About The Author

Barry Jay Epstein, Ph.D., CPA, CFF has practiced as a technical and litigation consultant, expert witness, writer and lecturer on US GAAP, IFRS, and auditing standards for over forty years. He is a principal in the Chicago and Detroit (USA) based firm, Cendrowski Corporate Advisors LLC, and holds degrees from DePaul University (B.S.C., 1967), University of Chicago (M.B.A., 1969), and University of Pittsburgh (Ph.D., 1979), as well as the CPA and CFF (certified in financial forensics) designations.

He was a founding and the lead author of the widely-used Wiley GAAP and Wiley IFRS through 2010, and author of Thomson Reuters’ Handbook of Accounting and Auditing, through 2013, and has authored scores of professional articles for major publications.

As a speaker, Dr. Epstein has appeared on over one hundred programs over his career, including previous lectures delivered in Singapore and Indonesia, as well as in the Middle East, Canada and the U.S. As an accounting expert, he has testified or assisted in 150 litigation matters, including white-collar (fraud) criminal matters and contractual disputes, and has assisted the US Securities and Exchange Commission and Commodity Futures Trading Commission some twenty times. He advised the US Department of Justice on both the Enron and WorldCom fraud cases, and is currently engaged on several major cases, including the Parmalat matter, which may be the largest accounting fraud to date, amounting to US$18 billion.

Barry Jay Epstein, Ph.D., CPA, CFF
Cendrowski Corporate Advisors LLC
Chicago, Illinois USA
bje@cendsel.com
About the Institute of Singapore Chartered Accountants

The Institute of Singapore Chartered Accountants (ISCA) is the national accountancy body of Singapore. ISCA’s vision is to be a globally recognised professional accountancy body, bringing value to our members, the profession and wider community.

Established in 1963, ISCA shapes the regional accountancy landscape through advocating the interests of the profession. Possessing a Global Mindset, with Asian Insights, ISCA leverages its regional expertise, knowledge, and networks with diverse stakeholders to contribute towards Singapore’s transformation into a global accountancy hub. Our stakeholders include government and industry bodies, employers, educators, and the public.

ISCA is the Administrator of the Singapore Qualification Programme (Singapore QP) and the Designated Entity to confer the Chartered Accountant of Singapore - CA (Singapore) - designation.

It aims to raise the international profile of the Singapore QP, a post-university professional accountancy qualification programme and promote it as the educational pathway of choice for professional accountants seeking to achieve the CA (Singapore) designation, a prestigious title that is expected to attain global recognition and portability.

There are about 28,000 ISCA members making their stride in businesses across industries in Singapore and around the world.

For more information, please visit www.isca.org.sg.
## CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Big A Problem Is Business Fraud?</td>
<td>4</td>
</tr>
<tr>
<td>Assessing An Organisation's Fraud Exposure</td>
<td>7</td>
</tr>
<tr>
<td>Cash Fraud Schemes</td>
<td>15</td>
</tr>
<tr>
<td>Accounts Receivable Fraud Schemes</td>
<td>19</td>
</tr>
<tr>
<td>Inventory Fraud Schemes</td>
<td>24</td>
</tr>
<tr>
<td>Fixed Asset Fraud Schemes</td>
<td>28</td>
</tr>
<tr>
<td>Payables And Disbursements Fraud Schemes</td>
<td>30</td>
</tr>
<tr>
<td>Equity Fraud Schemes</td>
<td>37</td>
</tr>
<tr>
<td>Miscellaneous Fraud Schemes</td>
<td>38</td>
</tr>
<tr>
<td>Some Of The Big Ones: Infamous Accounting Frauds</td>
<td>39</td>
</tr>
</tbody>
</table>
BUSINESS AND ACCOUNTING FRAUD

I. HOW BIG A PROBLEM IS BUSINESS FRAUD?

A. Introduction

1. It is generally acknowledged that fraud is a serious problem for businesses of all sizes, costing billions of dollars each year.
   a. Studies suggest that businesses may lose as much as 6% of revenue every year to fraud – which would equate to S$885 billion of the nation’s 2010 gross national product of S$14.5 trillion, if that estimate is correct.
   b. Fraud is also a major problem for accountants and auditors (both internal and external) because they are perceived (rightly or wrongly) to be the most directly responsible for establishing internal controls and for preventing or detecting fraud.

2. Fraud is the strongest leading indicator of a business’ demise.

3. When businesses fail, blame is often placed on the accountants and auditors, who are highly likely to find themselves embroiled in costly litigation, adding further to the social cost of fraud.

4. Concern over fraud in business has grown in the wake of recent, well-publicized accounting scandals.
   a. This has prompted the auditing profession and regulators to further define responsibilities relating to fraud prevention, deterrence, and detection, including that of the independent auditor.
   b. This is evidenced by the recent promulgation of various laws and auditing standards that emphasize the importance of controls relating to fraud prevention and detection along with the responsibilities for both management and their auditors.

B. What Is Fraud?

1. *Black’s Law Dictionary* defines fraud as:

   A generic term, embracing all multifarious [various] means which human ingenuity can devise, and which are resorted to by one individual to get advantage over another by false suggestions or by suppression of truth, and includes all surprise, trick, cunning, dissembling, and any unfair way by which another is cheated.

2. In the U.S., Statement on Auditing Standards (SAS) No. 99 (AU §316.05) defines fraud as “an intentional act that results in a material misstatement in financial statements that are the subject of an audit.”
   a. The primary characteristic that distinguishes fraud from errors in financial statements is intent.
   b. However, various statutes, cases, and organisations define fraud differently. Therefore, when investigating fraud, it is important to consider the applicable definition.

3. Under International Standards on Auditing, ISA 240, *The Auditor’s Responsibilities Relating to Fraud in an Audit of Financial Statements*, “[t]he distinguishing factor between fraud and error is whether the underlying action that results in the misstatement of the financial statements is intentional or unintentional.” This is consistent with U.S. GAAS and other national standards.

C. Categories of Fraud

1. The following are the three major categories of fraud:
   a. Financial reporting fraud (also known as management fraud);
   b. Misappropriation of assets (also known as employee fraud); and
c. External fraud.

2. Financial reporting frauds are:
   a. Intentional misstatements of amounts or disclosures in financial statements.
   b. The primary purpose is to misstate the financial statements to mislead those relying on the statements when some outcome – such as a bonus or financing – depends on the financial results reported.

3. Misappropriation of assets (also known as defalcations, embezzlement, stealing, or employee fraud) is theft of an organisation's assets by employees.
   a. Perpetrators often manipulate the financial records to accomplish or conceal misappropriations. For example, when cash is diverted, an expense may be misstated to conceal the offsetting debit.
   b. However, misstatement of the financial statements is secondary to the main purpose of stealing assets.
   c. There are many types of misappropriations of assets, but the most common are the following:
      i) Stealing cash by diverting cash receipts, manipulating accounts receivable postings (lapping), altering bank deposits, stealing or forging cheques, stealing petty cash, etc.
      ii) Creating fictitious vendors or overstated vendor invoices.
      iii) Stealing inventory or equipment by diverting goods received or sold, or by making unauthorised scrap sales.
      iv) Taking kickbacks.
      v) Abusing travel and entertainment reimbursements to include personal items.
      vi) Creating ghost employees or overstating hours worked.

4. External frauds generally are committed against an organisation by non-employees.
   a. For example, a perpetrator alters a cheque and cashes it at a financial institution or when a contractor delivers substandard building materials to a construction site.
   b. However, in some cases, an external perpetrator will collude with an employee (for example, in a bid-rigging scheme).
   c. The purpose of external fraud is the financial gain of the perpetrators.
   d. Generally, perpetrators will not have access to the organisation's financial statements so they will not be misstated in these cases.

D. Findings from COSO and other fraud studies

1. In May 2010, the Committee of Sponsoring Organisations of the Treadway Commission ("COSO") released a research study entitled, Fraudulent Financial Reporting: 1998-2007 (the "COSO fraud study").
   a. The COSO fraud study, which is based on an in-depth analysis of 347 accounting fraud cases investigated by the SEC over a 10-year period, discusses the nature, extent, and characteristics of these accounting frauds.

2. In October 2010, the U.S. AICPA's Centre for Audit Quality ("CAQ") issued its report Deterring and Detecting Financial Reporting Fraud—A Platform for Action (the "CAQ Fraud Report").
   a. The CAQ Fraud Report is based on a series of roundtable discussions held in the United States and London to capture participants’ perspectives on successful fraud deterrence and detection approaches, as well as other ideas on the topic.
b. The report sets forth ideas for mitigating fraud and related points to consider. Participants included corporate executives, boards of directors, audit committees members, internal auditors, external auditors, investors, regulators, academicians, and others.

c. The CAQ Fraud Report is based on the views expressed by participants in those discussions and presents, among other things, ideas for mitigating the risk of financial reporting fraud; it is thus an important first step in advancing longer-term initiatives and collaborations for the deterrence and detection of financial reporting fraud. The following paragraphs summarize the findings included in the CAQ Fraud Report.

3. The CAQ Fraud Report, which defines financial reporting fraud as “a material misrepresentation resulting from an intentional failure to report financial information in accordance with generally accepted accounting principles,” begins (as do most such dissertations) with a discussion of the fraud triangle.

a. The report then describes the roles of those involved in a company’s financial reporting process, including boards of directors, audit committees, internal auditors, and external auditors.

b. The bulk of the report is comprised of a discussion of how those involved in the financial reporting process can individually and collaboratively mitigate the risk of financial reporting fraud.

c. The CAQ Fraud Report states that participant discussions consistently centred around three themes, discussed in detail below:
   i) The need and importance of a strong and ethical “tone at the top;”
   ii) Scepticism among all involved in the financial reporting process; and
   iii) Strong communication among all involved in the financial reporting process.

4. Tone at the top. The CAQ Fraud Report reinforces the position that a strong, ethical culture creates an expectation to “do the right thing” and counteracts pressure and incentives to commit fraud within an organisation. It also supports well-designed, effective controls that reduce opportunities to commit fraud and increase the likelihood that fraud will be detected quickly.

a. To that end, management plays the most critical role in building a strong ethical tone at the top and reinforces it through the establishment of a comprehensive fraud risk management programme with a readily accessible and confidential whistleblower programme.

b. Boards of directors and audit committees support and further reinforce the tone at the top by choosing the right management team; audit committees oversee the financial reporting process, including monitoring fraud risk and the risk of management override of controls.

c. Furthermore, the internal audit function and monitors the design and effectiveness of the organisation’s fraud programmes and internal control over financial reporting.

d. Finally, external auditors have the responsibility to plan and perform an audit to obtain reasonable assurance that the financial statements are free of material misstatement, whether caused by error or fraud.

5. Scepticism. With respect to fraud deterrence and detection, scepticism involves the validation of information through probing questions, the critical assessment of evidence, and attention to inconsistencies.

a. Scepticism increases not only the likelihood that fraud will be detected, but also the perception that it will be detected. In turn, this reduces the risk that fraud will be attempted.

b. The CAQ Fraud Report noted that management exercises scepticism by periodically testing assumptions about financial reporting processes and controls, and always remaining aware of the potential for fraud within the organisation.
c. To that end, boards of directors and audit committee members should employ a sceptical approach in discharging their oversight responsibilities.

d. For both internal and external auditors, scepticism is important as they conduct their professional duties and should include consideration of the risk of management override of controls.

6. Communication across the financial reporting supply chain. The CAQ Fraud Report encourages those involved in an organisation’s financial reporting process to leverage their complementary and interconnected responsibilities for the deterrence and detection of fraud through frequent and robust communications.

   a. As the hub for many of these communications, the audit committee plays an important role.

   b. Together, the CAQ believes that these communications enable the sharing of information, perspectives, and concerns that provide a view into the organisation that is “greater than the sum of its parts.”

   c. Making these communications open and robust exchanges, rather than merely compliance-oriented discussions, will yield maximum benefits for all parties.

5. The CAQ plans to encourage continued collaboration with participants (and related professional organisations where appropriate) to leverage existing resources, share ideas, and prioritise future activities to advance the deterrence and detection of financial reporting fraud.

6. CAQ plans to focus its efforts in four areas:

   a. Understanding conditions that contribute to fraud;

   b. Promoting efforts to increase scepticism;

   c. Moderating the risks of focusing only on short-term results; and

   d. Exploring the role of information technology in facilitating the deterrence and detection of fraudulent financial reporting.

II. ASSESSING AN ORGANISATION’S FRAUD EXPOSURE

A. There are certain principles to keep in mind when designing internal control to deter employee fraud.

   1. While the goal is to design policies and procedures that discourage fraud from occurring, there are limits to what internal control can do to prevent fraud.

   2. It is impossible to implement internal control that eliminates the possibility of fraud. Collusion among employees can significantly undermine the effectiveness of the best-designed internal control.

