revenue, understating expenses, inflating assets.)

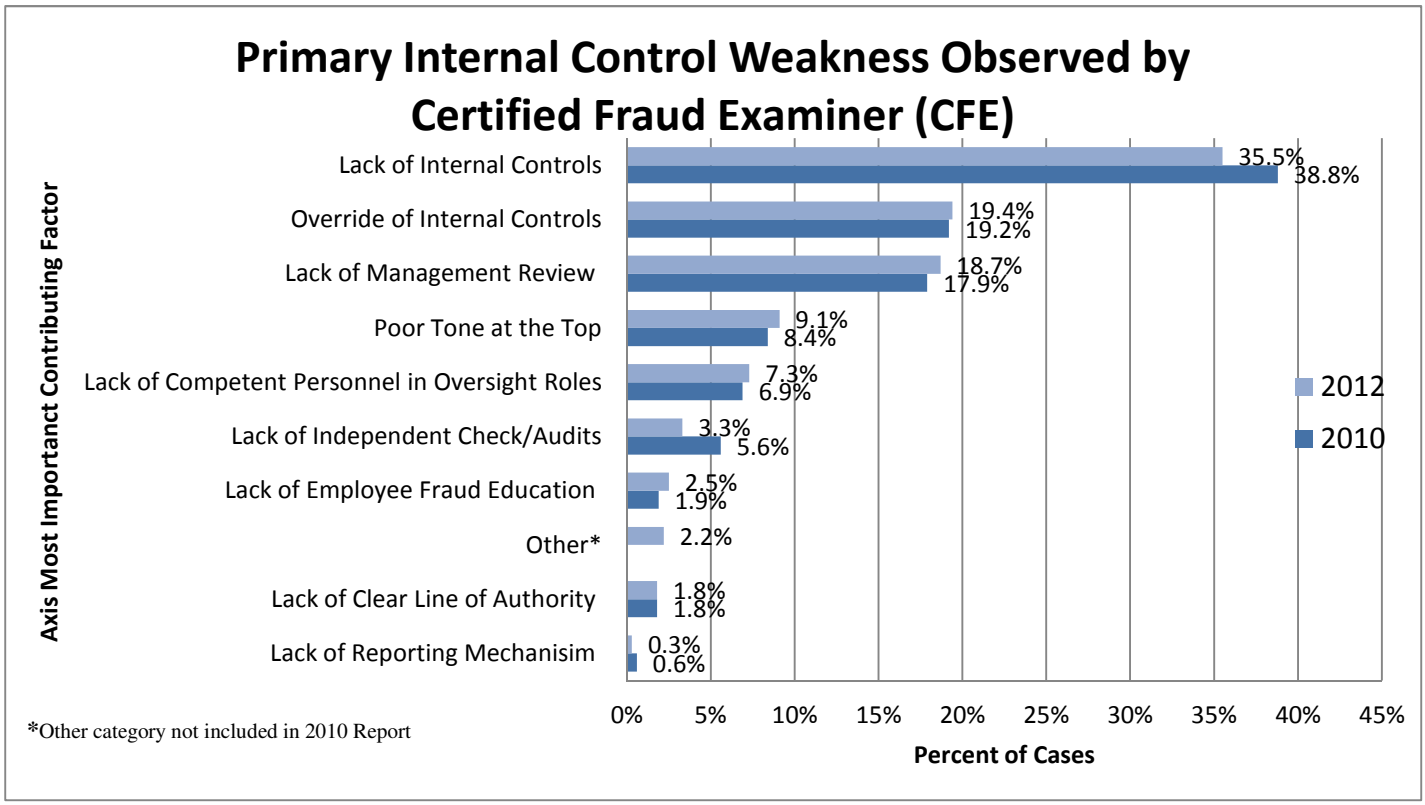
The chart below reflects data from the ACFE reports issued in 2012, 2010 and 2008. In the last three years the survey was conducted, asset misappropriation was the most prevalent fraud detected and is the easiest to commit against a small business.

Table 2



The ACFE survey revealed that occupational fraud is a significant threat to small businesses. The smaller businesses within the study suffered the largest losses because they employ fewer anti-fraud controls which increase the opportunity for fraud to occur. Comparing data from the 2012 and 2010 surveys, lack of internal controls represents the largest weakness observed by CFE's in fraud cases followed by overriding internal controls and lack of management review.

