Embezzlement: Are you at risk?©

By Fred Bartz, Barry Strock, and Jack D. Harris, Ph.D.*

It seems that there is an unusual rash of embezzlement scandals. Newspapers report that organizations, from small not-for-profits and small governments, to large governments, are at considerable risk. Even regional educational organizations are vulnerable as evidenced by one in which $3 million dollars was supposedly taken to illegally enrich an individual's pockets.

In a small city a employee was arrested for stealing $12,000. The more significant issue is that this former employee has now cast a cloud on all of the employees of the local government that everyone in City Hall is a crook. This is an unwarranted allegation.

How can managers, elected officials, and citizens help stop this dishonesty? Although technology could be the tool of modern embezzlers, there are many other questions that need to be asked and examined before focusing on the pure technology-related issues.

Without being cost-prohibitive, the large accounting firms cannot audit every transaction in every department of a government. This results in a limited sampling of accounting data, and the accounting audit does not often involve a careful and deliberate audit and analysis of process and cash controls. Thus, while many municipalities profess to follow GFOA and GAAP standards, too many of them have loose controls that make them subject to

---

* **Fred G. Bartz** is Chief Fiscal Specialist at BSCA. Prior to working for BSCA, he was the Finance Director and Tax Collector for the City of Schenectady. He still volunteers his time in an advisory capacity to the Mayor. 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.

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

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. He is a strategic information technology consultant and an expert in management organization.

embezzlement and fraud. Some examples that we have witnessed: Checkbooks that are not accounted for in the general ledger, revenue receivers reconciling their own drawers, treasurers collecting cash, making their own deposits, and making their own journal entries, and payroll clerks printing checks and electronically signing them without careful oversight.

Of course, in each of these cases, deliberate accounting principles need to be applied. But the clever embezzler will require vigilance through more indirect methods of discovery. In what follows, we provide a list of several conditions that should raise warning flags, and several procedures that will discourage even the most vicious and persistent embezzler:

1. NEVER LET ANYONE IN THE ORGANIZATION NOT TAKE VACATIONS. Be sure the person who takes the required vacations does NOT tell everyone to leave his or her work until he or she returns. [This is a giant red flag that not only this person is the one person able to do the task at hand, but that there could be more to their control than just doing tasks]. This is a clear opportunity to let the fox have the keys to the chicken coup without establishing checks and balances. No one in an organization should be indispensable, especially the person with 25 years of experience. It is the obligation of management to ensure that no one person is the only person controlling money or posting of transactions. For example, it is ridiculous to allow the building permit staff to both issue building permits and then collect the money. Similarly, a single person in Parks and Recreation staff should not be permitted to both register people for classes and to collect the money.

2. WHOEVER AUTHORIZES DISBURSEMENT [i.e., writing checks, authorizing electronic transfers, transferring money, etc.] OF ANY CHECKING ACCOUNT, SAVINGS ACCOUNT, MONEY MARKET, OR INVESTMENT ACCOUNTS CANNOT HAVE THE ABILITY TO RECONCILE THEIR CORRESPONDING STATEMENTS. In one case, a clerk was writing checks to herself every month for hundreds of months. But, when time came for her to reconcile the checkbooks, she would shred her canceled checks and show the books to be balanced. The culprits can be fiscal officers down to the lowest paid clerks -- no one is immune from the temptations of stealing.

3. ALWAYS HAVE A UNIVERSAL DOUBLE-ACCOUNTING OF ALL MONEYS COLLECTED. In one case there was a clerk in the water department who would collect money from contractors, who would dutifully mark the giant ledger that the contractor had paid his tap fees or other fees. Unfortunately, no one ever reconciled

the ledger with the money in the bank. This resulted in a one million dollar embezzlement over ten years.

4. LOOK FOR REVENUE PATTERNS. Someone should be checking for consistent patterns. For example, if on the average parking tickets yield a $20,000 a month in revenue, and normally has a $30,000 average April revenue -- someone should be looking over all of the year's parking revenues to identify these patterns. Then if in January the average falls well below the January averages, management needs to look for answers such as, we had five, two foot snowfalls in January.