   3. Also, even if it were possible to implement fraud-proof internal control, it would be prohibitively expensive and likely would impair the effectiveness of the organisation to conduct its principal activities.

      a. For example, a restaurant may be able to prevent its bartenders from stealing cash receipts (except through collusion) by having a second employee collect from customers.

      b. However, if slow service drives away customers, the lost business may be more costly than the fraud itself.

      c. The accountant, auditor, or consultant therefore must consider the balance between the nature and extent of fraud prevention controls and the cost of those controls.

B. Specialised industry considerations. The following discussion addresses misappropriation of assets that affects most organisations. Some specialised industries (financial institutions, construction contractors, etc.) have their own unique fraud exposures, which are beyond the scope of this material.

C. Designing internal control to prevent misappropriation of assets
1. A system of internal control is recognised as being an organisation’s most important deterrent to fraud.
   a. A well-designed and maintained system of internal control can prevent or timely detect most types of misappropriations of assets.
   b. Early detection is in itself a means of preventing fraud. There is evidence to suggest that employees who believe they will be caught may think twice when they are tempted to steal.

2. Conversely, internal control weaknesses may allow fraud to occur and remain undetected.

3. One solution, a five-step approach to designing internal control to prevent misappropriations of assets, is detailed as follows (and detailed immediately following):
   a. Step 1: Review the organisation level components of internal control and identify weak or non-existent controls.
   b. Step 2: Identify assets (and related transactions) susceptible to misappropriation.
   c. Step 3: Review the organisation’s systems and procedures relating to the vulnerable areas and identify weak or missing systems and procedures.
   d. Step 4: Develop controls to reduce the risk of misappropriation in the vulnerable areas.
   e. Step 5: Consider the cost/benefit relationship of the controls developed.

4. **Step 1: Review the organisation level components of internal control**
   a. The organisational level components of internal control are the control environment, risk assessment, communication, and monitoring. From the perspective of preventing misappropriation of assets, those components could be described as follows:
      i) The organisation’s control environment, including how the organisation sets a tone that emphasizes integrity and ethical behaviour, hires capable and qualified employees, and appropriately assigns authority and responsibility.
      ii) The organisation’s process of identifying risks relating to misappropriation of assets and developing appropriate responses to those risks.
      iii) The organisation’s communication to employees of how internal control should work, and the responsibilities of employees and management regarding internal control for preventing and detecting fraud.
      iv) The organisation’s monitoring of controls to ensure they continue to be relevant and able to address new fraud risks.
   b. For all types of fraud, including the misappropriation of assets, the board of directors and management should explicitly understand their responsibilities for fraud risk management. In larger organisations, written policies and procedures, such as codes of conduct, expense account policies, and investigation of suspected fraud incidents, should exist to manage fraud risks.
   c. Many organisations have written policies and procedures pertaining to fraud risks, but it has been observed that these are not regularly referred to by employees in the course of their day-to-day activities. These entities could benefit from having concise summaries that employees would regularly consult and eventually internalize in daily behaviours, and that internal and external auditors could confirm are being adhered to.
   d. The fraud guidance discussed in Managing the Business Risk of Fraud: A Practical Guide (“Guide”) refers to the aggregate of these fraud-related activities as the fraud risk management programme. The Guide indicates that the following should be found with a fraud risk management programme.
i) Roles and Responsibilities. The roles and responsibilities should be defined for all stakeholders—board of directors, audit committee, management, internal audit and staff—regarding managing the risk of fraud.

ii) Commitment. The board of directors and senior management should explicitly express their commitment to fraud risk management through various forms of communication such as codes of conduct, organisational values or principles, or other vehicles that demonstrate the importance of fraud risk mitigation to the organisation.

iii) Fraud Awareness. Fraud awareness is a proactive approach of considering the types of fraud that can occur (misappropriation or otherwise), the assessment of fraud risk, training of personnel, and frequent communication.

iv) Affirmation Process. When a code of conduct or other fraud control policy exists, directors, employees, and others should affirm that they have read, understood, and complied with the requirements (when legally permissible).

v) Conflict Disclosure. Processes should exist for directors, employees, and others to self-disclose potential or actual conflicts of interest.

vi) Fraud Assessment. A fraud risk assessment, overseen by the board, should be performed on a systematic and recurring basis that considers fraud schemes and scenarios and mapping those risks to controls.

vii) Reporting and Whistleblower Protection. The organisation's risk management documentation should clearly articulate a zero tolerance for fraud and include the expectation that suspected fraud should be reported immediately. Channels for reporting should be defined and communicated, along with the protections guaranteed to individuals reporting suspected fraud.

viii) Investigation Process. A protocol should exist for investigating suspected fraud, including associated roles and responsibilities, legal actions, and reporting.

ix) Corrective Action. Policies should communicate consequences and processes for those who commit or condone fraudulent activity. In addition, policies should establish the remediation activities for addressing identified deficiencies that may have resulted in the fraudulent activity.

x) Quality Assurance. Policies and procedures should address the periodic evaluation of the effectiveness of the fraud risk management programme and monitor changes.

xi) Continuous Monitoring. The fraud risk management programme, along with the related documentation, should be revised and reviewed on an ongoing basis to reflect current conditions.

e. The extent of formalised policies, procedures, and documentation of the fraud risk management programme will vary based on the size, complexity, and sophistication of the organisation. However, all organisations should consider embodying relevant aspects of the foregoing elements, in order to mitigate the risks of fraud either involving misappropriation of assets or fraudulent financial reporting.

5. **STEP 2: Identify assets (and related transactions) susceptible to misappropriation**

   a. The opportunity to commit and conceal fraud -

      i) Exists where

         • There are assets susceptible to misappropriation and

         • The controls are inadequate to prevent or timely detect fraud.
ii) Combined, these two elements create a fraud exposure – i.e., an area where the organisation is vulnerable to fraud.

iii) Identifying fraud exposures requires an understanding of the nature of the business (for example, the types of revenue received) and the systems and procedures used to record transactions.

b. The first step in identifying fraud exposure is to identify which assets held by the organisation are susceptible to misappropriation. The following assets are generally more susceptible to misappropriation:

i) Cash, including currency and instruments readily converted to cash, such as cheques or money orders.

ii) Inventory that has a small size, high value, or high demand.

iii) Assets easily convertible into cash such as bearer bonds, diamonds, or computer chips.

iv) Equipment or other fixed assets that have small size, ready marketability, or lack of ownership identification.

c. In identifying which assets are susceptible to misappropriation, consideration would be given to the likelihood and significance of the risk of misappropriation and the types of the fraud schemes that could occur. As part of this process of fraud risk assessment, the incentives, pressures, and opportunities for the misappropriation of assets would be considered.

d. Note that assets can be stolen in ways other than merely removing them from the premises.

i) For example, cash can be stolen by writing cheques to fictitious employees or vendors and cashing them for personal use or having them directed to a confederate outside the company.

ii) Inventory or other assets can be stolen through bogus “sales” to fictitious customers. Thus, when considering fraud risk, it is important to consider which assets are vulnerable, and the various ways they could be misappropriated, given the organisation’s activities.

e. The tabular presentation on the following page provides examples of ways assets can be misappropriated from commercial businesses.

f. Vulnerable assets can be identified based on knowledge of the organisation and its industry and discussions with organisation personnel.

i) Practice aids and checklists can be used to document the vulnerable assets identified and the ways they can be stolen.

ii) It also provides places to document key control weaknesses that would allow the fraud acts to remain undetected and ways the fraud might be concealed.

iii) Another consideration is whether there are any symptoms that fraud may be occurring.

6. **STEP 3: Review the organisation's systems and procedures relating to the vulnerable areas**

a. Once the vulnerable areas have been identified, the next step is to review the organisation's systems and procedures relating to these areas, including such matters as:

i) How transactions are approved, initiated, completed, recorded, and reported.

ii) The policies and procedures relating to the preceding steps, including the controls in place that are intended to safeguard the organisation's assets.

iii) The documentation relating to the preceding processes.
iv) The IT systems involved in the preceding steps. (Depending on the importance of IT to the processes or internal control, it may be necessary to consider the related IT controls.)
v) The personnel involved with these steps.
b. Control activities are policies and procedures established to help ensure management directives are carried out. These activities usually involve two elements:
i) A policy that establishes what should be done, and
ii) The procedure that implements the policy.
c. Commonly encountered types of asset misappropriation schemes are set forth in the table below.

<table>
<thead>
<tr>
<th>Financial Reporting Area</th>
<th>Asset Stolen</th>
<th>Type of Misappropriation</th>
</tr>
</thead>
</table>
| Cash                     | Cash         | • Stealing cash funds processed or on hand.  
                         |              | • Not recording and stealing cash receipts.  
                         |              | • Under-ringing sales and stealing cash receipts.  
                         |              | • Altering bank deposits (for example, in “less cash” schemes).  |
| Accounts receivable, sales | Cash         | • Lapping.  
                         |              | • Forging cheques received.  
                         |              | • Altering credit card receipts.  
                         |              | • Granting credit for merchandise not returned and stealing the cash.  
                         |              | • Writing off receivables as bad debts and stealing the cash received on the accounts written off.  
                         |              | • Collusion between the buyer and seller to process refunds for goods not returned.  |
| Inventory, fixed assets  | Inventory, fixed assets | • Stealing assets.  
                         |              | • Selling assets and keeping the proceeds for personal use.  
                         |              | • Setting up fictitious customers and shipping assets to them.  
                         |              | • Diverting shipments to a wrong address.  |
| Accounts payable, purchases | Cash         | • Using organisation cheques to pay personal bills.  
                         |              | • Setting up fictitious suppliers and “buying” goods or services from them.  
                         |              | • Collusion between an employee buyer and seller in which the buyer receives a kickback for paying inflated prices, buying unneeded goods, or accepting inferior quality.  |
| Accounts payable, purchases (cont’d) | Inventory or other assets | • Ordering goods or services for personal use.  |
| Payroll                  | Cash         | • Setting up fictitious employees (ghost employees) on the payroll records and taking their pay.  
                         |              | • Manipulating payroll records to divert wages or payroll taxes.  
                         |              | • Overstating hours worked.  
                         |              | • Working unauthorised overtime.  
                         |              | • Cashing unused payroll cheques.  
                         |              | • Perpetrator writing payroll cheques to self.  
                         |              | • Embezzling payroll withholdings.  
                         |              | • Keeping terminated employees on the payroll and diverting their pay.  |
d. Reviewing systems and controls. When reviewing an organisation’s systems and control over assets and related transactions vulnerable to misappropriation, the following information should be developed and obtained:

i) How is the type of transaction initiated and authorised? What processing steps are involved? Who performs those procedures? Do they have other duties that may be incompatible (e.g., to record entries to the accounting records and maintain custody of underlying physical assets)? When that person is not available, who is the backup? Who else has access to perform those procedures in addition to those assigned the procedures?

ii) What records and documents are involved? How are documents filed and stored? What do the employees call them? How are they completed? If they are completed electronically, who are all the individuals with access to that terminal, system, or password?

iii) How is the authorisation indicated (initial, signatures, electronic, or stamps)? Are the approvals verified? How? Are stamps and other approval tools available to others? Are they kept under lock and key (or password protected) and only made available to the individuals responsible for the authorisations?

iv) Have there been incidents where accounting and approval control procedures were not followed? How, when, and by whom?

e. There often will be found to be a difference between the controls as designed versus how they are being implemented. Therefore, make these inquiries of the employees who actually perform procedures instead of supervisors.

f. In some cases, internal and external auditors may have compiled some of this information in conjunction with other work. If so, the auditors should make sure that the documented procedures are still in place by inquiring of and observing employees who perform the procedures.

