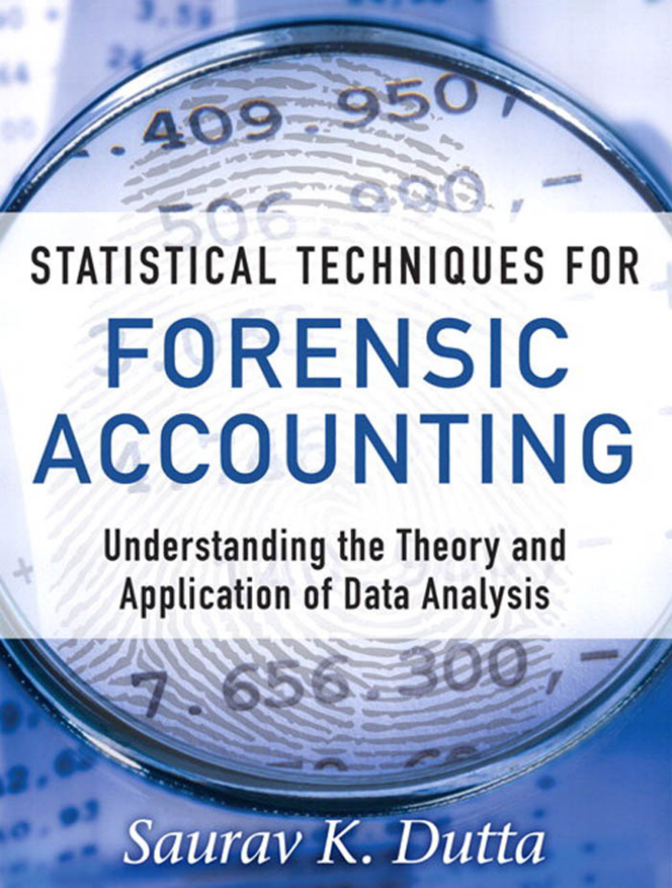

STATISTICAL TECHNIQUES FOR FORENSIC ACCOUNTING

Understanding the Theory and Application of Data Analysis

Saurav K. Dutta

Praise for *Statistical Techniques for Forensic Accounting*

"Financial statement fraud has never been a more serious threat to the integrity of our capital markets than it is today. Professor Dutta discusses the auditing and statistical tools available to detect and investigate financial fraud, set against a colorful backdrop of fraudsters, whistleblowers, and corporate scams that proves fact is stranger than fiction."

—**Dennis Caplan**, University at Albany, New York

"Quantified evidence is often most persuasive and is often required to propose adjustments or prove damages. All parties (management, auditors, regulators, litigants) are best served by applying defensible, well-thought-out techniques when estimating proportions or amounts. Professor Dutta's book uniquely addresses a variety of techniques that could be or are currently applied in supporting arguments and determining amounts. A number of these are illustrated with audit application examples."

—**Lynford Graham**, CPA, PhD, CFE, Bentley University, Massachusetts

"Financial crime causes severe damages to capital markets. It not only affects investors who were deceived, but also reduces overall market return through dissipation of trust after fraud scandals. This causes a demand to detect and prevent financial crime in a timely manner. However, financial crime has been deliberately perpetrated by financial or accounting experts, which could not be detected by simple analytical techniques. Advance techniques such as sophisticated statistical methods are more useful in detecting financial fraud schemes. This book will benefit researchers who conduct research using these techniques to detect financial statement fraud. Other parties, such as auditors and regulators, could use them in developing financial statement fraud detection models."

—**Thawatchai Kiatkwankul**, Security and Exchange Commission, Thailand

"I am very pleased to see this book by Prof. Saurav Dutta. It provides a rich discussion on statistical concepts within the context of forensic accounting and fraud detection. It covers topics from why and how fraud is committed, to how one can detect it by using statistical techniques. He has used simple, familiar examples to illustrate the statistical concepts applicable to forensic accounting and fraud. I wish him great success."

—**Rajendra P. Srivastava**, Ernst and Young Professor, University of Kansas

“Professor Saurav has advanced the accounting profession by providing students of forensic accounting with a resource that combines a superb overview of accounting tools for fraud prevention with a careful introduction to the data-mining and statistical tools needed for fraud detection.”

—**Glenn Shafer**, Dean, Rutgers Business School, Rutgers University, New Jersey

“In a passage cited by Professor Dutta, Holmes comments to Watson that: ‘It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts.’ Professor Dutta’s treatise demonstrates not only the methods used to collect, assemble, and classify data, but, far more importantly, how to transform those data into evidence—in short, how to develop theories to suit the facts available. The essential step in this analysis is, of course, inferential statistics. This path leading from data to evidence is expertly navigated by Professor Dutta in terms that will prove understandable and useful to accountants, auditors, and legal professionals engaged in forensic accounting.”

—**Dave Marcinko**, Skidmore College, New York

STATISTICAL TECHNIQUES FOR FORENSIC ACCOUNTING

This page intentionally left blank

STATISTICAL TECHNIQUES FOR FORENSIC ACCOUNTING

UNDERSTANDING THE THEORY AND APPLICATION OF DATA ANALYSIS

Saurav K. Dutta

Vice President, Publisher: Tim Moore
Associate Publisher and Director of Marketing: Amy Neidlinger
Executive Editor: Jeanne Glasser
Operations Specialist: Jodi Kemper
Marketing Manager: Lisa Loftus
Cover Designer: Alan Clements
Managing Editor: Kristy Hart
Project Editor: Elaine Wiley
Copy Editor: Chrissy White
Proofreader: Debbie Williams
Indexer: Christine Karpeles
Compositor: Nonie Ratcliff
Manufacturing Buyer: Dan Uhrig

© 2013 by Saurav K. Dutta
Publishing as FT Press
Upper Saddle River, New Jersey 07458

This book is sold with the understanding that neither the author nor the publisher is engaged in rendering legal, accounting, or other professional services or advice by publishing this book. Each individual situation is unique. Thus, if legal or financial advice or other expert assistance is required in a specific situation, the services of a competent professional should be sought to ensure that the situation has been evaluated carefully and appropriately. The author and the publisher disclaim any liability, loss, or risk resulting directly or indirectly, from the use or application of any of the contents of this book.