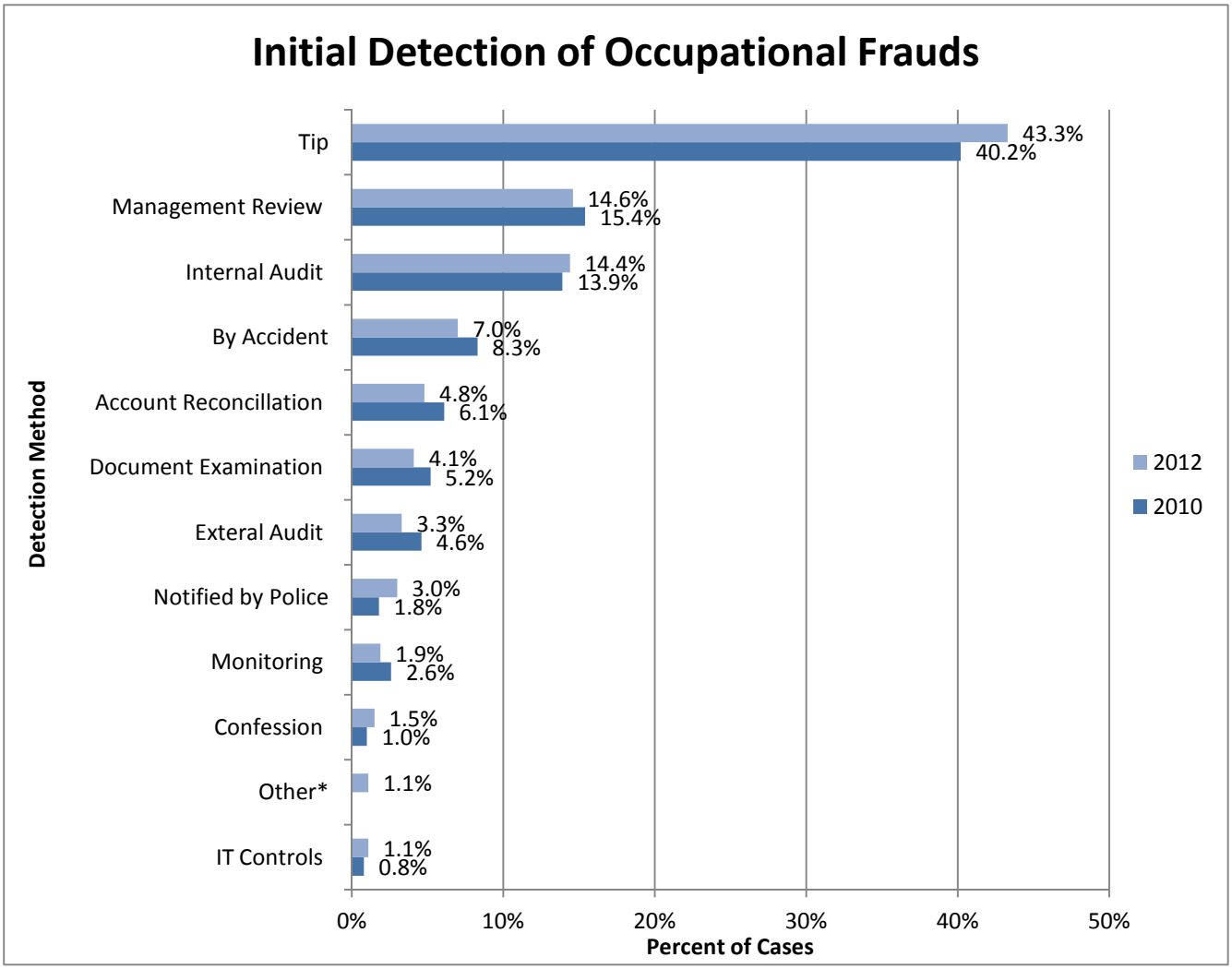
Table 2



The detection of occupational fraud cases is often a critical moment for the small business. Decisions must be made quickly to mitigate losses and a thorough investigation must be completed. The method of detection can open or close several options for a business. The outcome may vary substantially if management learns of an alleged fraud from an anonymous source as opposed to law enforcement. (Ratley, 2012) The ACFE survey results indicate that a tip is still the most prevalent trend in detecting frauds. Of the cases described in 2012 and 2010,

reporting a tip of the alleged fraud was highest the detection method at 43.3% and 40.4% respectively.