Examples of Asset Misappropriation Schemes from Commercial Businesses

<table>
<thead>
<tr>
<th>Borrowings</th>
<th>Cash</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Unauthorised borrowing against organisation assets.</td>
</tr>
<tr>
<td></td>
<td>• Diverting loan proceeds for personal use.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Equity accounts</th>
<th>Cash</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Diverting equity proceeds to personal use.</td>
</tr>
<tr>
<td></td>
<td>• Underpaying dividends to certain investors and diverting the difference to personal use.</td>
</tr>
<tr>
<td></td>
<td>• Selling shares of stock more than once.</td>
</tr>
</tbody>
</table>
7. **STEP 4: Develop controls to reduce the risk of misappropriation in vulnerable areas**
   
a. After learning about existing systems and controls in a vulnerable area, the next step is to consider what controls need to be in place to reduce the risk of fraud.

b. Controls can be either preventive or detective in nature.
   
i) Preventive controls are designed to keep fraud from occurring.
   
ii) Some examples of preventive controls include locking up the blank cheque stock, having someone independent of accounts receivable open the mail and prepare the deposit slip, using pre-numbered sales receipts, setting appropriate authorisation limits, and using a capital budget for fixed asset purchases.

iii) Detective controls, by contrast, are designed to detect fraud soon after it has occurred.

iv) Some examples include having an independent employee reconcile the checking accounts within a reasonable number of days of receipt, having an independent employee review the accounts payable master list periodically to ensure only valid vendors have been added, and conducting periodic surprise inventory counts.

c. The following are examples of the types of policies and procedures that may be used to prevent or detect misappropriations of assets (details follow):
   
i) Performance reviews.
   
ii) Independent checks.
   
iii) Separation of duties.
   
iv) Access and authorisation controls.

d. Performance reviews are comparisons of current financial reports to other information.
   
i) For example, a manager may compare current period sales or earnings information to budgets or prior year information.
   
ii) Another type of performance review is comparing financial information to operating data, such as sales to merchandise shipments.
   
iii) Investigating significant differences from expected results can uncover indications of fraud.

e. Independent checks test another employee’s work. Independent checks may be accomplished in many ways, such as:
   
i) Second check. An employee’s work might be re-performed or tested by a supervisor or second employee.
   
ii) Computer validation. Computers may test the employee’s work. For example, the computer may compare sales orders to a list of approved customers. It may report or refuse to process a transaction or entry with exceptions.
   
iii) Employee vacation or rotation. Sometimes concealing or perpetuating a fraud requires continual attention by the perpetrator. To deter those frauds, some organisations require annual vacations, preferably at least two full weeks. While they are gone, the employees’ duties are performed by others. This makes fraud more difficult to conceal. The same control objective can be met by periodically rotating employees’ duties.
   
iv) Audits. Periodic internal or independent audits of activities can help detect fraud, and the auditor’s presence can discourage dishonest employees from attempting to commit fraud.
f. Separation of duties. Separation of duties is one of the most effective controls to prevent or timely detect misappropriations of assets. Likewise, areas lacking separation of duties often provide opportunity for fraud. When possible, incompatible duties should be performed by different employees or an owner/manager. For example, the responsibility for authorising transactions, recording transactions, and maintaining custody of assets should be assigned to different people in the organisation.

g. Access and authorisation controls. These are controls that are designed to ensure that only appropriate employees can enter into transactions or have access to organisation assets, documents, and records. Examples of such controls include:
   i) Password protection of computer files.
   ii) Authorisation limits on purchase orders and cheque signing.
   iii) Dual custody of cash receipts or cash on hand.
   iv) Physical safeguards on assets susceptible to theft (for example, vaults for cash or stocks and security measures for inventory or small assets).
   v) Physical controls over organisation documents and records (such as storing cheques and invoices in locked cabinets).

h. Effective authorisation and access controls reduce opportunities to commit and conceal fraud. Simply put, employees cannot steal assets they do not have possession and control over, and they cannot alter documents or records to conceal fraud without access to those items.

i. Independent auditors, of course, cannot be charged with designing controls for audit clients (to do so would result in auditing one's own work, as well as a loss of auditor independence), but accountants are called upon frequently to help non-attest clients design and implement controls. Depending on the scope of the controls design assignment, it may be appropriate to take either of the following approaches, or a combination of both, to the development specific controls:
   i) Global approach. Perform a complete reassessment of all controls in the vulnerable area.
   ii) Targeted approach. Consider the organisation's vulnerability to specific fraud schemes and assess the related controls.

8. STEP 5: Consider the cost/benefit relationship of the controls developed

a. As stated, there are always practical limits to what internal controls can achieve, particularly since collusion among members of the organisation can significantly undermine the effectiveness of the best-designed internal control.
   i) Even if it were theoretically possible to implement fraud-proof internal control, it would likely be prohibitively expensive and could impede the effectiveness of the organisation to conduct its principal activities (for example, by requiring multiple levels of review and approval before even routine customer transactions could be consummated).
   ii) Therefore, when assessing an organisation's internal control, an accountant, auditor, or consultant should consider the relationship between the nature and extent of fraud controls recommended and the cost of those controls.

b. For example, instead of trying to prevent fraud, an organisation may choose to use more detective controls.
   i) As noted, detective controls ensure the organisation identifies and corrects errors and fraud in a timely fashion.
   ii) Because detective controls are performed after the original transaction occurs, they may be easier to implement and more cost effective.
III. CASH FRAUD SCHEMES

A. Cash is an inherently risky asset for most businesses. The table below summarizes common cash fraud schemes and the types of controls that are intended to reduce fraud risks. Additional observations follow the table.

<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
</table>
| Skimming all or part of a cash sale    | In general:  
• Separate responsibility for authorising the sale, delivering the goods, receiving payment, and bookkeeping.  
• Use pre-numbered sales receipts.  
• Have an employee independent of billing, accounts receivable, and cash handling, investigate customer complaints.  
• Compare current cash receipts volumes to historical or expected cash receipts volumes.  
• Perform analytical procedures that compare adjusted inventory levels to sales.  
• Rotate personnel who have physical custody of daily receipts.                                                                                                                                 |
|                                        | In a retail operation:  
• Use cash registers with cumulative totals, multi-part register tapes.  
• Lock the cash register tape compartment and have the manager keep the key.  
• Use cash register reconciliation forms each day. Attach a copy of the daily close-out tape to the form. Compare the tape totals to the reconciliation form and the deposit.  
• Review the close-out tape to see whether an excessive number of “no sales” or “voids” occurred during the shift.  
• Maintain separate register drawers for each cashier, if possible. Close out the register at the end of each shift.  
• Count and reconcile the cashier or teller funds at the close of each shift. Have a supervisor review reconciliations and investigate unusual reconciling items.  
• Maintain a cash “over” and “short” list for each cashier. Investigate both overages and shortages.  
• Maintain an adequate, but not excessive, amount of cash in the register during all shifts.  
• Consider using a time-lock safe that dispenses change for large bills. Require that large bills be deposited in the safe immediately on receipt.  
• Consider using surveillance or spotters.  
• Post notices offering customers gifts if they do not receive a receipt or it is incorrect.  
• Post a toll-free number to which customers can make complaints.                                                                                                                                 |
| Stealing daily deposits                | • Separate the duties of opening daily receipts, listing cash receipts, and preparing the deposit slip, from reviewing the validated deposit slips, recording payments, and originating non-cash credits to customer accounts.  
• Separate responsibility for cash receipts, accounts receivable, and cash disbursements from responsibility for reconciling the bank statement.  
• Consider using a lockbox for large volume cash receipts.  
• Use a “For Deposit Only” endorsement stamp on all cheques upon receipt.  
• Make all deposits intact daily. (The employee making the deposit should not be the cashier or work in accounts receivable.)  
• Maintain cash receipts separately from cash funds.  
• Keep un-deposited amounts in a safe.  
• Rotate personnel who have physical custody of daily receipts.  
• Use an armoured guard to collect the daily deposit if the business accepts large amounts of cash.  
• Use multi-part deposit slips and compare the amount on the in-house copy to the amount deposited on the bank statement.                                                                                                                                 |
<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>The “less cash” scheme</td>
<td>• Assess the knowledge of the tellers at your bank.</td>
</tr>
<tr>
<td></td>
<td>• Use multipart deposit slips. Compare the amount on the in-house copy of the deposit slip to the amount deposited on the bank statement.</td>
</tr>
<tr>
<td>Voids and sales returns schemes</td>
<td>• Use cash registers with cumulative registers and multi-part cash register tapes.</td>
</tr>
<tr>
<td></td>
<td>• Use a daily cash register reconciliation form. Attach a copy of the daily close-out tape to the form. Compare the tape totals to the reconciliation form and the deposit.</td>
</tr>
<tr>
<td></td>
<td>• Use cash registers that require a manager override key for voids and sales returns. (Managers should not let these keys out of their possession when on the job.)</td>
</tr>
<tr>
<td></td>
<td>• Use a standard pre-numbered form for sales returns.</td>
</tr>
<tr>
<td></td>
<td>• Review the close-out tape to see whether an excessive number of “no sales” or “voids” occurred during the shift.</td>
</tr>
<tr>
<td></td>
<td>• Require authorisation of all sales returns by a second clerk or the manager.</td>
</tr>
<tr>
<td></td>
<td>• Have the owner/manager or other appropriate person review actual sales returns versus budgeted or expected amounts.</td>
</tr>
<tr>
<td></td>
<td>• Collect the name, address, and phone number of customers returning merchandise. Call them on a test basis.</td>
</tr>
<tr>
<td>Stealing cash on hand</td>
<td>• Minimize amount of petty cash kept on hand.</td>
</tr>
<tr>
<td></td>
<td>• Lock up the petty cash fund.</td>
</tr>
<tr>
<td></td>
<td>• Use standard transaction tickets for each transaction.</td>
</tr>
<tr>
<td></td>
<td>• Require original receipts to support petty cash disbursements and review them closely.</td>
</tr>
<tr>
<td></td>
<td>• Reconcile and replenish petty cash monthly.</td>
</tr>
<tr>
<td></td>
<td>• Perform periodic surprise cash counts to verify that the sum of receipts and cash on hand agree to the book balance of the fund. If the fund “cashes” cheques for employees, the cheques should be deposited in a timely fashion.</td>
</tr>
<tr>
<td></td>
<td>• Rotate personnel who have physical custody of daily receipts.</td>
</tr>
<tr>
<td></td>
<td>• Be careful when using adding machine tapes provided by the petty cash custodian. Check to see that they start with a zero balance or that an item total is included and the number of items on hand agrees.</td>
</tr>
<tr>
<td></td>
<td>• Maintain cash receipts separately from cash funds.</td>
</tr>
<tr>
<td></td>
<td>• Make all deposits intact daily. (The employee making the deposit should not be the cashier or work in accounts receivable.)</td>
</tr>
<tr>
<td></td>
<td>• Use an armoured guard to collect the daily deposit if the business accepts large amounts of cash.</td>
</tr>
</tbody>
</table>

1. Skimming
   a. Skimming is stealing the proceeds from a cash sale before it is recorded.
      i) For example, a cashier in a retail store may simply fail to ring up a sale and keep the cash collected from the customer.
      ii) Alternatively, a cashier may record a sale at less than full amount and steal the difference. For example, a cashier may ring a S$250 sale as S$150 and keep the remaining S$100.
      iii) In a manufacturer with poor separation of duties, a clerk who prepares invoices and receives payments may invoice the customer for S$550, alter the invoice to read S$350, and pocket the S$200 difference.
   b. These thefts can be difficult to detect because they occur before a paper trail has been created.
c. In addition, it may be impossible to separate incompatible tasks because there may be only one or two employees on the premises during a shift. Therefore, some organisations supplement their internal controls by asking for customer assistance (for example, by giving customers gifts if they report to a manager the fact that a receipt was not provided).

2. Stealing Daily Deposits
   a. One simple cash fraud scheme is to steal daily deposits. The perpetrator may steal an entire deposit or part of the deposit.
   b. Unlike skimming, a paper trail generally is created, which can be a problem for the perpetrator.

3. “Less Cash” Schemes
   a. “Less cash” schemes involve diverting cash from a deposit.
   b. In commercial checking accounts, cash receipts are normally deposited intact. Thus, there are no “less cash” lines on these deposit slips. However, some perpetrators have written “Less cash $XXX” and received cash back from deposits.
   c. For this fraud to be effective, bank tellers must be unaware that they are not allowed to give cash back on those commercial accounts.
   d. In addition, there is usually a lack of separation of duties at the organisation.

4. Fraud Using Voids and Sales Returns
   a. Dishonest clerks may void legitimate sales transactions.
      i) For example, a clerk may make an $80 cash or credit card sale and properly record the sale in the cash register. After the customer leaves the store with the merchandise, the clerk may void the sale. The clerk can then steal $80 from the cash register.
      ii) In one case, the headwaiter for a restaurant obtained the assistant manager’s cash register keys under a pretext. He voided the last two cash sales from his shift—pocketing $150 in cash. Had another employee not reported the theft, use of the assistant manager’s keys would have made the voids appear legitimate.
   b. Clerks can also commit fraud with sales returns. There are many types of sales return schemes, such as:
      i) Fictitious Sales Returns. A clerk can process refunds for merchandise not returned and steal the refund.
      ii) Inflated Refunds. The clerk can process refunds at full retail price for goods purchased at a discount. (He would give the customer the discounted amount and keep the difference.)
   c. These schemes may be committed by an employee acting alone or in collusion with a customer.

5. Stealing Cash on Hand
   a. Individuals with access to cash drawers, petty cash funds, vaults, and other cash on hand can steal cash in a variety of ways.
   b. Examples include the following:
      i) Trade a personal cheque for cash but do not deposit the cheque. Periodically, the cheque may be replaced by a cheque with a later date or the “loan” may be repaid.
      ii) Steal the cash and dummy up receipts from vendors. For example, some beer suppliers accept only cash. Therefore, a bar may maintain a large petty cash fund that is frequently replenished.
iii) Claim reimbursement for personal purchases.

iv) Steal the cash (especially if multiple employees use the drawer during a shift).

B. Preventive and detective cash controls

1. Detecting misappropriations in a timely fashion, and once identified, firing and prosecuting the perpetrator may deter another employee who is considering stealing.

