FRAUD SCHEMES

By James F. Finlay

Frauds can be categorized by the type of victim involved. The most common groups of victims encountered by Fraud Examiners include:

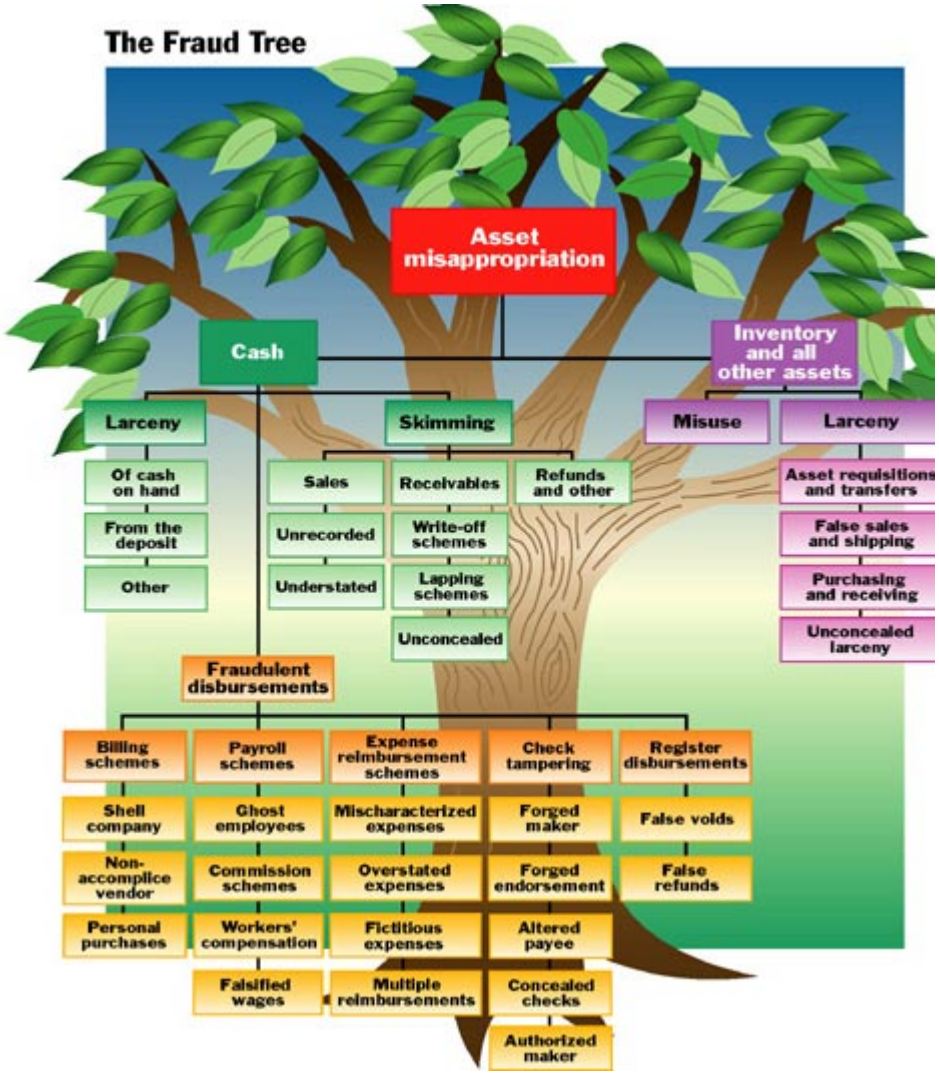
- Funders & Donors
- Creditors
- Businesses
- Banks or other financial institutions
- Central or local government
- Fraud by manipulating financial markets

Frauds can also be categorized by the technique or activity used by the fraudster. These include but not limited to:

- Advance fee frauds
- Bogus invoices
- Contract Procurement
- Computer hacking of information or property
- Conflict of Interest
- Corruption and bribery
- Counterfeiting, forgery
- Credit Card fraud
- False Accounting - manipulation of accounts, shares, accounting records
- Fraudulent bankruptcy - exploitation of cross-border corporate structures
- Financial Statement Fraud
- Fraud Risk Analysis
- Insurance fraud
- Internet online scams - auctions, credit card purchases, investment scams
- Investment fraud
- Misappropriation of assets
- Money laundering
- Payroll fraud - ghost employees
- Principal agents - failure of systems to restrict key individuals
- Pyramid schemes

THE FRAUD TREE – ASSET MISAPPROPRIATION

Over the years, the asset misappropriation chart has become known as the "fraud tree" for its numerous branches. The tree's trunk consists of two major asset types: cash, and inventory and all other assets. Crooked employees clearly favor misappropriating the former—nearly nine in 10 illegal schemes involve the cash account.
The reasons should not be surprising: Cash is fungible, has a specific value and is easily transported. Inventory—except for consumer goods—has limited usefulness to a thief; an employee in a ball bearing plant can have a hard time converting the loot into cash. And of course, many business enterprises don't have a physical inventory at all.



Source: "Report to the Nation," 1996. Institute of Certified Fraud Examiners. See the full report at www.cfenet.com.

THE BRANCHES

On the branches of the fraud tree are three main ways to embezzle cash: skimming, larceny and fraudulent disbursements. Skimming can be described as the removal of cash prior to its entry into the accounting system. It does not matter the size of the organization, non profit or charity the fraud schemes will fit if the employees are allowed to get away with it. **Here are some examples:**

• In a legendary story, the manager of a retail store with six cash registers brought in his own register and set it up in an empty checkout lane. All sales going through the seventh register went directly to the manager! Although you would think someone would notice, this scheme reputedly went undetected until a physical count showed huge inventory shortages. (this could also have been a charity selling clothing)
• A government mail-room employee skimmed more than $2 million in taxpayer refund checks that had been returned by the post office for bad addresses. The employee, with the help of several outside accomplices, was able to deposit the stolen checks into various banks and withdraw the proceeds. The scheme was uncovered when a taxpayer called about an overdue refund and found out that his check had already been cashed.
Larceny is the removal of cash from the organization after it has been entered into the accounting records. Most of these schemes are detected through bank reconciliation's and cash counts. Larceny is therefore not one of employees' favorite illicit methods; it accounted for only 3% of the cases in a study and 1% of the losses. Here are some examples of cash larceny:
• A bookkeeping employee, responsible for posting donors receivable in a small nonprofit, stole some of the cash receipts but nonetheless posted the transaction to the company's donors-receivable detail. Within months, the theft had risen to more than $200,000, seriously depleting the business's cash. A bank reconciliation revealed a major discrepancy between the donors-receivable detail and cash, the scheme was uncovered.
• An employee in charge of taking the company's money to the bank would regularly remove currency, then alter the company's deposit slip to reflect the lower deposit amount. The worker, obviously not an accounting genius, didn't realize the discrepancy would be discovered when sales and cash were reconciled.

Additional research of 732 fraudulent disbursement cases showed they can be subdivided into at least six specific types: check tampering, false register disbursements, billing schemes, payroll schemes, expense reimbursement schemes and other fraudulent disbursements. Following are a few common examples:
• A purchasing agent for a major corporation set up a vendor file in his wife's maiden name, then went on to approve more than $1 million in company payments to her. The supporting documentation consisted of the wife's invoices for "consulting services" that were never rendered. A clerk in the purchasing department, suspicious of the agent's recent purchase of a new boat and car, caught on to the scheme and turned him in.

• The ED of a small nonprofit agency stole $35,000 from its coffers by submitting "check requests" to the accounting department. The checks were made payable to outside bank

accounts the CEO controlled. The accounting personnel, fearful of angering the boss, made out the checks and delivered them to him. One accounting clerk finally had enough and alerted the outside auditors, who confirmed the disbursements were not legitimate.
• A worker for one charity submitted an expense reimbursement for a trip he supposedly took for business purposes. Actually, he took his girlfriend to a bicycle rally and attempted to charge the expense to the charity. One problem: On his itinerary, the worker listed the independent auditor who was examining his expense reimbursement as his traveling companion—not a smart move.
• Employees who set up dummy companies for fraudulent disbursements often give clues to their activities. They will use their own initials for the company name, rent a post office box or mail drop to receive checks, or use a dummy company name and their own home address. Therefore it is important that you have an approved vendor file.