Table 3



*Other category not included in 2010 Report

The detection tip percentage is further broken down in the list below. Tips from employees to management or a person of authority regarding occupational fraud occurring at the business was at 50% followed by information from a customer at 22.1% and an anonymous tip at 12.4%. Education of employees on definition of fraud and developing a procedure that will allow employees to make a report when they notice something will only increase that number.

Source of Tips	
Employee	50.9%
Customer	22.1%
Anonymous	12.4%
Other	11.6%
Vendor	9.0%
Shareholder/Owner	2.3%
Competitor	1.5%

The Fraud Triangle and Fraud Diamond

Before discussing the deterrents to occupational fraud in the small business, knowledge of why an employee may commit fraud must be understood. The Fraud Triangle and The Fraud Pyramid are models for explaining factors.

The fraud triangle originated from Donald Cressey's hypothesis published in "Other People's Money: A Study in the Social Psychology of Embezzlement." Cressey's theory discusses persons of trust having a non-sharable financial problem or pressure. This problem can be secretly resolved by violating the position of trust by using the opportunities available to them. Finally, the perpetrator adjusts his/her conceptions of himself/herself or rationalizes the use of the entrusted funds for his/her own use. This hypothesis became known as the Fraud Triangle.

Image courtesy of Association of Certified Fraud Examiners

Pressure: The first side of the triangle is represented by need for money, whether actual or just the desire for it. (Kapp/Heslop, 2011) The pressure serves as the spark to motivate the potential fraudster to start investigating and weighing the options of occupational fraud.

Opportunity: The second side of the triangle represents the ability to commit fraud with little or no probability of the potential fraudster getting caught. The opportunity is improved by weak internal controls or an employee having direct access to liquid assets such as cash, with little or no oversight. (Kapp/Heslop, 2011)

Rationalization: The third side of the triangle is the potential fraudster's justification of the act. (Kapp/Heslop, 2011) Some examples of rationalizations are:

"This is only a loan, I will pay it back"
"I am providing for my family."
"My employer is underpaying/cheating me."
"My employer is dishonest to others. They deserve to be fleeced"

Another theory that expands on the fraud triangle is the fraud diamond. The fraud diamond theory, introduced by David Wolfe and Dana Hermanson, enhanced Cressey's fraud triangle by adding another side entitled capability

Image courtesy of The Ohio Society of CPAs

Wolf and Hermanson, through their experiences in investigating frauds, proposed that not only do the pressure, need and rationalization need to be present to commit fraud, but capability. (Wolf and Hermanson, 2004) Capability is someone with a high position/function, high intelligence, confidence/ego, and good coercion skills. The person must also be a convincing liar and be immune to the inherent stress brought on by perpetrating a fraud.

1. A person's position with the company may create the opportunity for fraud not available to others. The higher the person's function gives the potential fraudster more information of the company systems and access to them.
2. The person committing fraud is smart enough to understand and exploit internal controls and weakness and to use their position and authorized access within the company to the greatest advantage.
3. The fraudster must have a strong ego and great confidence that he/she will not be detected or they believe they can talk their way out of the matter if discovered.
4. Successful fraudsters can coerce others to commit or conceal fraud. A strong personality can convince someone else to go along with the fraud or at a minimum look the other way and stay quiet.
5. Fraudsters must be effective liars. To avoid detection, they must look auditors, supervisors and others in the eye and lie convincingly. They must also have the skills to keep track of the lies so their story remains consistent.
6. Committing and managing fraud is stressful. Risk of detection, the possible personal ramifications and the need to conceal the fraud on a daily basis are all stress factors that must be managed by the fraudster.