FT Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact U.S. Corporate and Government Sales, 1-800-382-3419, corpsales@pearsontechgroup.com. For sales outside the U.S., please contact International Sales at international@pearsoned.com.

Company and product names mentioned herein are the trademarks or registered trademarks of their respective owners.

All rights reserved. No part of this book may be reproduced, in any form or by any means, without permission in writing from the publisher.

Printed in the United States of America

First Printing June 2013

ISBN-10: 0-13-313381-8
ISBN-13: 978-0-13-313381-3

Pearson Education LTD.
Pearson Education Australia PTY, Limited.
Pearson Education Singapore, Pte. Ltd.
Pearson Education Asia, Ltd.
Pearson Education Canada, Ltd.
Pearson Educación de Mexico, S.A. de C.V.
Pearson Education—Japan
Pearson Education Malaysia, Pte. Ltd.

Library of Congress Cataloging-in-Publication Data is on file.

To My Sons
Saahil and Samir
The Personification of my Aspirations

This page intentionally left blank

Table of Contents

Foreword xiii
Acknowledgments xv
Preface xviii

1 **Introduction: The Challenges in Forensic Accounting** 1
1.1 Introduction 1
1.2 Characteristics and Types of Fraud 3
1.3 Management Fraud Schemes 7
1.4 Employee Fraud Schemes 11
1.5 Cyber-crime 17
1.6 Chapter Summary 18
1.7 Endnotes 19

2 **Legislation, Regulation, and Guidance Impacting Forensic Accounting** 21
2.1 Introduction 21
2.2 U.S. Legislative Response to Fraudulent Financial Reporting 22
2.3 The Emphasis on Prosecution of Fraud at the Department of Justice 24
2.4 The Role of the FBI in Detecting Corporate Fraud 26
2.5 Professional Guidance in SAS 99 27
2.6 Chapter Summary 28
2.7 Endnotes 29

3 **Preventive Measures: Corporate Governance and Internal Controls** 31
3.1 Introduction 31
3.2 Corporate Governance Issues in Developed Economies 33
3.3 Emerging Economies and Their Unique Corporate Governance Issues 34
3.4 Organizational Controls 39
3.5 A System of Internal Controls 41
3.6 The COSO Framework on Internal Controls 46

3.7 Benefits, Costs, and Limitations of Internal Controls 52
3.8 Incorporation of Fraud Risk in the Design of Internal Controls 56
3.9 Legislation on Internal Controls 58
3.10 Chapter Summary 58
3.11 Endnotes 60

4 Detection of Fraud: Shared Responsibility 61
4.1 Introduction 61
4.2 Expectations Gap in the Accounting Profession 64
4.3 Responsibility of the External Auditor 66
4.4 Responsibility of the Board of Directors 68
4.5 Role of the Audit Committee 71
4.6 Management's Role and Responsibilities in the Financial Reporting Process 75
4.7 The Role of the Internal Auditor 78
4.8 Who Blows the Whistle 80
4.9 Chapter Summary 84
4.10 Endnotes 85

5 Data Mining 89
5.1 Introduction 89
5.2 Data Classification 91
5.3 Association Analysis 93
5.4 Cluster Analysis 95
5.5 Outlier Analysis 98
5.6 Data Mining to Detect Money Laundering 100
5.7 Chapter Summary 103
5.8 Endnotes 103

6 Transitioning to Evidence 105
6.1 Introduction 105
6.2 Probability Concepts and Terminology 106
6.3 Schematic Representation of Evidence 108
6.4 Information and Evidence 110
6.5 Mathematical Definitions of Prior, Conditional, and Posterior Probability 110

6.6 The Probative Value of Evidence. 114
6.7 Bayes' Rule 117
6.8 Chapter Summary. 122
6.9 Endnote. 123

7 Discrete Probability Distributions 125
7.1 Introduction. 125
7.2 Generic Definitions and Notations. 126
7.3 The Binomial Distribution. 127
7.4 Poisson Probability Distribution. 135
7.5 Hypergeometric Distribution 140
7.6 Chapter Summary. 145
7.7 Endnotes. 147

8 Continuous Probability Distributions. 149
8.1 Introduction. 149
8.2 Conceptual Development of Probability Framework. 150
8.3 Uniform Probability Distribution. 156
8.4 Normal Probability Distribution. 157
8.5 Testing for Normality 168
8.6 Chebycheff's Inequality 170
8.7 Binomial Distribution Expressed as a Normal Distribution. 171
8.8 The Exponential Distribution 172
8.9 Joint Distribution of Continuous Random Variables. 173
8.10 Chapter Summary. 176

9 Sampling Theory and Techniques 179
9.1 Introduction. 179
9.2 Motivation for Sampling 180
9.3 Theory Behind Sampling. 181
9.4 Statistical Sampling Techniques 182
9.5 Nonstatistical Sampling Techniques. 186
9.6 Sampling Approaches in Auditing 189
9.7 Chapter Summary. 191
9.8 Endnotes. 193

10 Statistical Inference from Sample Information 195
10.1 Introduction.. 195
10.2 The Ability to Generalize Sample Data to Population Parameters... 196
10.3 Central Limit Theorem and non-Normal Distributions........... 199
10.4 Estimation of Population Parameter 200
10.5 Confidence Intervals... 203
10.6 Confidence Interval for a Large Sample When Population Standard Deviation Is Known 205
10.7 Confidence Interval for a Large Sample When Population Standard Deviation Is Unknown...................................... 209
10.8 Confidence Intervals for Small Samples 211
10.9 Confidence Intervals for Proportions 213
10.10 Chapter Summary.. 214
10.11 Endnote 218

