

Embezzlement:

The Open Cookie-Jar and 10 Steps to Keep The Cookie-Jar Closed[©]



BARRY STROCK CONSULTING ASSOCIATES, INC.

154 ROSEMONT STREET, ALBANY, NY 12206

518-459-4252

BY FRED BARTZ, BARRY STROCK, AND JACK D. HARRIS, PH.D.

Embezzlement:

10 Steps to Keep the Cookie-Jar Closed[©]

By Fred Bartz, Jack D. Harris, Ph.D., and Barry Strock¹

Newspapers report that schools, governments and organizations small and large are at considerable risk to *white collar* crimes. One of the most difficult crimes to discover is embezzlement. It is for that reason that it is so critical that it be prevented.

Embezzlement is the fraudulent appropriation of money or property that has been entrusted to a person, for his or her own use. In the broader sense this also includes absconding with services or receiving favors. Ironically, when the economy is prosperous the rates of embezzlement rise as controls are relaxed. In harder economic times people tend to be more vigilant. In either circumstance, if you have not yet done so now is the time to implement controls that will prevent serious embezzlement by reducing temptation. Even little things can add up to bigger losses, such as illegally taking gasoline for personal use from the municipal supplies, taking office supplies from work to support a home business, using the photocopying machine for personal purposes, and taking rolls of postage stamps or unauthorized use of the employer's postage machine for personal uses. If a person takes thirty individual \$15 transactions every day, in a year it will add up to over \$100,000. In ten years it would exceed \$1 million dollars, without interest and compounding! Whether the amount of embezzlement is large or small, it is critical to implement methodical controls that prevent embezzlement.

Embezzlers often follow the "cookie-jar phenomenon" to begin their embezzlement career. This phenomenon begins with temptations that are innocently exploited, like buying an extra box of donuts for the organization's office party and then taking the donuts home for the family; or ordering an extra box of copy paper and taking it home. Interestingly, data on embezzlement indicates that the peak age of embezzlers is from the late teens to early twenties, with a decline thereafter, so that by age 37 the rate of embezzlement is half the rate

¹ **Fred G. Bartz** is Chief Fiscal Specialist for BSCA, Inc. Prior to working for BSCA, he was the Finance Director and Tax Collector for the City of Schenectady. He also serves on several not-for-profit boards. His fiscal experience began in the Commercial Banking sector and includes certificates awarded by the American Institute of Banking.

Jack D. Harris, Ph.D. is National Director of BSCA, co-author of THE MUNICIPAL COMPUTER SYSTEMS HANDBOOK, and a Professor of Sociology at Hobart and William Smith Colleges in Geneva, NY. He teaches the course on social deviance and white collar crime. He is an Information Technology and Change Management Consultant and an expert on organizational systems.

Barry Strock, is President of BSCA, Inc., co-author of THE MUNICIPAL COMPUTER SYSTEMS HANDBOOK, and consults and conducts workshops and seminars worldwide about management and technology issues.

at peak age.² While embezzlers used to be overwhelmingly male, the gap has narrowed and is now at parity – it is as likely that the embezzler will be a woman as it will be a man.³ Often embezzlers start innocently, but a sickness in the family, or gambling debts, or the strain of college tuition may push the innocent act into more deliberate acts of deviancy. For example, embezzlement due to gambling increased two to three times as a result of the introduction of gambling in the Town of North Stonington, Connecticut.⁴

Unfortunately many embezzlers are not caught until after they retire from a job, leave a volunteer position, or die. It is then that the organization begins to notice the “extra” revenue that has been siphoned off by the embezzler.

As security and technology consultants we often look for business security violations, but of greater value than finding the embezzler is to prevent their efforts before they get started. Organizations that have implemented computer-based systems are as much, or more, at risk than those that maintain paper-based systems. And organizations that handle lots of cash are also at heightened risk. In both cases it is the lack of clear financial processes and procedures in which there are embedded proven controls that makes the organization vulnerable.

There are a dozen rules that will help to prevent embezzlement:

1. Good Double Entry Accounting

As obvious as it may sound, it is problematic that too many organizations have poorly documented accounting of both revenues and expense transactions. We have seen many audit reports that can show that an organization has a 99% record of accurate transactions. The difficulty is that if the organization receives in and pays out \$1 million dollars a year, the cash flow [coming and going] of money could be actually twice the revenue, or in this case it would be \$2 million dollars. One percent of \$2 million dollars is \$20,000 and this can add up, year after year, to a considerable sum.

2. Separation of Duties

There should be different people that perform different and auditable parts of transactions. On the accounts payable side there must be separation of duties involving the collection or disbursement of money, from ordering product, authorizing the purchase, and paying for the purchase. On the accounts receivable side, there must be separation of duties involving receiving and recording payments, transaction and end of day reconciliation, to making the bank deposit. For example, think of the steps entailed in making a purchase, cutting a check, and proofing transactions:

² Roy Lewis, *White Collar Crimes and Offenders: A 20-Year Longitudinal Cohort*. iUniverse:2002.