Case: TeriLyn Norwood

TeriLyn Norwood was the ideal employee. The office worker, who kept taking on more responsibilities just because the jobs needed to be done, was becoming more trusted by her employer. In no time at all she was completely in charge of the human resource and accounts payable functions for a small truck manufacturing company in Hartford Connecticut. (Wilder, 2005) Unbeknownst to her employer, Norwood's personal life was in turmoil. She had recently gone through a divorce and owed back child support in the amount of $20,000. Under California law, Norwood had to pay the back child support or serve a jail sentence. She approached her employer inquiring about financial assistance and was denied. The pressure was mounting. Norwood saw no other way out and embarked on a four month scheme in which she stole $18,000 from her employer. (Wilder, 2005)

The asset manipulation was quite easy. She just simply placed a label with her name on company check over the original payee's name. Prior to her first theft, Norwood evaluated the probability of her employer discovering her fraud and found it to extremely low. Norwood was aware that the office manager only balanced the bank account off of the bank statement and check run produced by the accounting system. The office manager never bothered to look at the actual cancelled checks. (Wilder, 2005) Norwood saw a weakness in the accounting cycle as her opportunity to steal. Norwood's fraud was not discovered through internal controls but rather by meticulous bank teller. The bank teller simply lifted the label off of the check and revealed the actual payee of the check. (Norwood, 2003) Norwood was convicted of embezzlement and sentenced to two years in prison.

A positive pay system instituted at Norwood's employer would have discovered the fraud immediately. At a minimum, management should be reviewing the bank statements and the

actual cancelled checks. Knowing there was a positive pay system in place would have most likely stopped Norwood from attempting the theft in the first place. The opportunity would not have been available to her.

After the incident, Norwood's employer emphasized attempting theft would be met with serious consequences; the next employee at Norwood's old position also stole from the company. As a result, the employer now has outsourced the accounts payable and receivable functions for the company. (Wilder, 2005)

Case: Amy Wilson

Amy Wilson was the office manager for a small manufacturing firm in Indiana. Wilson was described as a hard worker. She came in early and stayed late. Her employer was confident in leaving the day to day operations of the business in her hands while he enjoyed the fruits of his labors. Wilson found that her theft was easy because her employer was not interested in internal controls. The one control in place was that Wilson did not have check signing privileges.

Wilson's pressure arrived in the form of legal trouble for one of her children. There was an altercation with the law and she needed funds to pay an attorney to represent her son in court. (Wilson, 2013) Since she was in charge of all aspects of accounts payable she simply made a check out to herself in the accounting system test module and forged an authorized signature. Wilson vowed to herself that it was only a loan and she would repay the funds as soon as possible. (Wilson, 2013) Her son's legal problems were resolved and no one noticed the missing funds. Wilson soon found she became addicted to the money. She began to use the funds for personal items such as to pay her monthly credit card bill and to help friends and

family that encountered financial hardships. In Wilson's own words, she became "An overachiever and people pleaser, I thrived on their appreciation of 'my generosity' and on my status as their savior." (Wilson, 2013)

Wilson hid her fraud in a cost of goods account for her employer's largest customer. When the CPA firms noticed the increase in the account activity over the previous year, they suggested doing a more detailed analysis. The employer rebuked the suggestion stating it was a waste of money. (Wilson, 2013) It was not her employer, internal controls or the outside CPA firm that discovered Wilson's theft; it was her own credit card's fraud department. They had noticed that the payments were being made with a company check and contacted the employer. Wilson embezzled over $345,000 from her employer over a four year period and pled guilty to eight counts of forgery and theft and was sentenced to six years in prison.

In both the Norwood and Wilson cases, the small business owners failed to recognize opportunities for fraud within their systems or the capabilities of employees working for them. Norwood's and Wilson's employers used trust as an internal control and it failed. Both Norwood and Wilson served their jail sentences and now have to explain to future employers that they are convicted felons. Both women also work as motivational speakers for The Pros and The Cons, an organization that educates businesses on fraud prevention using both industry professionals and those convicted of fraud crimes. (http://www.theprosandthecons.com/)

Case: U.F.C.W. Local 1776.

United Food and Commercial Workers Local 1776 ("The Local") employed 75 people in Pennsylvania, three of whom made up the accounting department, which was responsible for $14 million in revenue each year. The Local utilized a very manual system. Schedules were still

completed by hand and then analyzed. Information had to be compiled from two or three different systems to get information needed for simple transactions such as bank account reconciliation. Over the years some automation of the systems was implemented to improve efficiency, and with every request made to a supervisor, it was answered with "do whatever needs to be done." The only request that was constantly denied was additional help. The Controller had autonomy over all matters financial and the complete trust of management and the governing board.

