MPN INC.

Business Ownership White Paper

EMPLOYEE FRAUD

Case Studies of Typical Scams

© 2011 John F. Dini
CMBA, CExP, CBI

Why a White Paper?

A white paper is an authoritative report to educate and assist people in making decisions. I issue white papers when the subject matter is important to business owners, but it is too technical or complex to address in the length of an article or blog posting.

EMPLOYEE FRAUD
CASE STUDIES OF TYPICAL SCAMS

OVERVIEW: EMPLOYEE FRAUD IS WIDESPREAD

Privately held businesses are especially exposed to employee fraud. Often the issue is size; there simply aren't enough employees to effectively divide responsibilities and install appropriate checks and balances. Other times it is the closeness of employees, their tenure and relationship with the owner that encourages lax controls and oversight.

In every case, the issue is the same:

No employer was ever defrauded by an employee he or she didn't trust.
Put plainly, and employee has to first have access to something worth stealing. Without that access, there is no theft.

All employee fraud stems from three conditions, each or which is present in every case.

> *Need* (or motive): Between 10% and 15% of employees steal because they want to. Their need is to prove they are smarter, or can get something for nothing. Another 10% to 15% will never steal. Their need to feel honest and good about themselves trumps any temptation. The remaining 70% to 80% steal because they are pressed by outside financial strains, or because they are seeking revenge, or sometimes just because they can.

Opportunity: This is where my comment about "trust" comes in. There are few cases where an employee takes something that will be immediately noticed, although it sometimes happens. Most fraud occurs where it won't be easily missed, or at least not right away. Systems are for keeping honest employees honest, by making it riskier for them to do anything else.

Rationalization: This is different from motive. In most cases, an employee under financial pressure thinks "I'll put it back as soon as I get financially stable again."
It starts out as a "loan." Other times it is an employee's self-explanation of what is "fair." "She does less work than me and gets paid more. That's not fair." Or "I should have gotten a bigger raise. That's not fair." Sometimes the rationalization is that revenge is appropriate, but most often it is a justification that the defrauded value was earned.

In a meeting of constants who specialize in working with business owners, we discussed how many of our clients had experienced fraud. The general consensus was between 65% and 75%. The more cynical of us said that the rest had merely not discovered it.

Employee fraud is a common and recurring issue in the day to day running of the business. Any employer who says "We don't have people in our company who would steal" is evidencing the highest form of arrogance- a belief that he or she has the ability to unerringly see inside the soul of each new hire.

What follows are 5 true examples of employee fraud, and a personal story. There are hundreds more, but these may help you to understand how creative and diligent people can be at doing things they shouldn't.

These are true stories. Every one of them actually happened to a business owner that we have worked with. They are not unusual occurrences. The owners had decent systems in their businesses. They thought the checks and balances in their companies worked.

Most importantly, each of the thieves was a trusted employee. The examples happen to be mostly female, simply because the large majority of administrative employees are female. There are plenty of male thefts, but a lot of those are from plants, trucks and warehouses where the process and systems (and the opportunities!) are more obvious.

The people you don't trust are never given the opportunity to steal from you. They are watched more carefully. Every one of these thieves is someone who had the responsibility and the authority to do something that could divert money into their own pockets.

Employee fraud occurs in every business. If you are lucky, it is limited to a few highlighters for the kids or a six-pack of soda from the staff refrigerator. If you are unlucky (or sloppy) it can be enough to put you out of business.

CASES:

Case 1: At 6:30 one evening the owner of an engineering firm needs to check on a paid invoice amount. He goes to the envelope containing cancelled checks on the receptionist's desk which he saw come in the mail that morning. In it, he finds a check made out to his receptionist for several thousand dollars. He recognizes his personal signature on the check.

Case 2: A hardware store owner purchases a new computer system. Despite extensive training, his bookkeeper of 15 years cannot implement the software. In tears, she finally resigns. Over the next two months, he finds that the accounts receivable are overstated by $80,000.