2. Some techniques that have been found useful are the following:

a. Use spotters and surveillance. These can be effective methods for preventing and detecting skimming and other cash thefts perpetrated before sales are recorded. Retailers with a single employee on location during certain shifts (for example, petrol stations open 24 hours or self-storage units) frequently use surveillance cameras both to detect theft and to protect workers during robberies, on the theory that the perpetrator will be less likely to harm the workers if being recorded on camera. Some of the video cameras record cash register activity based on special criteria; for example, some ring alarms at remote locations and begin recording when the “no sale” key is pressed.

b. Perform inventory comparisons. In some businesses it is not possible to apply surveillance techniques. If there is inventory, managers should count the inventory periodically (in some cases, daily) and compare the change in inventory to recorded sales. The retail inventory method is particularly suited to this purpose. If recorded sales and cash receipts are less than the amount indicated by change in inventory at retail, adjusted for purchases also at retail, there are several possibilities: a transaction occurred that should be explained on the daily close-out form, cash was stolen outright, cash was stolen and sales were under-recorded, or inventory was stolen (increasing cost of sales).

c. Use alternate parties. Many companies require employees (especially employees who handle cash) to take an annual vacation lasting, at a minimum, one or two weeks. During the time an employee is on vacation, a co-worker should perform his or her tasks. If cash receipts increase during the days when the co-worker performs the procedures, it could mean that thefts have been occurring. Additional procedures will be required to identify the perpetrators and determine the amount of the loss.

d. Perform bank reconciliations. One of most effective ways of detecting cash fraud in a timely fashion is to have a properly trained employee independent of the cash receipts and cash disbursement function perform monthly bank reconciliations of all accounts (the “four column bank reconciliation” is the tool of choice). Thefts of cash often cause reconciling items on bank reconciliations. For example, an employee may list a cheque as void on the cheque register but actually issue the cheque to a phony company. This cheque will show up as a reconciling item on the bank reconciliation because it has not been recorded. The reconciling item can then be removed through a journal entry to cash and expense (or another account).

a. Bank statements should be mailed directly to a designated person, who should be trained to look for the following matters:

i) Timing. Reconcile all bank accounts as of the same date. Otherwise, the perpetrator can conceal fraud by shifting reconciling items among different bank accounts.

ii) Transfers. Make sure all matching inter-bank or inter-company transfers have the same date. This procedure could detect thefts concealed as inter-company transfers. For example, a deposit in transit from one account to another may be listed as a reconciling item repeatedly but never actually deposited.
Reconciling Items. Trace all reconciling items to supporting documents. Pay special attention to old reconciling items. Adding the cheque amount to another reconciling item could hide a “void” cheque that was actually disbursed. A journal entry can conceal the theft permanently. Other reconciling items, individually immaterial, may result from a significant amount “sliced up” for concealment.

Paid Items. Review all cheque fronts and backs. Look for cheques with more than one endorsement, endorsements by employees when the payee is not the employee, erasures or white outs of payees or amounts, unusual transactions, payee names that are similar to but not the same as typical vendors, and discrepancies between the payees on the cheque register and the cheque.

e. Review journal entries. The owner or manager should review the journal entries to the cash accounts on a timely basis. The owner or manager should be especially alert for journal entries that might be write-offs of reconciling items.

IV. ACCOUNTS RECEIVABLE FRAUD SCHEMES

A. Receivables fraud normally involves manipulating accounts receivable and sales to steal cash or other assets from an organisation. Accounts receivable is often a major target for fraud against businesses or other organisations. This section discusses common receivables fraud schemes.

B. Types of receivables fraud schemes

1. There are many ways to commit receivables fraud, but most of the schemes fall into one of the following categories:
   a. Lapping
   b. False credits, discounts, and other write-offs
   c. Unauthorised shipments
   d. Diversion of goods shipped
   e. Kickbacks
   f. Collection agency schemes

2. The table below shows common receivables fraud schemes and related controls. Each of these fraud schemes is further discussed in the text following the table.

<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lapping</td>
<td>• Have someone not involved in making the bank deposit or accounts receivable bookkeeping open the daily mail, count the cash and cheque amounts received, and report those totals to the owner/manager or another appropriate person, who compares the reported amount to the amount actually deposited.</td>
</tr>
<tr>
<td></td>
<td>• Have someone independent of cash receipts, cash handling, and accounts receivable recordkeeping compare the details of daily deposit slips with the postings to individual receivable accounts.</td>
</tr>
<tr>
<td></td>
<td>• Have the person who opens the mail stamp “for deposit only” on the back of each cheque received.</td>
</tr>
<tr>
<td></td>
<td>• Use a lockbox system.</td>
</tr>
<tr>
<td></td>
<td>• Separate responsibility for cash receipts, accounts receivable, and accounts payable from responsibility for reconciling the bank statement.</td>
</tr>
<tr>
<td></td>
<td>• Reconcile all bank accounts monthly, with review by the owner/manager or another appropriate person.</td>
</tr>
<tr>
<td>Fraud Scheme</td>
<td>Preventive or Detective Controls</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lapping (cont’d)</td>
<td>• Have someone outside the accounting function review the detailed bank reconciliation documentation and any adjusting entries made to the books.</td>
</tr>
<tr>
<td></td>
<td>• Use multi-part deposit slips. (One copy should be reviewed and maintained by someone other than the employee who completed it.)</td>
</tr>
<tr>
<td></td>
<td>• Regularly reconcile the accounts receivable general ledger balance to the subsidiary ledger, with appropriate supervisory review and follow-up.</td>
</tr>
<tr>
<td></td>
<td>• Separate receivables collections from receivables recordkeeping.</td>
</tr>
<tr>
<td></td>
<td>• Prepare an aged trial balance and have someone other than the person posting accounts receivable call customers to follow-up on delinquent accounts.</td>
</tr>
<tr>
<td></td>
<td>• Require mandatory vacations that are at least two weeks long for all personnel in accounts receivable and cash handling functions. Vacations should occur at the end of an accounting cycle. Cross train employees so that someone else does the job during the vacation.</td>
</tr>
<tr>
<td></td>
<td>• Require supervisory approval before customers are added to or deleted from the master file.</td>
</tr>
<tr>
<td>False credits, discounts, and</td>
<td>• Separate receivables collections from receivables recordkeeping. Accompany each write-off with a final letter demanding payment. (If the customer already paid the bill, he or she should complain.)</td>
</tr>
<tr>
<td>other write-offs</td>
<td>• Separate duties for maintaining the accounts receivable subsidiary ledger and the general ledger.</td>
</tr>
<tr>
<td></td>
<td>• Have a manager without responsibility for the accounting function, review allowances for doubtful accounts, sales returns, and open account balances based on his or her knowledge of the account's history.</td>
</tr>
<tr>
<td></td>
<td>• Have a manager review the aging reports each month for unusual items, making sure the aging report agrees to the general ledger.</td>
</tr>
<tr>
<td></td>
<td>• Separate the duties for the credit function from the billing function.</td>
</tr>
<tr>
<td></td>
<td>• Have someone independent of the preparer of the daily deposit list, cash handling, billing, and accounts receivable recordkeeping investigate customer complaints and billing questions.</td>
</tr>
<tr>
<td></td>
<td>• Have someone independent of cash receipts, cash handling, and accounts receivable recordkeeping compare the details of daily deposit slips with the postings to individual receivable accounts.</td>
</tr>
<tr>
<td></td>
<td>• Use pre-numbered and multipart credit memos, invoices, and shipping documents. Maintain one part in sequential order and check for missing or out of sequence documents.</td>
</tr>
<tr>
<td></td>
<td>• Require written supervisory approvals for write-offs and credit memos.</td>
</tr>
<tr>
<td></td>
<td>• Compare the volume of credit memos across periods.</td>
</tr>
<tr>
<td></td>
<td>• Retain voided shipping documents, invoices, and credit memos.</td>
</tr>
<tr>
<td></td>
<td>• Lock up unused shipping documents, invoices, and credit memos.</td>
</tr>
<tr>
<td></td>
<td>• Use software controls to limit access to billings, cash receipts, and accounts receivable applications and data files.</td>
</tr>
</tbody>
</table>
### Common Receivables Fraud Schemes and Related Controls

<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unauthorised shipments</strong></td>
<td>• Separate the duties for billing and shipping from cash and accounts receivable bookkeeping.</td>
</tr>
<tr>
<td></td>
<td>• Check shipments for shipping documents.</td>
</tr>
<tr>
<td></td>
<td>• Use two people to count the goods being shipped. Verify that the items and quantities being shipped match the shipping documents.</td>
</tr>
<tr>
<td><strong>Diversion of goods shipped</strong></td>
<td>• Separate the duties for the credit function from the billing function</td>
</tr>
<tr>
<td></td>
<td>• Have someone independent of the preparer of the daily deposit list, cash handling, billing and accounts receivable, recordkeeping, follow-up on customer complaints and billing questions.</td>
</tr>
<tr>
<td></td>
<td>• Review shipping documents looking for names and addresses that are unusual. (An internal auditor may use a computer to match the address portion of the accounts receivable master file with the shipping documents.) Research unusual items.</td>
</tr>
<tr>
<td></td>
<td>• Require written supervisory approvals for write-offs and credit memos.</td>
</tr>
<tr>
<td></td>
<td>• Compare the volume of credit memos across periods.</td>
</tr>
<tr>
<td></td>
<td>• Retain voided shipping documents, invoices, and credit memos.</td>
</tr>
<tr>
<td></td>
<td>• Lockup unused shipping documents, invoices, and credit memos.</td>
</tr>
<tr>
<td><strong>Kickbacks</strong></td>
<td>• Calculate sales commissions on the basis of recorded sales so the commissioned sales people effectively monitor the recording of sales.</td>
</tr>
<tr>
<td></td>
<td>• Have someone independent of cash receipts, cash handling, and accounts receivable recordkeeping compare the details of daily deposit slips with the postings to individual receivable accounts.</td>
</tr>
<tr>
<td></td>
<td>• Periodically compare billing records to shipping documents. Compare the quantity shipped to the quantity billed. Follow-up on any shipments not yet billed.</td>
</tr>
<tr>
<td></td>
<td>• Separate responsibility for inventory controls, billing, and shipping from cash and accounts receivable bookkeeping.</td>
</tr>
<tr>
<td></td>
<td>• Use software controls to limit access to billings, cash receipts, and accounts receivable applications and data files.</td>
</tr>
<tr>
<td><strong>Collection agency schemes</strong></td>
<td>• Calculate write-off and collection percentages for each collection agency used. Compare the different rates and consider why one agency is more effective than another.</td>
</tr>
<tr>
<td></td>
<td>• Have someone independent of cash receipts, cash handling, and accounts receivable recordkeeping compare the details of daily deposit slips with the postings to individual receivable accounts.</td>
</tr>
<tr>
<td></td>
<td>• Require written approval for all accounts identified to be sent to a collection agency.</td>
</tr>
</tbody>
</table>

3. **Lapping**

   a. Lapping is a classic receivables fraud. It involves stealing a customer’s payment on an account and concealing the theft by applying subsequent payments from other customers to the first customer’s account. For this to be workable, the perpetrator must have access to the customer receipts and must also have recording responsibilities.

   b. A lapping scheme requires a lot of time and effort. In a sense, lapping is like juggling. The more the perpetrator laps, the more “objects” he or she must keep “in the air.” The more objects in the air, the more difficult the juggling act.

   c. Also, because of the intense record-keeping requirements of lapping schemes, perpetrators must plan their absences carefully. They cannot risk taking long vacations, or missing days on which
significant payments are received, which is generally shortly after month end. However, the perpetrator normally has the perfect excuse for being present during this period. This is usually when the organisation closes its books, including the receivables detail.

4. False credits, discounts, and other write-offs
   a. Accounts receivable payments can be stolen and concealed using techniques other than lapping.
      i) For example, an accounts receivable clerk may be able to steal this payment and issue a credit, e.g., for defective merchandise. This credit reduces the customer's balance by the amount of its payment. Because the customer has been given credit for its payment, it may never question the fraudulent transaction.
      ii) Also, unless the vendor has good controls over its cash receipts and sales return functions, it may not notice that the fraud has occurred.
   b. Cash receipt thefts relating to accounts receivable payments can be concealed in the following ways:
      i) Unauthorised credits. The perpetrator can create credit memos (fictitious sales returns, unauthorised discounts, etc.) to reduce the customer's balance.
      ii) Bad debt or other write-offs. Perpetrators may write off a slow paying receivable (or even a good receivable) and steal the payments received on that account.
      iii) Reconciling journal entries. If the perpetrator credits the accounts receivable ledger but not the general ledger, it creates a reconciling item between the receivables ledger total and the general ledger account balance. The perpetrator then writes off the reconciling item using a journal entry.

5. Unauthorised shipments
   a. Unauthorised shipments are thefts of inventory or other assets that are committed or concealed by manipulating sales and accounts receivable. Generally, documentation is created to make it look like inventory shipments were made to fictitious customers set up by the perpetrator.
   b. These schemes typically result in bogus receivables, which must be written off or offset by bogus credits.