The Local was required by its financial lender to produce audited financial statements yearly. Once per year, an independent auditor would verify the financial statements. The Local used the same auditor for 12 years. Since the Local is not a publically traded company, they were not required to rotate audit partners as required by Sarbanes Oxley Act ("SOX"). The auditor's main job was to verify the accuracy of the statements, not to detect fraud. They did modify some of their methods after the enactment of SOX and the issuance of SAS 99, including requesting last minute schedules of accounts not normally analyzed, and asking the accounting department staff if they were aware of any fraud.

Humans are creatures of habit and that includes auditors. Every year there were specific accounts that were requested for more detailed analysis during the audit. The high volume accounts that were the heart of the financial statements were always in the review. Smaller accounts that had a significant difference, approximately 5%, in the account balance from the previous year would require specific information or at least an explanation to the auditors. If an account had a percentage difference under 5% from the previous year, the auditors would not question it. Those accounts were the best place to conduct any fraud.

The Controller instituted certain internal control policies to protect the Local from possible fraud.

1. A request was made to utilize another person from a different department to check in the cash receipts and make deposits. The work did not require a full time person and it added another layer of separation for the accounting staff.

2. A policy was written that all nonrecurring payables over $500.00 have approval of a department head and an executive committee member. Normal and reoccurring payables such as the electric and phone bills were only reviewed by the Controller but the invoice presented from a local auto repair shop required two signatures on it before the invoice would be released for payment.

3. All charges to the corporate credit card also had to have two signatures of a department head and an executive committee member before it would be processed.

4. Only two members of the accounting staff could enter a new vendor in the system. If the Controller was unavailable to do it, a report could be generated for review by management.

The Controller reported no incidents of occupational fraud within the accounting department.

Case: Intercool, Inc.,

Intercool, Inc. located in Carrollton, Texas, does approximately 7 million dollars a year in construction and leasing sales with 12 full time employees. At Intercool, the Controller is the

accounting department, including receivables, invoicing, entering and paying accounts payables, reconciling the bank account and creating the payroll files. At no time was a background or credit check conducted on the Controller. Trust is the internal control.

In order to deter fraud, Intercool is considering:

1. Segregation of duties. Any segregation of the accounting function would be an improvement. One person should not be responsible for the entire accounting cycle; checks and balances are needed.

2. A positive pay system. Intercool management should implement a positive pay system. The larger financial institutions offer this service at little or no cost to the customer.

3. Diligence with accounts receivable. Intercool management needs to be more diligent with accounts receivable in the leasing business. Management is fully aware of the funds owed in the construction and design side of the business. They are dealing with much larger invoices and receivables. The leasing side is vulnerable because the funds arrive in much smaller increments. It would be easy to divert a few hundred dollars here and there from customers into a bank account that was not the Company's.

The Controller and management have discussed the issue of segregation of duties which is a critical need. They agree it is an issue and it does not make good business sense to leave the organization so vulnerable. Future discussions are planned to improve the situation. Although Intercool has not had any known issues with occupational fraud in the past, there are

suggestions of a $100,000 embezzlement from about seven years ago that have not been substantiated.

Trust should not be used as a valid internal control. Both Local 1776 and Intercool both used trust as an internal control, but this needs to be augmented with practices and procedures to reduce potential fraud.

Best practices for the Small Business Owner.

Fraud affects small-sized companies because there is often a high level of trust among management and staff. This raises the confidence of the would-be perpetrators because they do not believe anyone would ever suspect them of fraud. Familiarity breeds a level of complacency that results in a higher susceptibility to fraud. Implementing good business practice involves identifying the critical responsibilities that must be done to keep a business in working order, and having the discipline to ensure that those tasks are carried out consistently and regularly. A best practice is just an improvement over existing systems and in this case the best practice is to deter occupational fraud. Small businesses can implement best practices through policies and oversight that are an inexpensive way to combat fraud. Some examples of best practices are:

1. Separate as much of the accounting functions as possible. One person should not be responsible for an entire accounting cycle. If segregation of duties is not feasible due to the lack of staffing, then consider job rotations. Job rotations will limit the opportunity for fraud by having employees cross check others work on a monthly basis.

2. Implement dual signatures on checks/Positive Pay Systems. Requiring multiple signatures on payment instruments is in itself a check and balance. Two sets of

eyes are reviewing every check leaving the business. If dual signatures are not feasible, a positive pay system will allow the financial institutions to be the second review. Any discrepancies to the positive pay system must be reported to someone other than the person in charge of the accounts payable function.