11 Determining Sample Size 219
11.1 Introduction.. 219
11.2 Computing Sample Size When Population Deviation Is Known.... 220
11.3 Sample Size Estimation when Population Deviation Is Unknown... 222
11.4 Sample Size Estimation for Proportions 225
11.5 Chapter Summary.. 228

12 Regression and Correlation.. 231
12.1 Introduction.. 231
12.2 Probabilistic Linear Models...................................... 232
12.3 Correlation... 233
12.4 Least Squares Regression 234
12.5 Coefficient of Determination 236
12.6 Test of Significance and p-Values 237
12.7 Prediction Using Regression 238
12.8 Caveats and Limitations of Regression Models................... 239
12.9 Other Regression Models... 242
12.10 Chapter Summary.. 245

Index.. 249

Foreword

The Supreme Court's 1993 *Daubert v. Merrell Dow Pharmaceuticals* decision has had far reaching consequences on the Federal Rules of Evidence and has set the standard for admitting expert testimony in federal courts. Daubert confirmed that statistics was a field of scientific knowledge and generally admissible under Rule 702 of the Federal Rules of Evidence.

If statistics can be used in cases involving scientific and medical research as in Daubert, and in opinion surveys, market analyses, and even in determining who will be the President of the United States, statistical evidence can also be used by forensic accounting experts in support of their findings.

Statistical evidence must be *precise* and *reliable* to be able to pass Daubert challenges and, if all such challenges are passed, be persuasively used in court to present the expert's opinion and to withstand opposing expert rebuttal and cross-examination by opposing counsel. Precision and reliability are words that also have very important statistical definitions.

Taking a "sample" from a population and drawing a conclusion about some characteristic of that population is something accountants do all the time; however, this is usually done in the context of an audit of financial statements, where data is already accumulated in journals and summarized into ledgers, and the accountant/auditor has had an opportunity to study the internal control environment. Moreover, financial statement audit conclusions are based on the results of many interrelated tests, such as confirmation with third parties, analytical analysis, and timely physical inspections, not just the result of the audit sample. This is often not the case in a forensic investigation.

Unfortunately, when accountants/auditors are taken out of the financial statement audit comfort zone and are engaged to conduct a forensic investigation, they often apply the audit sampling approach permitted by their professional rule-making body that permits reliability and precision to be expressed qualitatively instead of quantitatively. This can only lead them into trouble. It is the ability to quantitatively measure reliability and precision that makes statistical sampling the only real choice in litigation support services engagements.

EisnerAmper was engaged by Counsel ten years ago to provide assurances to the Court regarding the accuracy of 950,000 claims processed in the $6.1 billion WorldCom Securities Litigation Settlement Fund. A random sample across the population of claims that had over $46 billion in recognized loss amounts where over 95% of the claims were under $5,000 would yield a sample of a high proportion of small claims and a small proportion of large claims. Such a test would bias the results against finding the true error in the population of claims. I knew I had to reach out to someone who understood these ramifications and could communicate the approach taken to address them, and the results and conclusions reached, in a manner that would withstand scrutiny from many constituents on the one hand, but be communicated in a manner that would be understood by the Court, so it could be confident in authorizing payments to claimants. I reached out to the only person I knew who could do this, Dr. Saurav Dutta.

EisnerAmper has consulted with Dr. Dutta many times in past ten years in other litigation support services engagements and forensic investigations requiring the use of sophisticated statistical sampling applications and complex assignments involving derivatives, and he has proved to be a valuable resource to our firm.

It was natural progression for Dr. Dutta to apply his technical and communication skills to the writing of a book for forensic accountants and investigators, which can be used by attorneys and triers of fact as well. I have had the pleasure of reading this book during its development and believe you will find the sometimes complex word of statistics explained in a clear and concise manner, and its application will enhance your practice.

David A. Cace
Partner
EisnerAmper LLP

Acknowledgments

In March of 2011, when I was with the Securities and Exchange Commission, Ms. Jeanne Glasser, an Executive Editor at FT Press, contacted me to discuss publishing opportunities. SEC regulations precluded me from working on the book at the time. Exactly a year later, Jeanne reminded me that the publishing opportunity was still available and asked me to start writing. In sum, the book would not be possible without Jeanne's perseverance. Throughout the process, she was always available and provided necessary help and guidance. Moreover, she was patient during the inevitable delays and missed deadlines.

I was introduced to the topics of statistics and accounting during the course of my graduate study at the University of Kansas, for which I am forever indebted to the support of the faculty at KU. In particular, I am grateful to Professors Glenn Shafer and Rajendra P. Srivastava, without whose guidance and mentoring I would not possess the necessary skills to write this book. All of my coursework in probability and statistics were with Glenn. He also gave me my first copy of Strunk and White's *Elements of Style*. Raj relentlessly encouraged me to pursue graduate studies in accounting and chaired my doctoral dissertation.

I benefitted much from my interactions with many of my faculty colleagues at Rutgers University and at the University at Albany. My interactions with Dr. Lynford E. Graham were extremely valuable. Additionally, I thank many organizations for providing me with opportunities to apply statistical techniques to real-world accounting problems. Specifically, I thank Mr. Nicholas Adelizzi, Mr. Victor Albanese, Mr. David Cace, Ms. Robin Cramer, Mr. Tobias Feinerman, Ms. Marisol Gonzalez, Mr. Elliott Lee, Mr. Nicholas Sheridan, Ms. Dayna Shillet, and Mr. Timothy Van Noy for their interactions and practical insights.