Case 3: The owner of a technology company is surfing E-bay for some used equipment. She finds two new computers for sale in her town that exactly match two that she saw delivered for a customer's order the previous day. Subsequent investigation reveals over $300,000 in equipment sold on E-bay by two employees.

Case 4: The owner of an industrial services company receives a call from a collection agency regarding the past due balance on a credit card that the company does not have.

Case 5: An administrative assistant in an advertising agency quits to start her own business. When the owner gets the monthly statement from the office

supply company, it includes thousands of dollars of computers, furniture and supplies that were never delivered.

Case 1: What happened?

How did the owner's signature get on the check? The engineering firm created one check each day to the city regulatory authority for multiple permits and filings. The expenditure was not assigned to individual projects, and whomever was going downtown to the office asked the receptionist to draw a check from accounting for all the permits needed that day..

The receptionist analyzed and discovered the procedure then requisitioned checks for a "typical" amount on days when no permits were actually needed. She wrote the agency's name in as payee using an erasable pen. She then changed the payee to himself, deposited the check and intercepted the cancelled checks so that she could change them back. This scheme was complicated and easily discoverable, yet it still netted the employee over $15,000 in just a few months.

Case 2: What happened?

The hardware store bookkeeper was "floating" receivables. She would deposit collections from customers in an alternate account and then issue a check to herself.

The customers received statements showing that their bills were paid. Over the years, the bookkeeper had developed a complex set of double books.

A more common version of the receivables scam is the phone vendor. The A/R person will set up a dummy vendor, invoice the company and then pay the bill.

Case 3: What happened?

The stolen computers were simply a matter of poor checking procedures. Salespeople submitted purchase orders for customers' equipment. The technicians ordered and installed the equipment but it wasn't checked against the customers' purchase orders.

This case had an added level of fraud. The bookkeeper had been engaged in some minor receivable theft. When the head technician discovered it, he blackmailed her cooperation in the much larger scheme.

Case 4: What happened?

This is a case of poor mail control. A new receptionist opened a credit card offer. She filled it out with herself as the authorized company representative. When it arrived, she immediately charged it to the limit. She destroyed the first few statements. When the collection calls started coming in, she told the collectors that "she" wasn't in the office.

As the pressure increased, she quit without notice and moved out of the state.

Case 5: What happened?

Sometimes you are lucky enough to get a very stupid thief. The misuse of the company charge account showed up in writing within two weeks of the theft. They employee's signature was on the charge slips. The merchandise was delivered to her new business and was clearly still in her possession.

So – an open and shut case that sent the employee to jail, right? Well, not exactly.

The employee's claim, according to her attorney, was that she couldn't have possibly been *that* stupid. The theft was so easily discovered, it must not have actually been intended as a theft. She falsely claimed to have had a conversation with the owner about using the account with an agreement to repay when the bill came due. Her mother submitted a check for payment in full immediately.

Another thief walked away because it was simply too difficult, expensive and time consuming for a business owner to deal with.

CATCHING A THIEF

What happens when you catch an employee stealing? In most cases, the practical business owner is more concerned about recovering the money than getting "justice." They may file charges but negotiate with the defendant or an attorney to drop charges in return for reimbursement. Frequently, they sign a confidentiality agreement as part of the deal.

If you catch a thief, ask yourself whether cutting a deal is really participating in a future theft. Did this employee steal before? We've seen thieves who have

made two or three prior deals for confidentiality. When caught, they started negotiating immediately, so that they could move on and steal again.

If you found that your thief had stolen before, how would you feel towards the previous employer? We all share a responsibility to drive thieves from the workplace.

Assemble your evidence and present it to the District Attorney. He or she will tell you whether they will pursue the case. If not, consider civil litigation for recovery. Remember, if you don't take action, you cannot say that they employee was terminated for theft. They could sue you for defamation.