3. Conduct background and credit checks on anyone handling company funds. Employees with credit problems could be potential problems for the small business owner. (Johnston/Spencer, 2011)

4. Require mandatory vacations of accounting staff. It is a red flag if the employee does not want to be away from the office. (Laufer, 2011) Fraudsters need to control the scheme and must be present to do so. Another employee covering their desk while the fraudster is away risks detection of the fraud.

5. Restrict the use of company credit to all employees. Make a policy that advance approval must be obtained prior to using the credit. Request original receipts from employees and have management review the monthly statements.

6. Management must review key reports on a regular basis. This review should include potential fraud areas such as new vendors, credit memos, inventory write off and bad debt reports on a regular basis.

7. Accounts need to be reconciled in a timely fashion. Cash accounts are extremely susceptible to fraud and should be reviewed consistently for accuracy.

Even in the absence of actual internal controls, the perception that the owner is checking up on business operations can serve as a deterrent. (Kapp, 2011) Best practices are not just about

getting your businesses in order, it is about setting up your business for the challenges and opportunities it will face in the future.

Open communication

The small business owner can use communication to prevent fraud. By discussing it openly within the entire organization it may give pause to a capable employee who has seen an opportunity within the system to commit fraud. Some examples of open communication are:

1. Conduct basic fraud awareness training. Gather all the employees and discuss what is expected and how an employee can report a suspected fraud. (Biery, 2012)

2. Periodically remind employees of fraud awareness. Forward recent news articles of occupational fraud with the reminder that every employee is responsible for preventing and detecting fraud. (Biery, 2012)

3. Write a mission statement that is focused on ethics and the intention of a fraud-free work environment. (Lefebvre, 2012)

Setting a clear and open tone from the top of the business stating that fraud will not be tolerated is an inexpensive way for the small business to combat fraud. The potential fraudster will see fewer opportunities if management is openly communicating that they are aware of frauds and are actively looking to prevent it.

Conclusion

The ACFE survey of fraud examiners estimates that businesses will lose approximately 5% of revenue annually to occupational fraud. A small business creating $5 million in annual revenue will be estimated to lose $250,000 annually to fraud. Small businesses are found to be

disproportionately victimized by occupational fraud because they are typically lacking in anti-fraud controls compared to their larger counterparts. Small businesses do not have the structure or guidelines of state or federal legislation to assist them in the fight against occupational fraud; therefore, they must take it upon themselves to deter it prior to it occurring. In order to combat the possibility of fraud, the small business owner must first be familiar with the concepts of the fraud models. The fraud triangle theory states that three elements, pressure, opportunity, rationalization, must be present for fraud to occur. The small business owner can deter fraud by eliminating one of the elements. Opportunity can be weakened with the segregation of certain duties, requiring mandatory vacations, monthly account reconciliations and analysis. The fraud diamond adds a fourth element, capability, which must be considered when considering how fraud could occur. The small business owner should explicitly assess the capabilities of key personnel with background and credit checks. There is also no substitute for spending some time with a person to gain insight. When and if an employee's capabilities present significant risk factors, the small business owner must respond with stronger internal controls or enhanced audit testing.

Implementing best practices, openly communicating and educating staff on fraud awareness is also a vital tool in deterring fraud. Staff should be trained on what to look for and devise a system of how fraud can be reported if it is discovered. Employees should be made aware that management is conscious of the possibility of occupational fraud and that such actions will not be tolerated. Opportunity for a potential capable fraudster is further closed when the employee believe they may get caught.

The small business does not have to tackle the issue of fraud deterrence alone. There are organizations, for example the ACFE, that offer free information such as the fraud check list

attached in Appendix B, that can be used as a guideline in setting up fraud deterrence practices. The small business owner does not need to spend a lot of money on fraud deterrence measures. Establishing firm policies, communication with employees and consistent internal controls are all cost effective deterrents to combat the opportunity and capability of occupational fraud.

References

American Institute of Certified Public Accountants. *AU Section 316 Consideration of Fraud in a Financial Statement Audit*) Source: SAS No. 99; SAS No. 113. Retrieved from http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00316.pdf

Biery, M. E. (2012). Five ways small businesses can fight fraud. *CPAPracticeAdvisor.Com,* Retrieved from http://search.proquest.com/docview/1424443439?accountid=11999

Cressey, Donald R. 1973. *Other People's Money* Montclair: Patterson Smith, p. 30.