The book has benefitted significantly from comments and suggestions of two of my esteemed colleagues, Professors Dennis Caplan and David Marcinko. Both painstakingly reviewed earlier drafts of the chapters and made numerous suggestions to improve the content and the delivery. I am indebted to them for their time and generous help throughout the process. Scott Cestone, one of my former students, tirelessly worked in editing the chapters and providing a student perspective to the material. He did so while simultaneously preparing for his CPA examination, for which I am extremely grateful. I thank Ms. Elaine Wiley and Ms. Chrissy White of FT Press for their editorial suggestions and help in getting this manuscript to its published form.

About the Author

Dr. Saurav K. Dutta is an Associate Professor at the Department of Accounting, Business Law, and Taxation at the State University of New York at Albany, where he previously served as the Chairman of the Department. He has taught at the Graduate School of Management, Rutgers University, and at Zicklin College of Business, Baruch College, New York. He holds a Bachelor of Technology Degree in Aerospace Engineering from the Indian Institute of Technology (Bombay) and a Ph. D. in Accounting from the University of Kansas.

His research interests are in applying statistical and analytic methodology to accounting and auditing problems, and his current work involves analyzing problems in financial reporting, as well as studying the accounting aspects of corporate sustainability initiatives. He has published over 25 research papers in academic journals, including *Auditing: A Journal of Practice and Theory; Journal of Accounting, Auditing, and Finance; Journal of Accounting and Public Policy; Issues in Accounting Education; Journal of Cost Management; Journal of Corporate Accounting and Finance*; *International Journal of Technology Management; The Quality Management Journal; Corporate Social Responsibility and Environmental Management; Strategic Finance;* and others. Dr. Dutta has presented his research findings at numerous national and international academic conferences and has conducted research seminars at many universities including, Harvard, Oxford, New York University, Rutgers, University of Southern California, Michigan State, Bentley, and Maastricht. He has conducted professional teaching and training seminars at Dai-Ichi-Kangyo Bank, Merrill Lynch, Prudential Insurance Company, and KPMG LLP. He has been invited by the AICPA to conduct workshops on the use of statistics in forensic accounting, and he has also been the "Featured Speaker" for the Corporate Director's Group.

Dr. Dutta has been engaged to design and analyze statistical tests on numerous accounting/litigation projects under the jurisdiction of the New York State Attorney General's Office, U.S. District Court of the Southern District of New York, and the Securities and Exchange Commission, among others. Some of these engagements involved designing statistical procedures to verify claims for settlements of amounts ranging from $500 million to $6.1 billion and include the settlements for MCI-WorldCom, Global Crossing, Cendant Corp, and HealthSouth. He was involved with the reparations of more than 400 million

CHF from the Swiss banks, under the purview of the U.S. District Court of Eastern New York. He has also been engaged to evaluate accounting systems related to hedge accounting, fair value accounting, and mergers and acquisition. Since 2006 he has served as the Subject Matter Expert (SME) for the IMA in their preparation and updating of the CMA examination study guide.

Preface

Unfortunately forensic accounting is a growing profession. In fact, the FBI has added staff to its Forensic Accounting and Financial Crimes Division to address the increase in financial crimes. Further, forensic accounting is an expanding practice for the Big Four and other public accounting firms. This growth is attributable to the increased cost of fraud, the rise of Internet technologies that facilitate fraud, and recent legislation in some jurisdictions. Financial fraud is a global problem, and recent surveys conducted by KPMG and PwC show an increase in both the number and magnitude of fraud in many countries. Globalization, technology, and pursuit of business efficiency have made fraud easier to commit and harder to detect, making the forensic accountant's job more challenging. The ability to detect financial fraud, honed by years of experience, is an art. It is the art of skillful conjecture.

Many useful books are available to help forensic accountants develop this art of conjecture. These pioneering books laid the foundation for the discipline. Donald Cressey's *Fraud Triangle*, Steve Albrecht's books on fraud examination methodology and Joseph Wells' many books outlining fraud schemes are important contributions to the discipline. More recently, Mark Nigrini's book, *Forensic Analytics* applies Benford's Law to develop a tool for fraud detection.

This book, *Statistical Techniques for Forensic Accounting,* builds on the foundation of probability and statistical theory to help readers apply mathematical tools to the art of identifying financial fraud in that it provides a structure to conjecture. Financial information typically consists of large amounts of data. An occurrence of fraud or misrepresentation creates a pattern of errors within the data. Effective forensic accountants uncover those patterns based on intuition, conjecture, or experience. After the pattern has been identified, the onus rests with the forensic accountant to convince others—and ultimately the justice system—that the pattern was deliberate and not caused by random occurrence. This book makes a contribution to formalizing the process of pattern recognition and establishing the probability that it is deliberate. It requires no prior knowledge in probability and statistics and presents mathematical concepts, notation, and equations in a manner understandable to practicing accountants.

Statistics provides a structured process to synthesize and analyze large amounts of data as well as examines uncertainty. Additionally, the discipline has developed sophisticated and well-accepted tools that enhance the efficiency and effectiveness of the process. It is therefore natural that statistical tools such as data mining can be applied to financial data analysis to investigate the possibility of fraud. Statistical methodology has been gaining wider applicability and acceptance in the judicial system in general. For example, DNA evidence and ballistics are built on a foundation of probabilistic reasoning. Anecdotally, jurors often place more credence on DNA evidence, which is probabilistic, than on eyewitness accounts, which are often and notoriously unreliable.

Prior to the use of statistical evidence in forensic accounting, an understanding of the applicability and limitations of such methods is imperative. It is a widely accepted view that mathematics is often best learned within the context of the discipline itself. However for the discipline of forensic accounting, no such book is currently available. It is therefore the primary aim of this book to fill that gap. Several real-world cases of financial various parts of the world are briefly summarized and form a backdrop for the statistical methodology.