6. Diversion of goods shipped
   a. This scheme involves sending legitimately sold merchandise to an address not specified by the customer.
   b. These sales are typically reversed through credit memos or other adjustments to the customers’ accounts.

7. Kickbacks
   a. An accounts receivable kickback scheme may occur when a customer pays an employee to ship goods but to not bill for them, or to ship higher quality goods and charge for goods of a lesser quality.
   b. The corrupt employee receives a gratuity for doing this.

8. Collection agency schemes
   a. In a collection agency scheme, the employee in charge of writing off bad debts identifies certain current receivables as being past due. He or she writes them off, sends them to the collection, and diverts payments to his or her own accounts.
   b. Although not a type of misappropriation, it is also possible the collection agency is stealing the
payments for accounts turned over to them for collection. These schemes generally require collusion between the agency and an organisation employee, who typically receives a kickback.

c. A variation on this scheme is when an employee assigns good accounts receivable to collection agencies. When these receivables are collected, the agency typically receives a percentage of the amount collected. Part of this payment is kicked back to the organisation employee.

C. Preventive and detective accounts receivable controls

1. Review reconciling items and journal entries

   a. Lapping and other diversions can appear as reconciling items on bank reconciliations or the reconciliation between the accounts receivable subsidiary ledger and the general ledger. Reconciling items should be reviewed and traced to supporting documents.

   b. One way to eliminate bogus accounts receivable transactions that have created reconciling items is to write them off via journal entries. Appropriate personnel should review all journal entries and trace to supporting documents.

2. Review the detail of accounts receivable

   a. The detailed records include the accounts receivable trial balance and any other records supporting accounts receivable. An appropriate person should review the detail records of accounts receivable for unusual items.

   b. Examples of unusual items include:

      i) Unusually large entries or transactions (relative to the balance, the customer, or the organisation)

      ii) Unusual credits

      iii) Credit balances

      iv) Significant delinquent balances (especially among new customers)

      v) Unusual items or patterns (such as an unusual number of credits or write-offs by one employee)

      vi) Accounts that seem to be assigned to collection agencies prematurely

      vii) Unusual numbers of credit memos or voids, late charges, or misclassifications

      viii) Accounts written off shortly after being established, particularly ones on which no payments were recorded

   c. An appropriate person should also review the accounts receivable records for unusual customer names, addresses, or telephone numbers.

      i) Examples include customers with names very similar to legitimate company names, companies with P.O. Box addresses only, and customers with the same address.

      ii) An appropriate person may also compare customer addresses and phone numbers to employee addresses and phone numbers.

3. Review credit memos

   a. When inspecting credit memos, an appropriate person should also examine any documentation supporting the credits. An appropriate person may also try to match each credit with the original sales documentation.

   b. If the credit memo indicates the goods were not received, an appropriate person should review the original shipping documents (if any exist) and consider investigating the shipping address.
4. Review the allowance for doubtful accounts
   a. Some companies prepare detailed allowance schedules and specifically identify how much of their allowances relate to specific delinquent customers. If such detailed analyses exist, an appropriate person should obtain and review them for unexpected items such as the following:
      i) An allowance for a large customer who usually pays on time.
      ii) An allowance for a very old account that has not yet been written off.
      iii) An allowance for relatively new customers that never made a payment.
   b. Payments received on the first two accounts can be easily diverted. The third type of account may be a fictitious customer.

5. Perform interviews with collection agencies
   a. Consider asking the personnel at collection agencies used by the company whether customers are complaining of having paid a bill for which they are continuing to be charged.
   b. Because of the insignificance of the accounts or for other reasons, the collection agencies may not have informed the company. This information may help an appropriate person identify lapping.

V. INVENTORY FRAUD SCHEMES

A. Inventory fraud is a significant problem for many businesses.
   1. Unfortunately, inventory fraud is often more difficult to prevent and detect than other asset thefts.
   2. Some of the reasons for this include the large volume of items in inventory, the number of employees with access to the assets, complicated processes involved in production, and the many entries and complex systems used to account for the inventory and production process.
   3. Some inventories are more susceptible to fraud than others. Generally, the most vulnerable inventory has one or more of the following characteristics:
      a. Small and portable
      b. High value
      c. High demand

B. Types of inventory fraud
   1. Inventory can be stolen in many ways. The following are common inventory fraud schemes:
      a. Stealing inventory and scrap. This can include retail merchandise, raw materials, or finished goods. Employees may steal inventory for resale or personal use. In some cases, employees have colluded with shippers by putting extra inventory on the truck. The driver delivers the purchased amount to customers and sells the excess – splitting the proceeds with the employee.
      b. Scrapping and selling good inventory. This may involve collusion with customers, dealers, or distributors.
      c. Sales return schemes. In these schemes, returned products are recorded as sales returns, but the merchandise is never restocked in inventory. The products are usually sold by the perpetrators.
      d. Purchasing frauds. In a typical purchasing fraud scheme, the purchasing agent receives a kickback for buying excess, poor quality, or unsalable items.
      e. Concealing other frauds by increasing the inventory accounts. An example may involve a perpetrator who writes cheques to him/herself and debits an inventory account.
2. The table below summarizes common inventory fraud schemes and related controls.
   a. Other schemes that may involve inventory theft include sending unauthorised shipments or diverting shipped goods.
   b. These schemes are generally committed by manipulating sales and accounts receivable.

<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stealing inventory and scrap</td>
<td>In general:</td>
</tr>
<tr>
<td></td>
<td>• Fence or cage expensive components and products. Strictly limit access to these areas to authorised personnel.</td>
</tr>
<tr>
<td></td>
<td>• Secure the perimeter of the building. Limit the number of non-emergency exits from the building. Have a monitor at those locations.</td>
</tr>
<tr>
<td></td>
<td>• Separate the duties of purchasing and warehousing from approving inventory purchases and disbursements.</td>
</tr>
<tr>
<td></td>
<td>• Have the owner/manager or other appropriate person review monthly financial statements for reasonableness of inventory and cost of sales values, amounts,</td>
</tr>
<tr>
<td></td>
<td>and gross margins.</td>
</tr>
<tr>
<td></td>
<td>• Periodically analyse the components of cost of sales (material, labour, and overhead) as a percentage of sales.</td>
</tr>
<tr>
<td></td>
<td>• Use a computer to compare customer names and addresses with employee names and addresses.</td>
</tr>
<tr>
<td></td>
<td>• Have the owner/manager or other appropriate person periodically review budgeted versus actual production costs and investigate significant differences.</td>
</tr>
<tr>
<td></td>
<td>• Use computer controls to prevent unauthorised access to the sales order, invoicing, and shipping systems.</td>
</tr>
<tr>
<td></td>
<td>• Require employees with inventory, shipping, and receiving responsibilities to take vacations that are at least two weeks long and occur at the end of an accounting cycle. Cross train employees so that someone else does the job during the vacation.</td>
</tr>
<tr>
<td></td>
<td>• Bond employees with access to valuable inventory.</td>
</tr>
<tr>
<td></td>
<td>• Reconcile inventory ledgers to the general ledger control account, with appropriate supervisory review of the reconciliation and follow-up of unusual reconciling items and adjustments.</td>
</tr>
<tr>
<td>Stealing inventory and scrap (cont’d)</td>
<td>Shipping:</td>
</tr>
<tr>
<td></td>
<td>• Match actual counts of units, cartons, pallets, etc. to shipping documents before releasing the merchandise to the shipper.</td>
</tr>
<tr>
<td></td>
<td>• Require that only merchandise with an invoice or appropriate shipping document should be allowed to leave the facility.</td>
</tr>
<tr>
<td></td>
<td>• Maintain a perpetual inventory that is reconciled to control accounts. (Separate responsibility for the perpetual inventory from shipping, billing, and storekeeping.)</td>
</tr>
<tr>
<td></td>
<td>• Use pre-numbered invoices and shipping documents. Periodically account for missing numbers.</td>
</tr>
<tr>
<td></td>
<td>• Lockup unused invoices and shipping documents.</td>
</tr>
<tr>
<td>Fraud Scheme</td>
<td>Preventive or Detective Controls</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------</td>
</tr>
</tbody>
</table>
| **Stealing inventory and scrap (cont’d)** | **Receiving:**  
- Use pre-numbered receiving documents, requisitions, and raw material requisitions. Periodically account for missing numbers.  
- Forward copies of receiving reports to the accounting department for verifying purchase orders and invoices.  
- Do not allow the warehouseman to handle inventory receipts.  
- Periodically analyse the recorded amounts of major raw materials. (For example, calculate how many units of finished goods could have been produced from the amount of raw materials used. Compare estimates to the actual results.)  

**Valuation:**  
- Investigate and review inventory write-downs.  
- Reconcile labour and overhead costs charged to inventory.  
- Have the owner/manager or other appropriate person review and approve adjustments to inventory accounts or perpetual records.  

**Physical observation:**  
- Conduct periodic surprise inventory counts by employees independent of the purchasing and warehouse functions (but who can identify the inventory).  
- Use adequate written instructions.  
- Separate inventory on hand belonging to others and exclude it from the count.  
- Designate employees independent of the purchasing and warehousing functions (but who can identify the inventory) to conduct the physical count.  
- Use count sheets or tags to make sure items are not double counted. Collect them and document used, unused, and voided numbers. (When using count sheets mark through the unused portion of the sheet so that additions cannot be made after the count team passes by.)  
- Halt production or control movement between areas during physical counts.  
- Have the owner/manager or another appropriate person review reconciliations between the extended physical counts and control accounts.  
- Adopt formal policies for scrap sales, requiring appropriate approval of sales.  

**Scraping and selling good inventory**  
- Separate responsibility for identifying or designating scrap from disposing of it.  
- Periodically inspect trash receptacles to look for inappropriate scrap or discarded inventory.  
- If scrap haulers or salvage firms haul away scrap, ensure the products are destroyed and are not diverted or otherwise resold.  

**Sales return schemes**  
- Establish a sales return policy and publicize the policy by posting it on the premises or by sending a notice to customers.  
- Use multipart pre-numbered sales return forms.  
- Require approval by the owner/manager or another authority.  
- Inspect returned merchandise. If it is not defective, check the packaging and if possible, return it to the correct location.  
- Separate defective merchandise and return to suppliers for credit or rework. |
C. Preventive and detective inventory controls

1. Analytical procedures. It can be difficult to prevent inventory fraud. Some organisations rely on the following analytical procedures to help identify inventory fraud:
   a. Age of inventory \( \frac{365 \times \text{average inventory}}{\text{cost of sales}} \). This ratio indicates the average number of days needed to sell the inventory. An increase may indicate a problem in inventory.
   b. Gross profit margin \( \frac{\text{gross profit}}{\text{net sales}} \). This ratio indicates the average percentage of profit generated from each sale. A decrease could reflect losses of inventory.
   c. Inventory turnover \( \frac{\text{cost of goods sold}}{\text{average inventory}} \). Although this ratio is normally used to analyse the effectiveness of inventory management, it can also assist an appropriate person in determining if there may be a problem in inventory or cost of goods sold.

2. These ratios should be computed at the most detailed level possible to identify potential problems. For example, gross margin analysis should preferably be done at least by location and line of business. Comparisons among locations or lines of business can highlight problems.

3. Analytical procedures should be performed on periods throughout the year. Often, all accounts are “cleaned up” by various “window-dressing” devices (e.g., delaying purchases or paying down all payables balances) in the last quarter in preparation for the financial statement audit. Therefore, analytical procedures performed on accounts in other quarters may identify unusual or unexpected patterns.

4. Review the journal entries. Journal entries should be reviewed for any unusual patterns or timing anomalies. For example, a journal entry recording a physical count adjustment to the finished goods inventory would be unusual if it occurred during a period when a physical count was not taken. In some cases, all entries are made to subsidiary records and only a summary entry is booked to the general ledger at the end of each month. The summary entry may be manual or it may be made automatically by the system. If summary entries are made, an appropriate person should review adjustments to the detailed records. In some systems, journal entries are rare. In those cases, all entries should be reviewed and traced to supporting documents.

5. Perform surveillance. Surveillance can be an effective fraud prevention and detection technique procedure for inventory thefts or any theft of a physical asset. There are two basic approaches to surveillance:
   a. Individuals. An accountant can observe how inventory is secured in a particular location and detect theft as it occurs. While effective, this procedure may be inefficient. Surveillance may be required at more than one location and during several different time periods. An appropriate person may also want to use several different spotters so that employees do not become suspicious.
b. Static devices. Surveillance cameras or other static devices can be efficiently used for surveillance. Static surveillance devices may be particularly effective if used during off-hours of operations, when inventory may be removed from the premises.

