



## **WHITE PAPER**

# **EMPLOYEE FRAUD CASE STUDIES**

**Developed by  
John F. Dini, CMBA, BCB, CBI  
President, MPN Incorporated**



## **White Paper: Employee Fraud Case Studies by John F. Dini**

**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 which he knows came 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 San Antonio 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 starting 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.

### ***Most small businesses are struck by employee fraud at least once***

These are true stories. Every one of them actually happened to a San Antonio business owner that we have worked with. They are not unusual occurrences. The owners had good 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 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.

### **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. An employee discovered the procedure and requisitioned checks for a "typical" amount on days when no permits were actually needed. He wrote the agency's name in as payee using an erasable pen. He then changed the payee to himself, deposited the check and intercepted

the cancelled checks so that he 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.

### ***Why do employees steal?***

There are three factors in every employee theft: need, opportunity and rationalization. The need is very often driven by a personal problem. It sounds callous, but employees with new babies, going through a divorce, illness in the family or elderly parents may all be candidates who need extra scrutiny.

The opportunity is driven by the systems in your company. Approximately 10-15% of all employees will steal whenever they can. Another 10-15% would never steal under any circumstances. The vast majority, 70-80%, will only steal when they have a need **and** they are sure the theft won't be discovered.

The final component is rationalization. The employee who is "mostly" honest needs to justify the theft as something else. "I should have gotten a bigger bonus. I deserve the money." Or "I work harder than anyone else here, and they get paid just as much." Or "I take work home on the weekend, and never put in for the overtime." One of the most common rationalizations is "I'm only borrowing it." Many employees begin to steal to satisfy the pressures of a temporary need and they truly believe that they can and will replace the missing money before it is noticed.

### **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.

### ***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!

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.

### **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.

### ***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.

### **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 rose, she quit without notice and moved out of the state.

### ***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.

### **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. The 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 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 is simply too difficult, expensive and time consuming for a business owner to deal with.

### ***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.

*John F. Dini is a consultant and coach to business owners, and since 1998 has operated the most successful franchise of The Alternative Board® in the world. His business tips and thoughts can be found at [www.awakeat2oclock.blogspot.com](http://www.awakeat2oclock.blogspot.com). He can be reached at [jdini@mpninc.com](mailto:jdini@mpninc.com)*

MPN Incorporated 12015 Radium Street, Suite 100 San Antonio, TX 78216  
P: (210) 615-1800 F: (210) 615-1865 [www.mpninc.com](http://www.mpninc.com)