Kapp, L. A., & Heslop, G. (2011). Protecting small businesses from fraud. *The CPA Journal, 81*(10), 62-67. Retrieved from http://search.proquest.com/docview/900317892?accountid=11999

Laufer, D. (2011). Small business entrepreneurs: A focus on fraud risk and prevention. *American Journal of Economics and Business Administration, 3*(2), 401-404. Retrieved from http://search.proquest.com/docview/1025014883?accountid=11999

Lavery, C. A., Lindberg, D. L., & Razaki, K. A. (2000). Fraud awareness in a small business. *The National Public Accountant, 45*(6), 40-42. Retrieved from http://search.proquest.com/docview/232344331?accountid=11999

Lefebvre, R. (2012). Small businesses are mostly oblivious to fraud. *Bottom Line, 28*(5), 17. Retrieved from http://search.proquest.com/docview/1015209442?accountid=11999

Norwood, T. (2003) How an honest employee crossed the line. *White Collar Crime Fighter, 5(11).* Retrieved from http://www.theprosandthecons.com/TerlLynn_Norwood_WCCF.pdf

Ratley, James D. 2010. Report to the Nations on Occupational Fraud and Abuse. *2010 Global Fraud Study.* Retrieved from http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/rttn-2010.pdf

Ratley, James D. 2012. Report to the Nations on Occupational Fraud and Abuse. *2012 Global Fraud Study.* Retrieved from http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

Ratley, James D. 2012. Report to the Nations on Occupational Fraud and Abuse. *2012 Global Fraud Study.* Fraud Checklist. Retrieved from http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

United States. Department of Commerce. United States Census Bureau. (2012, August) *Statistics about Business Size (including Small Business) from the U.S. Census Bureau.* Retrieved March 31, 2014 from the United States Census Bureau website: http://www.census.gov/econ/smallbus.html

Wilder, B. (2005). Who's afraid of fraud. *Catalyst (2002),* , 28-31. Retrieved from http://search.proquest.com/docview/219412810?accountid=11999

Wilson, Amy. (2013) Deceit, lies and embezzlement. *Minnesota Society of Certified Public Accountants Feb-Mar 2013.* Retrieved from http://www.mncpa.org/publications/footnote/2013-02/deceit-lies-and-embezzlement.aspx

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal, 74*(12), 38-42. Retrieved from http://search.proquest.com/docview/212311888?accountid=11999

Appendix A

United States Census Bureau

Table 2b. Employment Size of Employer and Nonemployer Firms, 2007

Introductory text includes scope and methodology. Table includes both establishments with payroll and nonemployers. For descriptions of column headings and rows (industries), click on the appropriate underlined element in the table.

Employment size of enterprise	Firms	Establishments	Paid employees	Annual payroll ($1,000)	Sales or Receipts ($1,000)
All firms	**27,757,676**	**29,413,039**	**120,604,265**	**5,026,778,232**	**30,738.533,467**
Nonemployer firms	21,708,021	21,708,021	n/a	n/a	991,791,563
Employer firms	**6,049,655**	**7,705,018**	**120,604,265**	**5,026,778,232**	**29,746,741,904**
Firms with 1 to 4 employees (or with no employees as of Mar 12)	3,705,275	3,710,700	6,139,463	234,921,325	1,434,680,823
Firms with 5 to 9 employees	1,060,250	1,073,875	6,974,591	222,419,546	1,144,930,232
Firms with 10 to 19 employees	644,842	682,410	8,656,182	292,088,277	1,395,498,431
Firms with 20 to 99 employees	532,391	723,385	20,922,960	768,546,555	3,792,920,977
Firms with 100 to 499 employees	88,586	355,853	17,173,728	686,862,018	3,612,050,221
Firms with 500 employees or more	18,311	1,158,795	60,737,341	2,821,940,511	18,366,661,220
Firms with 500 to 749 employees	6,094	71,702	3,695,682	152,059,022	800,475,934
Firms with 750 to 999 employees	2,970	45,990	2,561,972	109,833,289	636,199,229
Firms with 1,000 to 1,499 employees	2,916	59,311	3,552,259	153,957,992	792,993,702
Firms with 1,500 to 1,999 employees	1,542	46,221	2,664,416	120,606,441	695,739,349
Firms with 2,000 to 2,499 employees	942	36,388	2,094,728	94,001,450	544,038,807
Firms with 2,500 to 4,999 employees	1,920	118,282	6,687,266	320,640,371	1,979,674,138
Firms with 5,000 employees or more	1,927	780,901	39,481,018	1,870,841,946	12,917,540,061
Firms with 5,000 to 9,999 employees	952	115,222	6,628,415	324,791,017	2,263,012,551
Firms with 10,000 employees or more	975	665,679	32,852,603	1,546,050,929	10,654,527,510