6. Perform a physical inventory count.
   a. Many companies conduct physical inventories at or near their balance sheet dates because this satisfies an annual audit objective – but, since doing so is entirely predictable, it is less useful in identifying frauds than a randomly-conducted surprise count would be.
   b. Other companies do not take a complete physical count, but rather rely on cycle counts, perpetual records updated continuously, or other methods to value their inventory.
   c. A physical count is an effective way to identify missing merchandise. The count should include scrap, obsolete, unsalable, damaged, slow-moving, and overstocked items. These assets and related accounts are often used for facilitating frauds or for hiding losses, particularly if the inventory turns over rapidly.

7. Some organisations hire an outside inventory firm. Such firms (which are often found in the yellow pages or online search engines using the term “Inventory Services”) provide a wide range of services from counting the inventory to pricing and extending it. These firms provide the following advantages:
   a. They provide efficient, accurate counts with little advance notice.
   b. They increase the element of surprise because organisation employees do not typically need advance notice of the count.
   c. They eliminate the risk that a fraud perpetrator will be on the count team or otherwise participate in the physical count.

VI. FIXED ASSET FRAUD SCHEMES

A. Fixed asset (such as plant and equipment) thefts are not as common as cash or inventory thefts, but they happen. The fixed assets most susceptible to theft are small, easily portable, readily marketable, or lack owner identification.

1. The table below summarizes common fixed asset fraud schemes and related controls; detailed discussion follows the table.

<table>
<thead>
<tr>
<th>Common Fixed Asset Fraud Schemes and Related Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud Scheme</td>
</tr>
<tr>
<td>Stealing fixed assets</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Common Fixed Asset Fraud Schemes and Related Controls

<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal use of assets</td>
<td>• Discuss the organisation’s asset use policy in the employee handbook.</td>
</tr>
</tbody>
</table>
| Personal capital improvements paid by entity     | • Separate authority for purchasing assets from approval for disbursements and bookkeeping.  
|                                                  | • Use pre-numbered and multipart requisitions and purchase orders.    |
|                                                  | • Use a capital budget and follow-up on projects with excessive costs. |
| Manipulating records to conceal other fraud      | • Review additions to and deletions from the fixed assets account.     |

2. Stealing fixed assets. Thefts of fixed assets occur in the same ways other assets are stolen. Assets can be stolen directly, or they can be inappropriately scrapped and sold for salvage, with the perpetrator keeping the proceeds. Rarely are complete physical counts of fixed assets performed. Assets that have been fully depreciated but still have economic value to the company may be (improperly) eliminated from the records and then stolen.

3. Laptop and notebook computer theft has become popular. Computer theft is a particular concern because the organisation loses both the fixed asset and valuable and/or sensitive data, which can be proprietary and highly confidential.

4. Personal use of assets. While personal use of copying machines, postage meters, computers, and other assets is generally tolerated by management, there have been cases where fixed assets were used to generate cash flows for the perpetrator. An employee may use fixed assets after hours or on weekends to produce a product or provide a service. Since the perpetrator does not have to buy fixed assets, his or her profit margins can be extremely high. Depending on the asset, this additional use may result in extra maintenance costs or earlier scrapping of an asset.

5. Personal capital improvements. Perpetrators may be able to divert capital improvement funds for their personal benefit. For example, the perpetrator may use company funds to pay for improvements to a personal residence and charge the cost to a new capital investment (such as large machinery or new facilities). Alternatively, the employee may order supplies for personal use. They may be delivered to the employee’s home or taken from the office after hours.

6. Manipulating records to conceal other frauds. The focus on the physical security of fixed assets can keep organisations from noticing the fixed asset account has been adjusted to hide thefts. For example, fixed asset and inventory accounts may be debited to hide cash thefts.

B. Preventive and detective fixed asset controls

1. Many of the preventive and detective controls regarding fixed assets centre on physical controls, separation of duties and monitoring. The following paragraphs discuss specific controls that may be implemented to reduce fixed asset fraud.
   a. Surveillance. Surveillance can be an effective method for preventing and detecting theft of fixed assets. The procedure is similar to that employed for inventory surveillance.
   b. Physical count. A complete physical count of fixed assets may be performed to determine if any are missing. Generally, a physical count will be necessary when the fraud is pervasive and a physical count is the only way to determine the extent of the problem. It may also be necessary to count fixed assets held at third-party locations. If a physical count of fixed assets is necessary, the procedures are similar to those used for inventories.
c. Review fully depreciated assets. If a complete physical count is not practical, the organisation may inspect all fully depreciated assets, whether or not currently recorded in the organisation’s books. An appropriate level of management may interview operations personnel to determine the physical handling and security of fully depreciated assets and to inquire about any unusual activity, including theft or personal use of the assets.

d. Analyse salvage and scrap sales. Analysis of salvage and scrap sales should include both a review of the accounting records and discussion with appropriate employees.

e. Review general journal entries. Many frauds necessitate changing amounts that would otherwise appear in the financial statements, and this can often only be effected via the booking of fraudulent journal entries, most typically in the general journal. Journal entry review should cover all accounts related to fixed assets, including revenue for scrap or asset sales and accumulated depreciation accounts. The following procedures should be considered for retirements, adjustments, sales, disposals, and similar entries:
   i) Vouch proceeds from sales of property to remittance advices or notes receivable.
   ii) Trace the original cost and acquisition date of the asset to prior period property records.
   iii) Re-compute depreciation through the date of sale.
   iv) Re-compute the gain or loss and trace it to the revenue/expense accounts.
   v) Determine whether each disposition was properly authorised and did not include assets pledged on existing debt.
   vi) Consider matching sales with reorders of replacement equipment.

f. Review reconciliations between fixed asset ledger and general ledger. Ideally, the totals in the fixed asset ledger should agree to the general ledger control accounts. If the totals do not agree, the organisation should consider reviewing the reconciliation of the fixed asset ledger to the general ledger. Each reconciling item should be investigated and traced to supporting documents.

g. Review capital expenditures. Consider analysing capital expenditures by location, department, employee, etc. for unusual patterns. If diversion of capital funds is suspected, examine documentation supporting capital expenditures, especially major construction projects. Pay special attention to the delivery addresses of materials and supplies used. Consider physically inspecting the improvements.

VII. PAYABLES AND DISBURSEMENTS FRAUD SCHEMES

A. Payables and disbursements fraud involves manipulating accounts payable or cash disbursements to steal cash, other assets, services, or other benefits. Some of these fraud schemes are easier to detect than others because there is a paper trail.

B. Kickback schemes can be difficult to detect because the paper trail is often outside the organisation’s normal accounting system. In fact, the only paper trail that may provide sufficient evidence for a civil or criminal action may be in the custody of the employee and the vendors or other parties involved.

C. Types of payables and disbursements fraud
   1. Payables and disbursements fraud may involve anything from kickbacks to outright theft.
   2. Generally, these schemes fall into the following categories:
      a. Kickbacks
      b. False or inflated vendor invoices
      c. Excess purchasing schemes
d. Duplicate payment schemes  
e. Employees writing cheques to themselves  
f. Stealing cheques  
g. Wire transfer schemes

3. Depending on the scheme, the perpetrator may be an employee, a vendor, or both acting in collusion. The table beginning below sets forth the common payables schemes and related controls. There are discussed further following the table.

<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
</table>
| Kickbacks                         | • Separate the purchasing from requisitioning, shipping, and receiving.  
|                                   | • Rotate purchasing agents.  
|                                   | • Use competitive bidding. All bids should be date stamped when received and two employees should open them at the same time.  
|                                   | • Review recent purchases to see whether the same vendor is winning all the bids led by a specific purchasing agent or for a specific commodity.  
|                                   | • Examine contracts with the same vendor for similar items. If there are similar items in two separate contracts, determine that performance has occurred under both contracts.  
|                                   | • Notify vendors that you are using a fraud hotline.  
|                                   | • Include a right-of-audit and access to books clause in contracts.  
|                                   | • Periodically have someone outside the purchasing department review purchase prices.  
|                                   | • Enforce mandatory vacations for employees in purchasing, accounts payable processing, disbursement, and related recordkeeping functions. The vacations should be at least two weeks long and occur at the end of an accounting cycle. Cross train employees so that someone else does the job during the vacation.  
|                                   | • Use pre-numbered purchase orders and receiving reports, and periodically verify that their sequence is accounted for.  
|                                   | • Require independent documentation of the receipt of acceptable goods or services before payment is made. In the case of professional services or construction, this verification should be made by individuals with the skills necessary to judge satisfactory conformity with the contract.  
|                                   | • Have personnel receiving purchased goods compare the quantities, brands, and product identification of goods received to the shipper’s bill of lading. |
| False or inflated vendor invoices and altering cheques | In general:  
|                                                   | • Separate invoice processing and accounts payable from the general ledger function.  
|                                                   | • Separate the requisitioning, purchasing, and receiving functions from the invoice processing, accounts payable, cash receipts, cash disbursements, and general ledger functions.  
|                                                   | • Use physical or software controls to prevent unauthorised access to the cheque writing and accounts payable systems.  
|                                                   | • Use an approved vendor list and make sure management approves all changes to the vendor master file.  
|                                                   | • Separate vendor processing, accounts payable, and cheque processing functions.  
|                                                   | • Reconcile the cash disbursement records to the accounts payable open invoice file.  
|                                                   | • Reconcile the accounts payable trial balance to the control account. Have the owner/manager or other appropriate person review the reconciliation.  
<p>|                                                   | • Have the owner/manager or another appropriate person review the actual cash disbursements versus expected, or budgeted amounts. |</p>
<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
</table>
| **False or inflated vendor invoices and altering cheques (cont’d)** | **Disbursements:**  
- All disbursements (except for petty cash) should be made via cheque or wire.  
- Use pre-numbered, multi-part cheques and pre-numbered debit/credit memos. Keep one copy in numerical sequence. Frequently check for missing or out-of-sequence cheque numbers.  
- Severely restrict the use of manual cheques.  
- Never sign blank cheques.  
- Lock up unused cheques.  
- Lock up signature stamps or plates (or password-protect electronic signature functions).  
- When cheques are voided, they should be defaced and kept in an appropriate location for inspection.  
- Prohibit cheques written to “cash” or “bearer.” (Some companies make an exception for petty cash reimbursements.)  
- Investigate, void, and reissue cheques outstanding more than 90 days, if necessary.  
- Require two signatures for cheques above a specified dollar amount. (Cheques should not be countersigned in advance and left for the other signor.)  
- Limit authorised signors to corporate officers or employees who are independent of the initiator of purchases, approver of purchases, receiving, shipping, preparer of cheques, cash receipts, accounts payable, and cash bookkeeping.  
- Check the mathematical accuracy of vendor invoices.  
- Compare vendor invoices to purchase orders and receiving reports.  
- Attach vouchers or vendor invoices, purchase orders, and receiving documents to cheque requests. Agree quantities, brands, and product descriptions. Make sure they are all stamped “paid” and are marked with the cheque number.  
- Consider the use of electronic data interchange with certain vendors.  
- Do not return the signed cheques to the employee who drew them or the accounts payable clerk. Have someone independent of these functions mail them.  
- Limit authorised signors to corporate officers or employees who are independent of the initiator of purchases, approver of purchases, receiving, shipping, preparer of cheques, cash receipts, accounts payable, and cash bookkeeping.  
- Check the mathematical accuracy of vendor invoices.  
- Compare vendor invoices to purchase orders and receiving reports.  
- Attach vouchers or vendor invoices, purchase orders, and receiving documents to cheque requests. Agree quantities, brands, and product descriptions. Make sure they are all stamped “paid” and are marked with the cheque number.  
- Consider the use of electronic data interchange with certain vendors.  
- Do not return the signed cheques to the employee who drew them or the accounts payable clerk. Have someone independent of these functions mail them.  
- Utilize “positive-pay” services offered by the organisation's bank. (Positive-pay is a service where the disbursing bank matches cheque numbers and dollar amounts of cheques submitted for payment against a listing provided by the organisation of cheques authorised for payment. Cheques that do not match or are not on the list are not paid.)  
- Enforce mandatory vacations for employees in purchasing, accounts payable processing, disbursement, and related recordkeeping functions. The vacations should be at least two weeks long and occur at the end of an accounting cycle. Cross train employees so that someone else does the job during the vacation. |
<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>False or inflated vendor invoices and altering cheques (cont’d)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Bank reconciliations:</strong></td>
<td>Arranged for bank statements to be sent directly to the owner/manager or someone who does not have responsibility for the cash receipts and disbursement records.</td>
</tr>
<tr>
<td></td>
<td>Have the bank account reconciled each month by someone who does not prepare or sign cheques. Have the owner/manager or another appropriate person review the bank reconciliation.</td>
</tr>
<tr>
<td></td>
<td>Separate responsibility for cash receipts, accounts receivable, and accounts payable from responsibility for reconciling the bank statement.</td>
</tr>
<tr>
<td><strong>Purchasing:</strong></td>
<td>Separate authority to contract for an item and authority to approve the invoice.</td>
</tr>
<tr>
<td></td>
<td>Use pre-numbered purchase requisitions, purchase orders, and receiving reports.</td>
</tr>
<tr>
<td></td>
<td>Have personnel receiving purchased goods compare the quantities, brands, and product identification of goods received to the shipper’s bill of lading.</td>
</tr>
<tr>
<td><strong>Excess purchasing schemes</strong></td>
<td>Rotate purchasing agents.</td>
</tr>
<tr>
<td></td>
<td>Enforce mandatory vacations for employees in purchasing, accounts payable processing, disbursement, and related recordkeeping functions. The vacations should be at least two weeks long and occur at the end of an accounting cycle. Cross train employees so that someone else does the job during the vacation.</td>
</tr>
<tr>
<td></td>
<td>Use competitive bidding for purchases. Review recent purchases to see whether the same company is winning all the bids.</td>
</tr>
<tr>
<td></td>
<td>Have personnel receiving purchased goods compare the quantities, brands, and product identification of goods received to the shipper’s bill of lading.</td>
</tr>
<tr>
<td></td>
<td>Notify vendors that you are using a fraud hotline.</td>
</tr>
<tr>
<td></td>
<td>Use monthly budgets. Compare the actual expense with budgets and follow-up on differences.</td>
</tr>
<tr>
<td></td>
<td>Require that personnel approving or processing vendor invoices for payment be alert for excessive quantities of supplies (such as copy machine paper or paper towels) and lower quality goods than traditionally used.</td>
</tr>
<tr>
<td><strong>Duplicate payment schemes</strong></td>
<td>Require that payments to all employees (even those to managers) be authorised.</td>
</tr>
<tr>
<td></td>
<td>Require original invoices and receiving reports. As invoices are processed for payment, mitigate the possibility of additional submission by stamping the invoice “paid” or “processed.”</td>
</tr>
<tr>
<td></td>
<td>Compare the petty cash reimbursements to the regular reimbursement process to ensure employees are not asking for reimbursement from both.</td>
</tr>
<tr>
<td></td>
<td>Flag duplicate invoice numbers submitted for vendor payment. (Many payable systems have control features that identify potential duplicate payments based on previously processed invoice numbers for that vendor.)</td>
</tr>
</tbody>
</table>
### Common Payables and Disbursement Fraud Schemes and Related Controls