This page intentionally left blank

1

Introduction: The Challenges in Forensic Accounting

I spent about ten years exposing corporate and financial fraud for Barron's *magazine, and I found a lot to write about.*
—Ben Stein

1.1 Introduction

Investigating corporate fraud cases is one of the highest priorities of the United States Federal Bureau of Investigation (FBI). At the end of 2011, 726 fraud cases were being actively investigated by various FBI field offices throughout the U.S.,[1] which was an approximately 10% increase from the number of cases being pursued at the end of 2010 and a 37% increase over a five-year period. It is estimated that several of these cases resulted in losses to investors exceeding $1 billion.

In response to the growing importance of accounting investigative skills within the Agency, the FBI established a Forensic Accountant Unit in March 2009 to support FBI investigations requiring financial forensics. The creation of this program was the culmination of the FBI's efforts to advance and professionalize its financial investigative capabilities. The mission of this unit is to develop, manage, and enhance the FBI's Forensic Accounting and Financial Analysis programs.

Corporate fraud has been a persistent problem in the U.S. economy since the early days of the stock market. One of the oldest and most commonly known frauds is the Ponzi scheme, named after Charles Ponzi, who duped thousands of New England residents into investing in postage stamp speculation back in the 1920s. He promised his investors a 50% return in just 90 days at a time when the annual interest rate at banks was just 5%. He was able to fulfill his promise by using incoming funds to pay off early investors. His name is now synonymous with investment fraud schemes that involve attracting new investor money to fulfill the obligations owed to early investors. As long as the amount of incoming funds in the form of investment by new or existing investors exceeds the outgoing funds that are withdrawn by outgoing investors, the scheme thrives. However, it quickly unfolds in an economic downturn when investors have little excess funds to invest and more investors wish to cash out their investments. In the recent financial crisis of 2007, many investment funds, including that of Bernie Madoff and Stanford International, were found to have engaged in the decade-old Ponzi scheme to defraud investors. In the 1920s, Charles Ponzi's investors lost upwards of $20 million. About a century later, in 2007 Bernie Madoff's investors lost upwards of $20 billion.[2] Although there are obvious red flags to detect Ponzi schemes,[3] these are often ignored by trusting investors who are sometimes in awe of the personality, success, and demeanor of the perpetrators.

Investment fund managers who perpetrate Ponzi schemes most often defraud investors by promising high returns. However, other businesses, though not directly engaging in Ponzi schemes, can still defraud investors by painting a false financial picture. By recording fictitious transactions or other accounting gimmicks, a business might inflate income or revenue or understate expenses to paint a rosier picture of its financial prospects. At times, senior officers of public companies with much personal wealth and reputation vested in the financial success of their companies resort to such means. In this chapter you learn about some of the recent well-publicized cases of corporate fraud.

Not all types of corporate fraud are committed by management to misinform investors and other third parties. A majority of occurrences and investigations of fraud involve acts by individuals committed against their organizations. One notable case prosecuted by the FBI in 2011 involved a former vice-president of Citigroup who embezzled more than $22 million from Citigroup over a period of eight years. The perpetrator transferred money from various Citigroup accounts to Citigroup's cash account and then wired the money to his personal bank account at another bank. False accounting entries were created by the perpetrator to conceal the theft. In this chapter you read about common fraudulent schemes undertaken by employees to steal from the organization and the accounting cover-ups undertaken to conceal the crimes.

The remainder of this chapter discusses the nature of fraud schemes, presents the statistics of fraud investigations conducted by the FBI, and examines trends of various types of fraud. It then briefly covers the common management fraud schemes undertaken in recent years. Next is a discussion of common employee fraud schemes, which summarizes the results of a study conducted by the Association of Certified Fraud Examiners (ACFE). In recent years, with the Internet being so widely accessible, coupled with an immense growth in e-commerce, cyber-crime against businesses is rampant. The chapter concludes with an analysis of the ramifications and challenges imposed by this growing crime.

1.2 Characteristics and Types of Fraud

Fraud is not only a theft of assets but also an attempt to conceal it. Misappropriation of assets without an attempt to conceal is merely a theft, which is usually uncovered quickly through normal checks and balances procedures. Concealment distinguishes fraud from theft. As perpetrators attempt to conceal fraud, they might continue to engage in similar misappropriations over an extended period of time. A theft often occurs only once because the victim becomes armed with the knowledge of that theft and takes necessary precautions to deter future occurrences; the victim of a fraud, on the other hand, is usually unaware of the loss, and hence the perpetrator can repeatedly commit the crime. In that sense, fraud is nothing but recurring theft on the similar type of victim by the same perpetrator. In the instance of corporate fraud, there is a sole victim, the organization, and usually there are multiple occurrences of theft that impact that organization.

The FBI characterizes fraud as comprising of deceit, concealment, and or violation of trust. Fraud is not usually dependent on the application or threat of physical force or violence. The FBI has recently investigated and prosecuted many financial crimes, including corporate fraud, securities and commodities fraud, health care fraud, financial institution fraud, mortgage fraud, and others. This section provides an overview of these schemes, and subsequent sections discuss in more detail corporate fraud committed by insiders (employees and management) of an organization.

Figure 1.1 plots the number of cases in each category investigated by the FBI over the seven-year period from 2005 to 2011. The “other” category is comprised of money laundering, insurance fraud, and mass marketing schemes. The plot represents the total number of ongoing investigations at the end of each reporting period. It is important to note that this does not reflect the number of new cases for each year. An upward sloping line indicates that the number of new cases in that category exceeded the number of cases that were settled or resolved. Similarly, a downward sloping line indicates that the number of cases settled for that category was greater than the number of new cases. Thus, a decline in the number of open cases does not necessarily indicate a decrease in that category of crime but could be due to speedier resolution of the pending cases from previous years.

Over the seven-year period, health care fraud cases have been steadily high at about 2,500 cases annually. In contrast, investigations related to mortgage fraud spiked in 2008 and 2009, exceeding the 2,500 mark. This spike was primarily related to investigations following the collapse of the sub-prime lending market in the United States. Investigations related to securities fraud also increased in the 2008–2009 timeframe, but the increase was not as drastic as the increase in mortgage investigations. Open investigations on corporate fraud were relatively steady over the seven-year period. In contrast, investigations of financial institution fraud and others have been declining in recent years. The percentage of growth or decline in the number of cases over the previous year for each category is plotted in Figure 1.2.