³ J. Hagen, A.R. Gillis, D. Brownfield, *Criminological Controversies: A Methodological Primer*. Westview Press: 1996.

⁴ *Casino Impact on the Town of North Stonington, CT*. North Stonington Board of Selectmen: 2001.

- Verify and enter a vendor
- Purchase order entry
- Inventory receiving
- Invoice entry
- Payment entry
- Check writing
- Bank reconciliation

An additional safeguard is to require at least two separate physical signatures on all checks.

3. Accountability Procedures Must Be In Place

Something as simple as an employee using their work computers for gambling, on-line shopping, pornography, and private chat room communications are forms of stealing from the employer. It is important that every employee read and sign that they agree to the organization's business policies, and security measures, such as site blockers and monitoring systems, be in place to prevent such activity.

4. Background Checks of People Handling Money

It is not just prudent but essential to run a background check of any person who will be handling money. Depending upon the size of the organization's cash flow, it may be of value to bond the money handlers through an outside insurance agency as well.

5. Controls Apply to Everyone, Even the Nice People

Nice People Can Steal Money. Sometimes it is shocking to learn that the nice little old lady who brings in homemade sweets every week is rolling truckloads of cookies out the back door in the form of stolen money, services, or products. It could be that nice young man who looks so responsible and honest who may be using the organization's credit cards to buy more than just the required office supplies. With pressures and stress at the workplace and at home it is no surprise that some of the most delightful people can be tempted to go astray. The rule must be: No exceptions. No one should be trusted, and therefore exempt, from procedures and controls more than any other.

6. Business Process Analysis

Outside auditors routinely provide standard accounting audits. Typically these audits are validating selected random transactions to ascertain if best accounting practices have been undertaken. Another form of audit is a business process audit that analyzes the flow of

information, business processes, and money flow in search of gaps that could signal possible improprieties. This type of analysis often finds small cracks in the accountability work flow that could permit a curious mind the ability to take a truck load of money.

Moreover, such an assessment is likely to result in adopting process improvements that may include such methods as positive pay, purchasing cards, document control, and periodic cross-checks.

- Positive Pay automates fraud detection by pre-sending the payroll run information to the bank. When employees make their payroll check deposit, or cash the check, the bank automatically matches the account number, check number and dollar amount and will withhold payment if there is any mismatch.
- Purchasing cards are used to provide an employee with the convenience of a credit card that is pre-loaded with the authorized transactions. This allows the card to be limited to specific payments, preventing abuse and eliminating considerable administrative work linked to reimbursement.
- Document control requires that all fiduciary instruments have pre-printed sequential numbers. Any document that could function as a form of monetary exchange should have pre-printed sequenced numbers that are tracked. This includes any receipts for payments, purchase orders, checks, or other paper or electronic document that could or should attest to the authorizing of payments or purchases.
- It is useful to cross-check standard activities that may be the vehicle for embezzlement. For example, random and periodic review of payroll and vendor checks may discover that some recipients are not actual employees or actual vendors.

7. Never Let An Employee Refuse A Vacation

Too often the most industrious employee or volunteer makes him or herself so busy and so central to the operation that he or she claims they cannot take time off. Common to many embezzlers is the fact that they resist taking vacations. In the rare case that they do they work hard to restrict access to their work, especially their financial records and the handling of monetary transactions.

As a fiduciary practice it is imperative that no one is “the only person” who handles money or monetary transactions. This makes cross-training and periodic rotation of duties an essential practice and the taking of vacations mandatory. The latter is a common practice of banks. If your organization thinks they cannot afford two people doing such

tasks, they may be saving pennies and losing thousands of dollars.

8. Using a Lockbox and Managing Petty Cash

Embezzlement can be chump change. Although there are the Enron-type sleuths, most embezzlers are smart enough to steal small sums of money on a periodic basis. If someone is taking thirty individual \$15 transactions every day, in a year that adds up to over \$100,000, and in ten years it will exceed \$1 million dollars, without interest and compounding.

9. Develop rapport and a reward system for reporting violations

Much of the prevention of embezzlement requires creating organizational processes and procedures. However, there are strong human factors that can also mitigate against embezzlement, one the carrot, the other the stick. The carrot is developing personal relationships with employees such that there is knowledge of what is happening in their lives, and how they do their work. The stick is a clear reward system that encourages employees to report unusual activity. The message must be that stewardship of the organization's resources is everyone's responsibility.

10. Make Any Violation A Public Denouncement

When one person is caught stealing money it becomes a black mark on all employees if that person is not publicly admonished for such a transgression. Too often embezzlers who are caught are quietly discharged. Companies are often embarrassed that they did not have the proper controls in place. Regardless, employees must understand that the organization will be vigilant and will prosecute violators to the full extent of the law.

Following these ten recommendations will go a long way to effectively protecting your organization from people who think the cookie-jar is open for taking free cookies.