While most of these data are published every year, receipts data are available for employers only for the years for which an economic census is taken (2007, 2002, 1997).

Source: Statistics of U.S. Businesses (See industry and state detail) and Nonemployer Statistics

Economic Census Establishment and Firm Size reports, present national data classified by NAICS industry.

http://www.census.gov/econ/smallbus.html

Appendix B

ACFE
Association of Certified Fraud Examiners

Fraud Prevention Checklist

The most cost-effective way to limit fraud losses is to prevent fraud from occurring. This checklist is designed to help organizations test the effectiveness of their fraud prevention measures.

1. **Is ongoing anti-fraud training provided to all employees of the organization?**
   - ❑ Do employees understand what constitutes fraud?
   - ❑ Have the costs of fraud to the company and everyone in it — including lost profits, adverse publicity, job loss and decreased morale and productivity — been made clear to employees?
   - ❑ Do employees know where to seek advice when faced with uncertain ethical decisions, and do they believe that they can speak freely?
   - ❑ Has a policy of zero-tolerance for fraud been communicated to employees through words and actions?
2. **Is an effective fraud reporting mechanism in place?**
   - ❑ Have employees been taught how to communicate concerns about known or potential wrongdoing?
   - ❑ Is there an anonymous reporting channel available to employees, such as a third-party hotline?
   - ❑ Do employees trust that they can report suspicious activity anonymously and/or confidentially and without fear of reprisal?
   - ❑ Has it been made clear to employees that reports of suspicious activity will be promptly and thoroughly evaluated?
   - ❑ Do reporting policies and mechanisms extend to vendors, customers and other outside parties?
3. **To increase employees' perception of detection, are the following proactive measures taken and publicized to employees?**
   - ❑ Is possible fraudulent conduct aggressively sought out, rather than dealt with passively?
   - ❑ Does the organization send the message that it actively seeks out fraudulent conduct through fraud assessment questioning by auditors?
   - ❑ Are surprise fraud audits performed in addition to regularly scheduled audits?
   - ❑ Is continuous auditing software used to detect fraud and, if so, has the use of such software been made known throughout the organization?
4. **Is the management climate/tone at the top one of honesty and integrity?**
   - ❑ Are employees surveyed to determine the extent to which they believe management acts with honesty and integrity?
   - ❑ Are performance goals realistic?
   - ❑ Have fraud prevention goals been incorporated into the performance measures against which managers are evaluated and which are used to determine performance-related compensation?
   - ❑ Has the organization established, implemented and tested a process for oversight of fraud risks by the board of directors or others charged with governance (e.g., the audit committee)?

5. **Are fraud risk assessments performed to proactively identify and mitigate the company's vulnerabilities to internal and external fraud?**

6. **Are strong anti-fraud controls in place and operating effectively, including the following?**

   - ❑ Proper separation of duties
   - ❑ Use of authorizations
   - ❑ Physical safeguards
   - ❑ Job rotations
   - ❑ Mandatory vacations

7. **Does the internal audit department, if one exists, have adequate resources and authority to operate effectively and without undue influence from senior management?**

8. **Does the hiring policy include the following (where permitted by law)?**

   - ❑ Past employment verification
   - ❑ Criminal and civil background checks
   - ❑ Credit checks
   - ❑ Drug screening
   - ❑ Education verification
   - ❑ References check

9. **Are employee support programs in place to assist employees struggling with addictions, mental/emotional health, family or financial problems?**

10. **Is an open-door policy in place that allows employees to speak freely about pressures, providing management the opportunity to alleviate such pressures before they become acute?**

11. **Are anonymous surveys conducted to assess employee morale?**