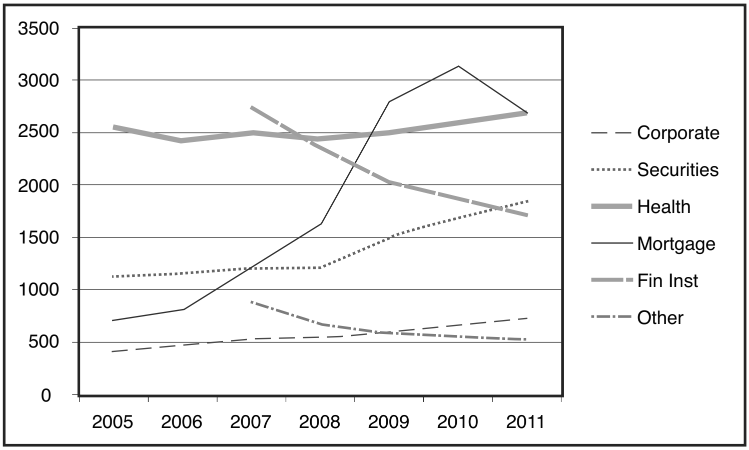

Figure 1.1 Number of fraud cases by category investigated by the FBI between 2005 and 2011

Data for the graphs obtained from the FBI's *Financial Crimes Report to the Public* from the years 2009 and 2011. The 2009 report covers the years 2005–2009, and the 2011 report covers the years 2010–2011.

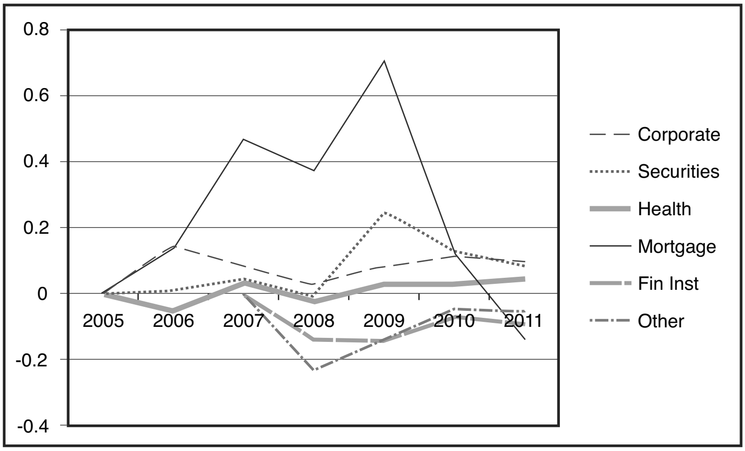

Figure 1.2 Percentage change in cases by category investigated by the FBI 2005–2011

Investigations related to corporate fraud are usually conducted by the FBI in collaboration with the Securities and Exchange Commission (SEC). Often the investigation is initiated at the SEC following a tip from a whistleblower. Upon follow up if the SEC suspects criminal wrongdoing, the FBI is alerted, and a criminal investigation ensues. Corporate fraud cases usually involve accounting schemes designed to deceive investors, auditors, analysts, and others regarding the true financial condition of the corporation. The usual objective for such crimes is to artificially lower the cost of borrowing by inflating the share price based on fictitious corporate performance indicators. As can be seen in Figure 1.2, the number of such cases has been relatively stable over the seven-year period. In 2011, the pursuit of these cases led to 241 convictions, and the FBI secured $2.4 billion in restitution orders.

Corporate fraud investigations focus not only on the misrepresentation of a firm's financial conditions, but also on the investigation of allegations involving insider trading. A multitude of parties can potentially engage in trading based on insider and nonpublic information. These parties include corporate insiders, corporate attorneys, traders, and other financial intermediaries such as accountants and investment bankers who are privy to confidential and nonpublic information.

The volatility of the financial market in recent years has caused investors to seek alternative investment opportunities. This investor need has created a demand for new and innovative investment products and opportunities. Concurrent with investors' growing need for alternate investment vehicles and their eagerness to invest in new and untested products, the FBI saw a steady rise in securities and commodities fraud in 2009 and 2010. These new schemes and trends included

- Securities market manipulation through cyber-intrusion
- Increased commodities fraud
- A continuing rise in Ponzi schemes
- Onslaught of foreign-based reverse merger schemes

Figure 1.2 showed the plot corresponding to securities fraud spikes in 2009, signifying that such fraud schemes are increasing at a faster rate following the recent financial crisis. The victims of securities fraud include individual investors, pension and retirement funds, government entities, financial institutions, and private and public companies. The creation of complex investment vehicles makes prevention and early detection of such schemes difficult, resulting in higher losses for the victims of such schemes.

As seen from Figure 1.1, health care fraud, an important area of investigation for the FBI, has traditionally been their most prolific type of case; however, the number of cases has been relatively stable over the seven-year period if you compare the data to that shown in Figure 1.2: the graph is close to the x-axis, or zero, denoting little change. Data mining techniques, which are covered in a later chapter, are used to detect health care-related fraud schemes. In 2011, the FBI recovered $1.2 billion in restitution, $1 billion in civil settlements, and an additional $1 billion in fines. The prevalent schemes for health care fraud identified by he FBI include

- Billing for services not rendered, either wholly or partially.
- Duplicate billing.
- Upcoding of services to generate higher payments.
- Upcoding of items.
- Kickback schemes.
- Unbundling, which involves billing separately for individual items to maximize reimbursement when they are required to be billed together at a reduced cost. For example, a laboratory test can be ordered individually or as a panel. A panel test usually costs less than the sum of the individual tests.