<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
</table>
| Stealing cheques             | • Separate responsibility for cash receipts, accounts receivable, and accounts payable from responsibility for reconciling the bank statement.  
|                              | • Lock up unused cheques.  
|                              | • Utilise “positive-pay” services offered by the organisation’s bank. (Positive-pay is a service where the disbursing bank matches cheque numbers and dollar amounts of cheques submitted for payment against a listing provided by the organisation of cheques authorised for payment. Cheques that do not match or are not on the list are not paid.) |
| Stealing cash by using a wire transfer | • Use passwords for individuals authorised to make transfers.  
|                              | • Require bank callback verifications for telephone transfers exceeding a predetermined dollar amount. (Have the owner or manager review transfer activity on the bank statement. Look for transfers just under this dollar limit.)  
|                              | • Ensure that wire transfers are subject to the controls over other disbursements (such as requiring original invoices).  
|                              | • Bond the employees responsible for purchasing, accounts payable processing, cash disbursements, and wire transfer functions. |

4. **Kickbacks.** In a kickback scheme, an employee with authority to purchase materials, supplies, or services receives a benefit from a vendor in return for funnelling business to that vendor. The benefit to the employee can take many forms, including cash, travel, payments to third parties for the employee’s benefit, hiring relatives, vacations, clothes, sexual favours, or entertainment. The employee then agrees to:
   a. Purchase excess or inferior goods or services from the vendor,
   b. Pay for goods or services not received, or
   c. Pay a premium price for the goods or services received.

5. The organisation may also suffer in less tangible ways.
   a. For example, the organisation may receive shoddy service, products, or workmanship that can result in additional costs later.
   b. Also, the organisation can lose its good reputation or goodwill in the business community because vendors may learn that employees are taking kickbacks and refrain from bidding or providing other services later.

6. **Kickback schemes may be difficult to detect and prove, especially through conventional internal controls and audit procedures.** Many factors create difficulties in detecting kickbacks.
   a. For example, employees involved in kickback schemes are generally in positions to hide the fraud. Many perpetrators are sophisticated employees who know the organisation’s controls.
   b. They know how to circumvent the controls (for example, by authorising payment or receipt) or what information to include in supporting documents to ensure that the accounts payable system will process the payment routinely.

7. Likewise, analytical procedures may not be effective in detecting kickback schemes.
   a. Most of these schemes start small and may increase at a rate commensurate with the growth of the business. Consequently, analytical and other procedures may not detect the fraud because the fraudulent amounts are “built in” to the historical base.
b. One technique that can be effective is using database software or data extraction software to create a list of the largest vendors in descending order. This list can be exported to a computer spreadsheet and additional procedures can be performed. For example, if the file includes current and prior-year balances, a computer spreadsheet can calculate a dollar and percentage change. This will highlight new vendor relationships.

8. False or inflated vendor invoices. False or inflated invoice schemes may arise from any of the following scenarios:
   a. Employees submit false invoices to perpetrate a theft
   b. Vendors may submit false or inflated invoices without collusion
   c. Employees may collude with vendors to accept false or inflated invoices in return for kickbacks

9. Phantom vendor schemes generally require the following steps: an employee with access to the accounts payable system (either as a clerk, the controller, or CFO) creates fictitious vendors and puts them on the list of approved vendors.
   a. The employee creates, and possibly approves, invoices for nonexistent purchases. Cheques are issued and mailed to the address noted on the invoice. (This address will frequently be the employee's home address, a P.O. box, or a mail drop box opened for this purpose by the perpetrator.
   b. Alternatively, the perpetrator may go directly to the accounts payable department and pick up the remittance to hand deliver it to the “vendor.”) Perpetrators retrieve the cheques and deposit them into one of their accounts.

10. False invoice schemes occur when perpetrators use the names of actual vendors but create alternate addresses for them. They then create false invoices by copying legitimate vendor invoices.
    a. Vendors sometimes perpetrate fraud by carrying out product substitutions, billing for work not performed or services not provided, padding overhead charges, or under-shipping items.

11. Altering cheques. Dishonest employees may steal a cheque written to a legitimate vendor and deposit in his or her account. Sometimes, the perpetrator creates elaborate schemes to generate the cheques, and other times the scheme may be flagrant and obvious. Altering or destroying the cancelled cheques may conceal the fraud.

12. Excess purchasing schemes. There are several ways a creative purchasing agent can steal by purchasing more goods or services than an organisation needs. For example, purchasing agents may do one of the following:
    a. Purchase goods or services in excess of the organisation's needs, then convert the excess for their own benefit.
    b. Obtain a bonus by reducing the cost per item of a material or product by buying in bulk but in excess of the company's needs.
    c. Purchase excess goods or services and take a kickback from the vendor.
    d. Often, these schemes are known to exist by co-workers who observe the conversion to personal use, are responsible for costing or other controls, or who must find a place to store the excess. If the organisation has an ethics policy and an ethics hot line, these co-workers may report these schemes.
13. Duplicate payment schemes. In this scheme, the perpetrator manipulates the system to produce a second payment on a vendor invoice, which he or she then alters and cashes. In a variation of this scheme, the perpetrator writes a manual cheque to himself/herself for the same amount as a legitimate payment generated through the accounts payable system. The perpetrator cashes or deposits the manual cheque and, when the cancelled cheque is returned, he or she alters the payee on the cheque so it appears to be written to the vendor.

14. Stealing cheques. Sometimes, perpetrators steal an organisation’s cheques, forge an authorised signature, and cash or deposit the cheques in their accounts. Organisations are most vulnerable to this type of fraud when they have poor safeguards over unused cheques or lack of separation of duties (especially when employees with access to unused cheques also prepare bank reconciliations). Organisations should consider whether they have other negotiable instruments (for example, blank airline tickets or travellers cheques) and ensure they are kept in a safe.

15. The theft of completed cheques has become a favourite target of many gangs. With sophisticated computer equipment, they can easily duplicate the facsimile signature and all other pertinent information on a cheque. The cheques are then cashed in large quantities, leaving the organisation with a large loss from a single theft. Some large retailers have reported massive thefts relating to reimbursement-type cheques. The perpetrators may be employees or third parties.

16. Stealing cash using a wire transfer. Companies use wire transfers for a variety of purposes such as to pay vendors or fund pension plans, payroll accounts, and subsidiary or other bank accounts. Wire transfers can be used to commit fraud just like cheques or other forms of disbursement. For example, an employee may forge a signature of an authorising employee and wire the funds to a personal or phony business account.

D. Preventive and detective payables and disbursement controls

1. Review the vendor lists. The owner/manager should review vendor lists for any unusual patterns, such as names that may be similar, but not identical to the names of approved vendors and vendors that have multiple addresses. In addition, the owner/manager periodically should inspect files of unpaid invoices and vendor statements to look for items such as the following:
   a. Invoices that appear different from the norm.
   b. Non-consecutive vendor invoice numbers.
   c. Customized rather than pre-printed forms.
   d. Different delivery addresses and/or telephone numbers.
   e. Changes in purchase order numbers, item descriptions, prices, or other unusual patterns.
   f. Old or unusual vendors who recently had an address change.
   g. Current activity on an old or outdated vendor.

2. Vendor lists should be periodically reviewed to determine the date of last activity. The organisation should consider inactivating those vendors without a recent history of purchases.

3. Use a Positive-pay or a Reverse Positive-pay System. With a positive-pay system, the company sends the bank a list of authorised disbursements, and the bank pays only items on the list. With reverse positive-pay, the bank sends the company a list of cheques presented for payment, and the company notifies the bank within a short time period of any unauthorised disbursements. Both of these systems can be costly but can be highly effective in preventing unauthorised disbursements.

4. Review the general journal entries. Journal entries should be reviewed for any unusual patterns or timing anomalies.
5. Verify vendors. If the validity of a vendor is questioned (for example, in a false invoice scheme), an appropriate person should take steps to verify the vendor’s existence. Perhaps the most effective way to verify a vendor is to call the vendor and visit the vendor’s facilities. Alternatively, an appropriate person can consult other information sources, such as the Better Business Bureau, credit reporting companies (such as Dun & Bradstreet), telephone directories, secretary of state incorporation records, or local partnership and assumed name records.

6. Call vendors which did not win the contract. Some organisations have an employee independent of the purchasing function call vendors after a bid is awarded to inquire as to whether the process was perceived as fair.

VIII. EQUITY FRAUD SCHEMES

A. Equity embezzlement schemes generally involve manipulating equity transactions to steal cash. Examples of equity embezzlement schemes include:

1. Diverting equity proceeds for personal use
2. Underpaying dividends to certain investors and diverting the difference for personal use
3. Selling shares of stock more than once.

B. The following table and discussion summarizes common fraud schemes and related controls.

<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
</table>
| Diverting equity proceeds for personal use | • Separate responsibility for approving transactions from issuing stock certificates and maintaining stockholder records.  
• Monitor and periodically reconcile the stock records to the general ledger and have the owner/manager or other appropriate person review the reconciliation. |
| Underpaying dividends and diverting the difference | • The board of directors should approve all dividends.  
• Review the dividend cheques based on information in the stock register and the dividend rate.  
• Announce dividend rates to the shareholders before the cheques are issued. |
| Selling shares of stock more than once     | • The corporate charter should authorise all shares sold and the board of directors should authorise all stock sales.  
• Use pre-numbered stock certificates, issue them sequentially, and review their sequence periodically.  
• Unissued shares of stock should be safeguarded by someone not in charge of cash handling or accounting.  
• In a closely held business, investigate any reports of bogus shares or ownership by individuals not known. |

1. Diverting equity proceeds. This scheme involves stealing some of the proceeds from sales of stock (or other equity interests).

2. Underpaying dividends. In this scheme, the perpetrator underpays the dividends due to stockholders and steals the difference. The dividend total is correct, but the individual stockholders are victimized.

3. Selling shares of stock more than once. With this scheme, the perpetrator sells shares of stock more than once and steals the proceeds. Perpetrators may use stolen certificates or duplicate or forged shares.
IX. MISCELLANEOUS FRAUD SCHEMES

A. Borrowing schemes

1. Borrowing fraud is generally committed to steal cash. The following embezzlement schemes involve borrowings:
   a. Unauthorised borrowing, and
   b. Diverting loan proceeds for personal use.