5. NOTHING IS TOO SMALL TO OVERLOOK. Unfortunately, governments are usually large revenue driven operations. What if an accountant were to tell the City Manager that the books were balanced to within 99.5% accuracy. One could think that may be good. But, if the accountant were auditing a $150 million dollar budget, then a .05% margin of error would yield a $75,000 opportunity for embezzlement for one year and $750,000 over ten years, and $1.5 million over twenty years. One and a half million dollar retirement fund is not bad for a twenty year employee who may believe that she/he is been underpaid and overworked for twenty years. It is shocking to learn that many of these scoundrels are so arrogant that they take their millions and put them in auditable checking accounts, savings accounts and stocks. We know of one city wherein the CPA from the accounting firm believed that .05% was not *"materially significant"* when dealing with a $150 million dollar budget.

6. MAKE A MODEL PUBLIC DENOUNCEMENT OF EVERY INFRACTION. We had a client who had a fiscal officer who was also the data processing manager, the purchasing and accounts payable guru, the payroll and the auditing manager. It was not surprising that this person was buying "X" million dollars a year in computers, but only had on hand, about 1/2 "X". When the disclosures were made to the Mayor and City Council chairperson, they responded that they would change this person's titles and make sure this possible embezzlement ceased. Since they did not prosecute the individual, they had immediately sent the grapevine message that they would condone irregular behavior. There must be a clear-cut separation of duties.

7. DON'T LET ANYONE BE THE ONLY PERSON TO KNOW SOMETHING. Sometimes there is only one person who knows how to do something. Look out for an employee or manager who insists that their duties or functions cannot be performed by or shared with others; hence, when they are out, or not present, their functions

stop and resume only when they return. Look out when only one person knows how to prepare financial reports. Look out for long tenured employees who are overly protective or secretive of their work [i.e., with such statements as *"this is my area, and you cannot be here", "these reports are too complex for you to understand"*, etc.] Look out for a person who frequently assumes financial duties in areas outside of their own work. No public entrusted entity should make themselves so vulnerable to let only one person be the only person who knows something. Unfortunately, in organizations [public or private or small or large] there are too many lazy people. I had worked in an organization where there were dozens of small tasks which required deliberate attention to detail. Since I was responsible for the final reporting of the information, for the sake of expedience, I slowly asked people if they would let me do their job. Over time I did the majority of all of the fiduciary and statistical task related to the management of a $100,000 million dollar operation. Fortunately, I had no larcenous tendencies, but, now as a consultant and I am on the other side of the process I realize that my innocent taking over of other people's work made me into a prime position to do mischief.

8. ASSUME ANYONE IS OPEN TO DISHONESTY. With the every increasing pressures and stress at the workplace, at home with loved-ones who have very expensive medical requirements, personal drug and substance abuse, and parents frustrated with too little money for their children -- it is no surprise that some of the most outstanding people can be tempted and go astray. It may be that a twenty five year employee who was the most honest and diligent employee for twenty years. However, the last five years could have been a short period in their life where stress forced them to be a wee-bit dishonest.

9. STRANGE PURCHASES One of the easiest give-aways is the $30,000 a year clerk who drives a corvette and who has a million dollar home. Some people believe that it is not the business of the employer to know how a person pays for expensive new toys. However, as a public servant, conspicuous purchases should raise the concern of any responsible official.

10. HOLD MANAGEMENT RESPONSIBLE If a fiscal officer delegates tasks to a lower level employee, he/she should be equally held responsible for illegal acts perpetrated by the lower level employee. Delegation of tasks should not imply or result in delegation of <u>all</u> responsibiliy and accountability.

11. STATUS QUO In one city they had a quarterly sale of surplus items and lost and found items. The person in charge of the operation was loading five bicycles into his car. When asked what he was doing, his reply was that it was the custom that anyone who works on the quarterly sale was entitled to take his/her choice of the best items. So the person received overtime for working on Saturday, plus free bikes. If this behavior is condoned, then where is the line of ethics?