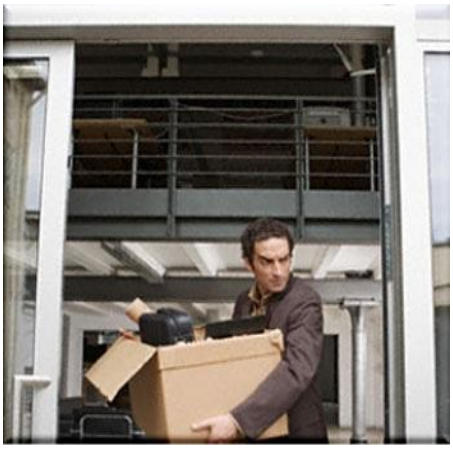
In the cases above, charges were pressed against the bookkeeper who took $80,000 in receivables. She served jail time. The bookkeeper who sold computers on EBay was charged, and settled with a plea bargain and a restitution schedule. The receptionist with the fraudulent credit card had moved out of state, and got off Scott-free.

The receptionist who changed the recipient on the checks and then changed it back?

She was an experienced thief. The owner made the mistake of confronting her alone to avoid embarrassment. She immediately threatened to call the EEOC and file charges, claiming that he had fondled her and demanded sexual favors instead of repayment.

They settled on her immediate voluntary termination.

CONSPIRACY



Each of the cases above involved a single point of theft. Even the stolen computers were dependent on one person; her cohort was merely engaged in blackmail. But sometimes you have a conspiracy to steal, and that can be much more difficult to discover.

I owned an auto parts warehouse. We delivered to scores of repair shops around the city daily via a fleet of delivery vans. Salesmen called on the shop owners, distributing special offers and premiums. Parts were pulled according to written order, checked by a supervisor, and checked again by the driver, who was responsible for shortages once the truck left on its route. I thought the checks and balances worked.

I was wrong. The salesman would make a deal with a shop owner. The salesman would communicate an "order" directly to the route driver for small but expensive items, on the pretext of telling him about scheduling challenges or even road construction. As the truck filled with parts the next day, the driver would simply put a few more items on after the final check, while the supervisor was engaged elsewhere in the warehouse. The shop owner would pay the salesman a deeply discounted price in cash, and the salesman gave a relatively small commission to the driver.

While the salesman wasn't, strictly speaking, needed as an intermediary, his role was important. He screened the shops for likely partners in crime. He knew which shops were serviced by specific routes and drivers, and could give the owner warning when he had to "really" order needed parts because the driver was on a different route that day.

The salesman's communication role avoided having a driver approach owners directly, which was far more dangerous. The products involved were always items to be used immediately. Once installed, it was impossible to prove that they were from our warehouse. The driver avoided the risk of being seen by a customer or employee receiving money directly. The salesman never touched the stolen merchandise.

Eventually the salesman made a mistake and approached an honest owner, who tipped us off to what was happening. A quick check of the suspect truck just before departure proved our case, but it was impossible to present evidence against the salesman.

Because the parts were obviously not labeled for a delivery, we couldn't identify exactly who the complicit customers were.

We had talked to the police about setting up a sting, but we couldn't tell them which customers to watch. They were understandably unwilling to follow a driver and the salesman around for days. We couldn't even be sure if only one driver was involved.

Like most fraud conspiracies, this one involved an inside employee, an outside employee, and willing recipients. Of course we fired the salesman and the driver, and changed our check procedure to include an overall "last look" at each truck before it was closed for departure. We saw the order frequency of a few customers drop dramatically as soon as we acted, but we could only suspect their involvement. A physical inventory count showed almost $100,000 missing in the previous few months.

The salesman had been out of work for a long time before we hired him, and thanked me almost weekly for giving him a job. In meetings, he was the most vocal about what a great company we were. The driver was one of our most efficient, and drew regular compliments from many customers for his courtesy and accuracy. We trusted them.

DEFENDING AGAINST FRAUD

What can you do to protect your business?

Of course, the best way to avoid the pain of employee fraud is to have systems in place to prevent it. The first and easiest method for testing your systems is to think like a thief yourself.

Spend a few hours putting yourself in each job in your company. Stand in the work area and go through the motions of the job. If you were intent on stealing, how would you do it? What would you take? Where would you hide it?