Another area of fraud that is rapidly increasing is mortgage fraud, the victims of which include financial institutions and investors. Mortgage frauds primarily occur at *entry* or *exit points*. In other words, they occur at the time of loan origination or at the time of foreclosure or delinquency. After underwriting rules were tightened in response to the financial crisis that began in 2007, the year 2011 was the first time that distressed homeowner frauds outnumbered loan origination fraud. As seen in Figures 1.1 and 1.2, the investigations of mortgage fraud spiked considerably in 2009 following the financial crisis and the near-abolition of the sub-prime market.

Following the global financial crisis, many incidents of financial institution fraud came to light. Having started at the highest level in 2007, the cases corresponding to this category have been declining over the years. This includes investigation of financial institution failures. The number of bank failures during 2009 and 2010 had significantly increased to about 150 per year but then in 2011 decreased to under 100 per year. Over the five years following the global financial crisis, there have been about 400 bank failures. Although still a large number, this cumulative total compares favorably to more than 1,000 banks closing over the five-year period from 1987 to 1992 and more than 9,000 bank failures during the Great Depression (1930 to 1933).

Other types of financial fraud investigated by the FBI include insurance scams, money laundering, and mass marketing frauds. One of the most prevalent mass marketing frauds in recent times is the Nigerian email/letter that you might have personally encountered. In this scheme victims are asked to act as U.S. agents to facilitate transfers of huge sums of money held in foreign accounts into the U.S. The victims are promised a generous portion of the total proceeds for their efforts. The victims are then required to open accounts at fraudulent websites and transfer their holdings from legitimate banks to fictitious ones; once completed, the funds are stolen by the perpetrator.

1.3 Management Fraud Schemes

Management fraud, as the name suggests, is perpetrated by the top management of a company who has the intention of misleading investors. The most common form is through accounting manipulation, which materially misstates the financial statements of the company. The motivation behind the fraud is usually to maintain a high stock price and thereby lower the cost of capital for the company.

One of the most common ways to inflate earnings is by simply overstating or misclassifying revenue. There are many well-known fraudulent schemes that have been used to inflate revenue, such as

- Bill and hold sales. In such schemes the company bills the customer for the sale, hence creating a perception that a legitimate sale was made, but it never ships the goods. Instead in the following accounting period it simply reverses the sale, reporting that there was a customer return.
- Booking fictitious sales. This scheme is discussed shortly in the context of fraud committed at HealthSouth.
- Holding books open at the end of the period. Through this method the next period's sales are recorded in the current period, thus inflating the revenue of the current period while understating revenue in the subsequent period. This scheme was used by Computer Associates.
- Delaying reporting of customer returns. When customers return merchandise, the revenue initially recognized from those sales must be reversed. By delaying the reporting of returns to the next period, management effectively reports higher revenue in the current period.

The overstating of revenue would in most cases also overstate accounts receivables and hence would also overstate assets.

The overstatement of revenue may not always be sufficient to inflate income to the desired level; hence management might use a combination of understating expenses along with overstating revenue. The common schemes to understate expenses include

- The understatement of cost of goods sold by padding inventory. When a periodic inventory accounting method is used, the cost of goods sold is indirectly determined by measuring ending inventory. Inventory is overstated, causing a decline in the cost of goods sold expense.
- Capitalization of costs in order to reduce expenses. When costs are capitalized, the resulting expense is spread over multiple years rather than reporting all of it in the current year. Capitalizing costs that should be expensed results in the understatement of expenses in the current period, leading to a overstatement of income. The capitalized costs are reflected as assets, hence also overstating total assets on the balance sheet. This scheme was used in the Worldcom fraud and is discussed in a subsequent section.
- Extending the depreciable lives of assets, thereby reducing depreciation expense. As depreciation expense is linked to the management's estimation of the useful life of an underlying asset, overestimating the lives of assets reduces the depreciation expense, resulting in an overstatement of income. This scheme was employed by Waste Management.

Understating expenses also leads to overstatement of assets or understatement of liability. When costs are capitalized and not expensed, it leads to higher assets. When accrued expenses are not recorded, it leads to an understatement of liability.

Balance sheet fraud is committed with the intention of reporting lower debt and liabilities than the company actually bears. This is often accomplished through the use of off-balance sheet financing. Schemes to fraudulently reduce liabilities include

- Misclassification of leases. Although capital leases are recorded as a liability, under U.S. Generally Accepted Accounting Principles (GAAP), operating leases currently are not required to be reported as a liability. Misclassification of a capital lease as an operating lease allows a company to remove the underlying liability from its balance sheet.
- Not recording accrued expenses. As just discussed, a failure to record accrued expenses results in the income being overstated and the liabilities being understated.
- Concealing liabilities in the accounts of unconsolidated subsidiaries. As in the case of Enron, shell companies were created with the sole purpose of off-loading liabilities from Enron's financials onto the financials of these shell companies.
- Structuring sophisticated financial transactions such as Repo 105 to remove liabilities from the balance sheet. As discussed next, Lehman structured a "round-trip"

> transaction, which enabled them to reduce both assets and liabilities on the reporting date thereby presenting a lower leverage ratio.[4]

The remainder of this section discusses a few prominent cases of recent business failures in which the use and interpretation of accounting rules were questionable.

Fraud at WorldCom

WorldCom was accused of having inflated profits by $3.8 billion over a period of five quarters. The company undertook the massive fraud by capitalizing costs that should have been expensed. Capitalization of these costs allowed the company to spread the expenses over several years instead of recording all the costs as expense in the current period. Such deferral of costs allowed the company to report lower expenses and therefore inflated income.

From 1998 to 2000 WorldCom reduced reserve accounts held to cover the liabilities of acquired companies resulting in $2.8 billion in additional revenue. They misclassified expenses and marked operating costs as long-term investments. There were undocumented computer expenses of $500 million, which were treated as assets. The fraud was uncovered by the internal auditors in July 2002; soon thereafter WorldCom filed for bankruptcy.