12. ACCOUNTABILITY PROCEDURES MUST BE IN PLACE. Accountability procedures are a good first step in discouraging mischief. For example, when parking tickets books are given to an officer, he/she must be accountable for every ticket in his/her book, and there must be an independent procedure to keep track of the tickets issued, voided, or in the collections process. In one police department we found thousands of dollars in cash and personal checks stapled to parking tickets. Years worth of stapled moneys. One does not need to be a rocket scientist to figure out what was happening. But, it was confusing to see a crooked operation not covering their tracks.

13. INDEPENDENT CONFIRMATION OF REVENUE AND EXPENDITURES There must be an independent confirmation of revenues and expenditures. In one case the fiscal officer had been choosing the auditor each year, and since the fiscal officer was absconding with funds, it was curious how all of the other responsible auditors could never get to win the audit contract. Sometimes, it may be of value to consider an auditor of the auditor. It is always of value to look at the bank statements to verify that the money listed in the reports balances with the money the bank seems to have in their accounts.

14. REASONABLE EXPLANATIONS OF FAILURE TO MEET BUDGETED FINANCIAL OBJECTIVES [i.e. revenues or expenditures] It should be a red flag if an individual refuses to give a reasonable -- and written -- explanation as to why revenue is either reduced or expenditures are increased. There should be routine analysis of revenue and expenditure projections with corresponding longitudinal statistical analysis of the past five years. It is especially valuable to have comparative line or column charts. Graphics permit quick and visual identification of significant aberrations. Look out if someone has hostile responses for requested information. It may be the person is just overworked or annoyed. However, it may be that the person is covering up something. We had one fiscal officer who refused to provide five years of historical data processing purchases. He tried every trick for procrastination that was

possible. He even alleged that the consultant and the CPA were not sufficiently intelligent to understand his sophisticated finacials. Fortunately, through surreptitious means, the records were uncovered, and the reasons for his obfuscate were plan to understand. He was a crook!

15. MAINTAIN RECORDS If records management activities are being undertaken, it is important not to destroy possible evidence for a possible trial of money mismanagement.

16. INSIST ON TIMELY WRITTEN FINANCIAL REPORTS. It is imperative that management require timely and written financial reports, prepared by internal staff and/or external auditors. When individuals in an organization insist on verbal reports, a red flag should be raised. The timely factor is an interesting one. One city had a clerk that routinely had provided for detailed financial reports on the third day of the month, each month. Then, it was submitted on the ninth day of the month, and then on the twentieth of the month. Over time the reports were not being submitted monthly, but only nine months a year. The missing three months went into the clerk's private accounts. There needs to be written reports, but also, there must be monthly statements which reconcile with the reports. If the money is not in the bank, then there is good reason to believe that it is missing.

17. MAKE SURE THAT REVENUES ARE CAPTURED TO A CENTRAL JOURNAL All revenue entry, whether it be tax bill collection, receipting of licenses and fees, collection of utility payments and the like should be entered systematically into point of sale capture stations. Petty cash should also be subject to cash controls that require daily reconciliation. Such stations have the virtue of tracking every transaction, identifying the cashier and balancing the cash drawer, and check validation and receipting. This makes reconciliation of cash receipts an efficient process while protecting government from theft. The use of lock box receipting also prevents easy embezzlement by using receipting controls by agents such as banks, and controlling journal entry via ACH processing. In one of our client municipalities, the use of a video camera pointed at the cash stations significantly discouraged attempts to embezzle money during transactions.

18. VIRTUALLY ALL EXPENSE PAYMENTS SHOULD BE PROCESSED THROUGH COMPUTER CHECKS OR PROCESSED ELECTRONICALLY Multiple checking accounts that are not accounted for regularly in the general ledger are a potential source of

significant embezzlement. Modern computer-based accounting systems allow convenient printing of even single checks to a laser printer. With the exception of specific funds that require a separate cash account (such as an electric utility enterprise fund), as much as possible should be passed through a central cash account using due to/due from functionality. Fund transfers can easily be accomplished through ACH processing and electronic transfer so that expense checking accounts such as payroll and accounts payable can be kept at zero balances until expenditures are approved and ready for payment.