2. These fraud schemes are set forth in the following table, along with symptoms and related controls.

<table>
<thead>
<tr>
<th>Fraud Scheme</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorised borrowing</td>
<td>• The board of directors should approve all debt or other liability transactions.</td>
</tr>
<tr>
<td></td>
<td>• Separate the authority to borrow from the cash handling and accounting functions.</td>
</tr>
<tr>
<td></td>
<td>• Separate responsibility for the debt accounting records from the invoice processing, cash receipts, and cash disbursement functions.</td>
</tr>
<tr>
<td></td>
<td>• Maintain and reconcile detail subsidiary ledgers to the general ledger.</td>
</tr>
<tr>
<td></td>
<td>• Have the owner/manager or other appropriate person periodically review accrued liabilities for reasonableness.</td>
</tr>
<tr>
<td></td>
<td>• Have the owner/manager or other appropriate person review interest expense calculations periodically.</td>
</tr>
<tr>
<td></td>
<td>• Periodically obtain copies of the entity’s credit report and a list of UCC filings.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Diverting bond or loan proceeds</th>
<th>Preventive or Detective Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The board of directors should approve all debt or other liability transactions.</td>
</tr>
<tr>
<td></td>
<td>• Separate the authority to borrow from the cash handling and accounting functions.</td>
</tr>
<tr>
<td></td>
<td>• Separate responsibility for debt accounting records from the invoice processing, cash receipts, and cash disbursement functions.</td>
</tr>
<tr>
<td></td>
<td>• Have the owner/manager or other appropriate person periodically review accrued liabilities for reasonableness.</td>
</tr>
<tr>
<td></td>
<td>• Have the owner/manager or other appropriate person review interest expense calculations periodically.</td>
</tr>
</tbody>
</table>

a. Unauthorised borrowing.
   i) The perpetrator may borrow money without company authorisation and steal the proceeds.
   ii) Alternatively, perpetrators sometimes pledge the organisation’s assets for personal loans. This occurs most often with investments, accounts receivable, or other assets that are not otherwise pledged.
   iii) If the interest expense for the period is higher than expected, this could be a sign of an unauthorised borrowing.

b. Diverting bond or loan proceeds.
   i) A perpetrator may steal some or all of the proceeds from a bond issuance or a loan.
   ii) If the board has approved the borrowing, there should be an expectation as to how much will be received. The owner/manager should follow-up to make sure that amount was recorded. Thefts of this type have been in the news. Some SEC listed companies were borrowing money and “lending” it to executives who were large shareholders. These loans were never repaid or were forgiven. In effect, this transaction looted the company’s assets.
SOME OF THE BIG ONES: INFAMOUS ACCOUNTING FRAUDS

I. Adelphia Communications (2002)
   A. A cable television provider in semi-rural areas of Pennsylvania and adjacent states, aggressive growth fuelled by stock price rise, which in turn depended on good, growing record of earnings.
   B. Unfortunately, accounting fraud had resulted in some $2.3 billion in debt being concealed, vastly altering the company’s actual record of performance and risk (debt/equity ratio). The controlling owners of this publicly-traded company were accused of stripping out $100 million for themselves, also.
   C. The principals (family members) were criminally indicted, some were convicted of fraud and sentenced to jail terms; the company filed for bankruptcy and assets were later sold.
   D. The auditors failed to observe the various fraudulent practices, involving, e.g., undisclosed related party transactions, including $2.3 billion in loans to controlling family. The auditors also did work for the family, making it even less comprehensible that these transactions and obligations were not understood.

II. Parmalat
   A. Perhaps the biggest accounting fraud ever, this involved the concealment, over many years, of some $18 billion in debt and losses.
   B. One of the few instances of actual auditor complicity, the auditors, when superseded by mandatory rotation rules in Italy, were appointed as continuing auditors for the subsidiaries where the fraud was thereafter concentrated, and supervision by the new group auditors was inadequate to find these ongoing fraudulent acts.
   C. There were multiple “red flags” missed (or deliberately ignored), including improbably large cash balances putatively held by branch banks in Caribbean island nations (fraudulently confirmed), and outrageously improbable huge purchases of dairy products in Singapore (a city-nation lacking substantial farmlands) then ostensibly resold to the Cuban state-run food agency in quantities that would have literally drowned the island in milk, were it true.

III. Enron (late 1990s–2001)
   A. One of the most infamous cases, which (together with WorldCom) spurred development of the Sarbanes-Oxley Act in the U.S., stripping the accounting profession (as regards audits of publicly-held entities) of its self-regulatory role.
   B. Made extensive use of the so-called “special purpose entities” (now known as “variable interest entities”) to move large amounts of debt off its balance sheet, improperly, and to create bogus transactions with these captive related entities that provided large portions of the profits being reported over a stretch of years.
   C. The SPEs (VIEs) were structured with the assistance of outside counsel Vinson & Elkins and auditors Arthur Andersen (the former escaped unscathed from the Enron collapse; the latter was indicted and collapsed, although later partially vindicated), which attempted to use narrow exceptions to the rules to create ostensibly independent entities (thus justifying profit recognition from transactions with them), although in truth these were thinly-capitalized shells (some “owned” by minor Enron employees, fully funded indirectly by Enron itself). Hundreds of these so-called “partnerships” were created and used for one-off transactions, to either create imaginary profits or to off-load debt from the Enron balance sheet (or both).
   D. Enron grew rapidly, using over-valued stock to make acquisitions, and was the 7th largest company on the Fortune 500 list right before its collapse.
   E. Changes to accounting rules pertaining to VIEs were largely stimulated by the Enron fraud.
IV. WorldCom (late 1990s–2002)

A. Another company that grew by aggressive acquisitions fuelled by high stock valuation, which in turn was the result of growing large reported earnings.

B. The company’s actual performance was vastly less impressive; over a period of less than a decade, over $11 billion of imaginary profits had been reported. When the truth emerged, the company collapsed and multiple parties were criminally prosecuted.

C. The financial reporting fraud sequentially involved three bogus practices.
   1. Expenses that should have been recognised currently were instead charged (debited) against accruals already on the books for other reasons. This practice depleted these other liability balances, which would have meant that payment of those obligations in later periods would have created losses.
   2. Once the available reserves had been eliminated as a means of concealing current expenses, the fraud orchestrators began a procedure of capitalizing certain operating costs (line connection fees paid to telephone carriers controlling the “last mile” to subscribers’ homes) that were in truth current period sunk costs but were handled, fraudulently, as long-lived fixed assets to be amortized over extended periods.
   3. In desperation, after the other fraudulent practices had been exploited to the maximum, WorldCom began to accrue subscriber cancellation penalties that, although provided for in the contracts with consumers, had never previously been enforced. This created revenues that in fact never came to fruition.

D. The auditors (Arthur Andersen), although not shown to be complicit, were grossly negligent in applying auditing procedures and apparently missed finding any of the three large ($3 – 4 billion each) multi-year frauds being perpetrated by the CEO and the CFO, both of whom were later prosecuted and sent to prison.

V. Lehman Brothers (2008)

A. Used the commonly employed financing device known as “repurchase agreements” (“repos”) to periodically borrow funds, collateralizing the loans with marketable securities owned.
   1. Under U.S. GAAP, repos are secured borrowings, not sales (nor later repurchases) of the securities being used as collateral.
   2. Proper accounting would have shown the repo borrowings as additional debt (and the cash borrowed as additional assets, of course), leaving in place the other assets and liabilities not altered by the repo-based borrowings.

B. Instead, Lehman contrived a technique (“Repo 105” and “Repo 108,” so named because the repurchase agreements were over-collateralized by 5% [for debt collateral] or 8% [for equity collateral]) that is successfully sold to its auditors as being tantamount to actual sales, since the over-collateralized counter-party would presumably not object to a default (i.e., failure to exercise the repurchase commitment), since it could well prove profitable to the lender.
   1. This was coupled with using the proceeds from the borrowings (improperly accounted for as proceeds from sales of securities) to pay down unrelated debts.
   2. The net result of this series of actions and accounting treatments was to materially distort Lehman’s debt/equity ratios.
   3. This pattern was repeated around each (quarterly) reporting date over several years, thus distorting the key debt/equity ratio statistic multiple times, suggesting the company was less risky than its true debt positions warranted.
C. However, this violated GAAP (and common sense), since the netted items were obligations with unrelated counter-parties, and because defaulting on the “Repo 105s” and “Repo 108s” was never intended nor contractually agreed to. Lehman was considerably more highly-leveraged than its fraudulent financial statements suggested.

D. At its peak, this scheme resulted in concealing $50 billion in debt obligations that were actually owed by Lehman.

E. When Lehman’s actual financial position was revealed (in conjunction with the credit crisis in 2008), the company collapsed. The auditors have been sued, but matters are still unresolved.

F. A later fraud, involving MF Global, a financial firm headed by a former U.S. senator and governor, used a variant on the “Repo 105” theme: the so-called “repos-to-maturity.” These violated GAAP for the same reason that Lehman’s repurchase agreements did: they treated certain secured borrowings as actual sales, thus netting down the balance sheet, distorting key ratios and trends, and concealing real obligations to make payments to counter-parties in the future.


A. This company had several accounting scandals, but the key one involved recognition of unearned advertising revenues amounting to over $1 billion.

B. The scheme involved paying advertisers to buy advertising that was unwanted. Since the key metric being evaluated by investors was the amount of sold advertising (not the profitability of the advertising, for example), this pumped up the metric even if it didn’t distort net income overall (although it did result in crediting the wrong periods).

VII. Xerox (late 1990s – early 2000s)

A. Long-established, highly-respected company faced with slumping earnings found a way to use creative lessor accounting to boost reported earnings.

B. The company engaged in copier and related leasing, offering packages of machine time, supplies, services, and other features. Under U.S. GAAP, front-end profit recognition was permitted for manufacturers (or dealers) who leased products, as long as profit related to portion of net future rental streams that pertained to the machinery itself, excluding executory fees for services and supplies.

C. Xerox manipulated the portion of the net present value of future rental streams so as to exaggerate the portion attributable to the machine usage, thus justifying booking excessive front-end manufacturer/dealer profit.

D. When this was uncovered, restatements of several years’ financial statements were required in order to eliminate $3 billion in revenues and $1.4 billion in profits, and fines and penalties were levied against the company and its auditors.

VIII. Global Crossing (2002)

A. One of a number of telecommunications companies that emerged in the early days of fibre optic technology, it intended to build (and did build) a large network of cable, far more than it had demand for in the near term.
B. Employed a bogus theory of accounting (which had been developed for the telecommunications industry by former Big Five firm Arthur Andersen), referred to as indefeasible rights to use, to create instant revenue coupled with deferred costs to be amortized over extended periods, all from “swaps” of excess capacity (“dark cable”) with other similarly-positioned cable network developers.

C. The “indefeasible rights to use” debacle was one of the events that motivated the large scale IASB-FASB project to re-write revenue recognition standard (just finalized in Spring 2014).

IX. Phar-Mor (1992)
A. Chain of discount drug and general merchandise stores in the U.S., reporting rapid growth and profitability.
B. Concealed $300 million in losses by creating bogus inventory, spread across many of the chain’s 300+ stores.
C. Was able to conceal this only because the auditors informed management of which locations would be sample-tested by inventory observation audit teams each year, and thus corrupt management could arrange book transfers of bogus inventory to those locations that were not to be observed.
D. The book entries showing purported inventory transfers across stores were “red flags” that were ignored by auditors, even as they appeared implausible.
E. Key lesson is that the element of surprise should never be surrendered by auditors, particularly when client entity is geographically dispersed and thus only to be subjected to small sample testing.
About ISCA Technical Standards Development and Advisory

The Technical Standards Development and Advisory (TSDA) team is part of the Technical Knowledge Centre and Quality Assurance division of the Institute of Singapore Chartered Accountants (ISCA). It is committed to supporting the Institute in advancing and promoting technical developments within the profession as part of the effort to transform Singapore into a leading global accountancy hub by 2020.

ISCA TSDA engages external stakeholders in soliciting meaningful feedback on accounting and auditing related issues to develop a consistent approach to addressing industry issues identified. It also prescribes auditing and assurance standards that are closely aligned to international best practices, champions thought leadership initiatives with key stakeholders and drives projects in collaboration with various ISCA technical committees.

It actively engages international standard setters and strives to be an advocate of matters pertinent to the development of Singapore’s accountancy profession. Furthermore, it aims to cultivate a mindset change and raises awareness of new and revised standards through the publication of articles authored by the team.

Additionally, ISCA TSDA seeks to empower members and the profession at large to achieve their aspirations by equipping them with relevant technical expertise and this is achieved through the development of a range of resources that they can tap on.

Knowledge sharing with accounting community is facilitated through a variety of print and online channels including the sharing of regular updates and thought leadership articles via in-house publications like the journal, “IS Chartered Accountant”, the E-newsletter, “ISCA Weekly”, and various online knowledge centres and a technical forum. Seminars and workshops are regularly organised and ISCA TSDA also provides value-added technical clarification services to assist the profession in resolving accounting, auditing and ethics related issues.

© 2014 by Dr Barry Epstein

Disclaimer

This document contains general information only and the author and ISCA are not, by means of this document, rendering any professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a professional advisor. Whilst every care has been taken in compiling this document, the author and ISCA make no representations or warranty (expressed or implied) about the accuracy, suitability, reliability or completeness of the information for any purpose. The author, ISCA, its employees or agents accept no liability to any party for any loss, damage or costs howsoever arising, whether directly or indirectly from any action or decision taken (or not taken) as a result of any person relying on or otherwise using this document or arising from any omission from it.