For a more professional look at your security, consider hiring a Certified Fraud Examiner. They are specially trained to spot flaws in your systems.

Above all, don't make the mistake of ignoring invitations to theft because "My employees will think I don't trust them." Trust is an important part of any employment relationship, but it only takes one thief to risk everyone's job security.

What if you can't assign check and balances?

Many small businesses have difficulty separating responsibilities. There are simply not enough employees for a system of checks and balances. One bookkeeper handles payables, receivables and reconciles the check book. In these cases, the owner has to be the safety factor.

Have bank account statements sent to your home so that you get a first look at all of the activity. Do the same with credit card statements. Always sign checks personally. (On vacation? Two or three signed blank checks will usually cover any emergency. But remember to reconcile them as soon as you return.)
Who opens your mail? If you can, open it yourself. If not, have it opened, but placed on your desk for sorting and distribution.

Is watching the books enough?

Not all employee theft involves financial accounts. There is a lot of truth in the old saying, "If your business has a door, you can be sure something stolen is going out of it."

Inventory leaves in clothing and purses, in trash and in delivery or service vehicles. Office supplies, coffee and food are "fair game" because employees think of these items as theirs anyway. Postage is a common form of petty theft.

After all, "It's only a stamp." Employees punch in early or have a friend punch them out late.

We know of one clerk who was given payroll figures to transmit for direct deposit. One week she made an error entering in her own salary as $1,631.00 instead of $1,361.00. When the mistake went undiscovered, she made the same "error" on the next 14 payrolls!

If you have inventory, whether product, food or raw materials, you are particularly prone to theft. Much of this type of theft can be controlled by simple checks. Don't let employees park their cars near the back door. Lock down the trash at night so that employees can't return to fish out stolen goods after hours. Check the list of transfers against an original. Have a log for postage used. The simple threat of possible discovery will discourage most casual thieves.

No business can completely protect against fraud. The small percentage of practiced thieves and conspiracies involving vendors or customers are particularly difficult to stop.

You have to trust someone, but appropriate checks and systems will make the majority of folks who aren't natural thieves stay in line. As my father said, "Locks are only for honest men."

AUTHOR'S BIO

JOHN F. DINI

Business Ownership Expert

John F. Dini is widely recognized as one of the nation's leading experts on small business ownership. He is a consultant and coach to hundreds of business owners, CEOs and Presidents of companies. John is an outlier in coaching business owners, having achieved the rare feat of delivering over 10,000 hours of face-to-face, personal advice to entrepreneurs.

Mr. Dini is the author of *11 Things You Absolutely Need to Know About Selling Your Business*, now in its second edition. He is a serial entrepreneur currently operating his 9th company, and has conducted business in all 50 United States, Canada, South America, Europe and Asia.

John founded and operates the most successful peer group franchise in North America, overseeing 15 monthly meetings of business owners' groups under the auspices of The Alternative Board®. He holds a Bachelor of Science in Accounting from Rutgers University, a Master of Business Administration from Pepperdine University, is a Certified MBA, and holds six additional certifications in exit planning, business brokerage, behavioral analysis, medical practice management, facilitation and coaching.

Mr. Dini writes numerous articles on business topics for newspapers and magazines, in addition to his weekly column on business ownership on this website Awake at 2 o'clock in the morning? and his opinion blog at Awake at 3 o'clock. He speaks frequently to business groups and national associations, and is a 10-year member of Jim Blasingame's "Braintrust" appearing regularly on "The Small Business Advocate" nationally syndicated radio program as an expert in the issues of business ownership.

CONTACT INFORMATION

John F. Dini
President, MPN Incorporated
12015 Radium St., Suite 100
San Antonio, TX 78216
P: (210) 615-1800
F: (210) 615-1865
M:(210) 643-2015
jdini@mpninc.com

Company: www.mpninc.com
Author: www.johnfdini.com
Boards: www.TABSanAntonio.com
Exit Planning: www.exitmap.com
Weekly Column on Business Ownership: www.awakeat2oclock.com
Blog from an Owner's Point of View: www.awakeat3oclock.com