19. CONTROL YOUR PASSWORDS Technology provides for electronic signature without the use of a signature cartridge. The use of a PIN number to authorize check signing is a very weak link if someone discovers the signatories PIN number. This also impacts electronic approval of requisitions and purchase orders. A stolen PIN number can result in collusion between vendors and the corrupt employee. Thus, there should be vigilance by department heads, comptrollers, and managers that checks, purchase orders, and refunds are being released to properly authorized parties.

20. WATCH YOUR CHECK STOCK Laser printers can transform plain paper stock into handsome purchase orders, invoices, and checks. Check stock can be an attractive tool for the embezzler. To discourage this behavior, build your controls into the check stock. One of our clients chose multiple security features to make its checks theft and tamper proof. They chose to use control paper that is not sold in the open market, an artificial watermark, faint diagonal lines on the back of the check to prevent cut and past, a "void" pantograph that revealed itself in a photocopy, chemically protected paper to prevent lifting the signature or amount, and an inventory number pre-printed on each check to discourage theft.

21. BE POSITIVE THAT YOUR CHECKS ARE BEING CASHED FOR THE AMOUNTS THAT YOU INTENDED Positive payroll and positive payables prevents changes to check amounts that lead to fraud by notifying banks in advance of payroll or accounts payable cashing of the amounts that have been authorized for payment. Having check stock that is tamper-proof also discourages fraud, but a less vigilant bank employee may miss the telltale signs of tampering.

22. NICE GUYS MAY BE THE BAD GUYS Ironically, the nasty people mat be the good guys. Do not assume that nice people are good guys and nasty people are bad guys.

Dishonest people may actually be so sweet and passive that no one would every think of them as criminals. If you were acting as a thief, would it be wise to be the old curmudgeon who is crusty and complaining or the nice helpful person?

23. BLAME TECHNOLOGY. One of the clear advantages of technology is that most people, especially the mischievous often project their dishonest character onto the possibilities of technology. Technology often is a weapon that permits un-earthing of mischievous deeds. However, technologists are the modern sleuths. Technologists too often become the technology gurus who "know-it-all." They say, "I will take care of it," "don't worry I will make sure the computer knows," or they become the sole knowledge base of how information is captured and retrieved. Thus, at the time of bringing in technology innovations, be sure that non-technologists are managing the process and the security access codes. Also, be sure that fiscal detail-oriented bean counters are very involved in the set-up and the transfer to the new technology. Very often we have found that utility conversions unearth the fact that customers have been erroneously charged for decades. The errors could be as major as wrong rates, to as minor as to rounding of pennies each month. The people who are the trusted bean counters are too often discarded in the conversion process. This discarding could be a fatal blow. Many of these bean counters may be so fastidious that they are a pain. However, management, not the technologist, should determine whether the bean counter is trying to protect his/her old tedious task-based job, or whether this person has the legitimate concerns of his/her employer. Maintaining the integrity of the system is most critical to the survival of an organization.

When one realizes that all of the viable audit trials are linked to the little computer black box, it become clear that it is imperative someone in management is entrusted with:

- routine daily back-ups off site
- routine independent auditing of the system by outside auditors
- highest level security access to be shared with the CIO, CFO, and the CEO.
- defined steps to change security codes when a person leave the employ
- secure access of back-up data, source, and systems documentation

Never allow only the technology department or the finance department the right of computer access to records. With a reasonable audit trail, upper management or their designated representative must have access to all financial records. Computers can encourage larcenous temptations. When we find that only the IS director can

> "really" secure all of the required information -- this is a giant red flag. The electronic database must be more secure than the paper databases and it must be [within the reasonable security clearances] fully accessible by key management professionals. Management cannot be at the mercy of the CIO, CFO, or any other individual who is the only person who both understands the system or who is the only one who knows how to get valid information.

Good management protects the fiscal health of a local government, and protects the integrity of its employees. The computer can be a vehicle for effective security controls, or it can be the gateway to embezzler paradise. Computer software has yet to embed the intelligence wrought from a careful understanding of the weak management and human desire that can result in compromised work flow, sloppy cash handling, concealed transactions, and opaque rather than transparent financial reporting. A vigilant management that uses the computer as a tool to reinforce fiscal security will lead to citizen confidence in the accountability and integrity of local government.