New Study: Insiders Who Steal from Charities go to jail

Nearly 70 per cent of insiders who defraud nonprofits face jail time, according to new research released today by the CA-Queen's Centre for Governance. The study is the first in Canada to document the scope, severity and profiles of Canadian nonprofit frauds, using data gathered from reports in Canadian daily newspapers between 1998 and 2008.
"Our goal was to simply profile the types of insider frauds in Canadian nonprofit organizations, but after analyzing the data, we were surprised to learn how many of these thieves get caught and convicted," said Professor Steve Salterio, Director of the CA-Queen's Centre for Governance and co-author of the study with doctoral student Qiu Chen. "In fact, we found only one acquittal in 53 cases, and a high likelihood of jail time."

Highlights of the Queen's study

Profile of the nonprofit fraud:
- The average fraud cost to a nonprofit is $119,821 per occurrence.
- Smaller nonprofits (those under $100,000 in revenue) lost on average an entire year's revenue when fraud occurred whereas slightly larger organizations (less than $1 million in revenue) lost nearly 50% of their revenue when fraud occurred.
- Fraud was more likely to occur in large urban centres than in smaller centres. Almost 82% of the reported frauds were committed in census metropolitan areas of 200,000 or more. Nonetheless, both the largest and smallest centres reported similar dollar averages in amount of reported fraud losses.

Profile of the "Fraudster":
- More that 90 per cent of reported frauds of nonprofits are committed by one person.

- The most frequently reported fraudsters held senior management positions (Chief Executive Officer or Executive Director, 30%; Chief Financial Officer or Treasurer, 28%; and fundraisers, 28%).
- CEO-committed frauds cost nonprofits the most, at $176,000, while fundraiser fraud averaged $60,000.
- Men and women are equally likely to commit fraud.
- Very few fraudsters have criminal records.
- Age is highly correlated with fraud. Board members, management and employees who are older or longer serving are more likely to commit fraud.
- However, when younger employees do commit fraud it is for large amounts (average of $868,667).

The study documents jail sentences ranging from three to 90 months, with an average of 32 months behind bars where jail time was sentenced. The study found no difference in prosecution rates and convictions between individuals occupying senior levels in their organizations (i.e. board members, treasurers, presidents, and chief financial officers) and other levels (e.g., fundraisers, non-management employees). Other common sentences included probation and house arrest, sometimes in conjunction with jail time.

"This finding refutes the popular notion that white-collar crime, particularly involving charities, is punished by little more than a slap on the wrist," said Chen. The study acknowledges that the number of un-reported and non-prosecuted cases is unknown.

"As the world heads into an economic downturn, nonprofit managers and boards will come under increasing stress to deliver services," said Professor Salterio. "In the rush to meet mounting pressures, there is a risk that the principles of good management including strong internal controls may be neglected, but the result can often to catastrophic both for the organization with its lost funds and for the individual facing cold hard jail time."

The above study was conducted by:

Qiu Chen MSc. - Doctoral candidate

Steven Salterio Ph.D. FCA
PricewaterhouseCoopers

Tom O'Neil Faculty Fellow in Accounting
Professor of Business
NOTE: The full study is available at -
http://business.queensu.ca/centres/CA-QCG/documents/reports/Canadian_NPO_Frauds_Report.pdf

In the next article, we will start look at the detail of fraud schemes from the fraud tree that could affect your organization.

For further information, go to www.finlay-associates.com and download Detecting Occupational Fraud in Canada.

James Finlay is a Certified Fraud Examiner; he can be contacted on 905 870-1832 or at info@finlay-associates.com or via www.finlay-associates.com.