Fraud at HealthSouth

HealthSouth, a publicly traded company headquartered in Birmingham, Alabama, with 1,600 locations spread over all 50 states and three other countries, was by many accounts the first company to be prosecuted under the provisions of the Sarbanes-Oxley Act of 2002. Its former CEO, CFO, and other senior officers fraudulently inflated the company's reported income to meet Wall Street's earnings expectations. The fraud began in mid-1996 and spanned for about seven years, during which time their true cumulative income was $1.7 billion or about 40% of what the company had reported. The SEC charged the senior officers in March 2003 for knowingly falsifying accounting records and designing fictitious entries to overstate cash by $300 million and overstating total assets by at least $800 million.

Evidence presented at the trials showed that facilities owned by HealthSouth submitted legitimate financial reports to the headquarters in Birmingham. However, at the corporate office those numbers were inflated at the time the consolidated financials were prepared. A fictitious account called *contractual adjustments* was created to book fake revenue numbers. Additionally, the company failed to properly record the sale of technology to a related company, resulting in a $29 million overstatement. Also HealthSouth twice recorded a sale of 1.7 million shares of stock in another company, netting a $16 million gain. Examiners also found fictitious assets totaling close to $2 billion.

The fraud mechanism used by HealthSouth required collusion among various employees who were known as "family" and attended quarterly "family meetings" to cook the books. Top company officials reviewed unpublished financial results and compared those with Wall Street expectations. The shortfall was termed as a gap or hole that had to be filled using "dirt." Staff accountants were instructed to make fictitious entries to fill the "gap," and false documents were created in an attempt to conceal the false entries from the auditors. It was common knowledge that auditors verified transactions over $5,000, hence fictitious transactions were made for amounts between $500 and $4,999. To gain a proper perspective on the sheer enormity of the fraud, it required an upward of two million falsified journal entries to overstate the income by almost $5 billion. This was a clear indication of how widespread the involvement and knowledge of the fraud was within the organization. At the conclusion of the investigation, it seemed that everyone in the organization was aware of the massive fraud—except the auditors.

Questionable Accounting Practices at Lehman

In September 2008, Lehman became the largest company in U.S. history to file for bankruptcy. Nine months earlier, Lehman had reported record revenue and earnings for 2007. In early 2008, Lehman's stock was trading in the mid-sixties with a market capitalization of more than $30 billion. Over the next eight months, Lehman's stock lost 95% of its value and was trading around $4 by September 12, 2008. In March 2010, Lehman's Bankruptcy Examiner, Anton Valukas, issued a 2,200-page report that outlined the reasons for the Lehman bankruptcy.[5]

Lehman routinely engaged in short-term borrowing but structured some of these loans under a scheme known as Repo 105. Repo transactions are quite common in the financial industry. Under a Repo agreement a bank borrows funds and transfers assets to the lender as collateral. At a later date, the bank pays back the loan with accrued interest and repossesses the transferred assets, hence Repo. Normally, the collateral is 2% above the borrowed amount. Lehman altered the agreement slightly and transferred assets whose market value was 5% above the borrowed amount. However, instead of classifying these transferred securities as collateral for the loan, to be returned upon the settlement of the loan, Lehman would record the transfer as a sale with an agreement to repurchase on a specified date.

Interestingly, during the term of a Repo 105 transaction, Lehman continued to receive the stream of income through coupon payments from the securities it transferred.

Additionally, just as in an ordinary repo transaction, Lehman was obligated to "repurchase" the transferred securities at a specified date. Moreover, Lehman used the same documentation to execute both Repo 105 and ordinary repo transactions, and these transactions were conducted with the same collateral agreements and substantially with the same counter-parties. Lehman's usage of Repo 105 was timed around the end of reporting periods. The Examiner's Report analyzed the intra-quarter data on the usage of Repo 105 and concluded that its usage spiked at quarter-ends and fell off on an intra-quarter basis. The amount of Repo 105 activity at period-end from late 2007 to mid-2008 ranged from $39 billion to $50 billion. The use of Repo 105 transactions enabled Lehman to remove assets and corresponding debt from its balance sheet, yielding a marked improvement to its leverage ratio. The ratings agencies and counter-parties to Lehman's Repo transactions were concerned about the high leverage ratio of Lehman. Thus, being able to show a decrease in their leverage ratio was beneficial to Lehman. It is unclear as to whether or not the use of Repo 105 led to the demise of Lehman; however, it is evident that Lehman employed a questionable accounting treatment of Repo 105 that had no business purpose or economic significance other than to understate their leverage ratio.

Lessons Learned

As illustrated through these examples, management fraud, although not rampant, could have potentially devastating effects on the reputation and sometimes the viability of the company and the auditor. Moreover, management fraud is usually ongoing over several years. Even though cleverly concealed, many employees are aware of the scheme and usually would have raised red flags or otherwise tried to warn auditors and regulators. Complaints from former employees should not be dismissed casually as being vindictive, but due professional care has to be exercised by the auditor. Statistical techniques presented later in the book can perhaps lead to early detection of such fraudulent schemes and limit losses to investors, employees, and society.

1.4 Employee Fraud Schemes

The Association of Certified Fraud Examiners conducted a substantial study to classify occupational fraud cases. The recent edition published in 2010 presented updated descriptive statistics on the occurrence, damages, and so on of occupational fraud. The schemes discussed in this section are the common schemes reported in that study. Further details on the schemes and methods of prevention and detection are available on ACFE's publication.[6] The following sections present a brief description of the common fraud schemes and ways to detect and deter them.

Skimming

Organizations that engage in cash transactions are vulnerable to skimming by their employees. Skimming involves theft of cash, generated usually from sales, prior to its entry into the accounting records. Skimming is a relatively common occurrence in professional practices where fees are collected in cash. The cashier responsible for collection might pocket the cash and not enter the transaction into the accounting records or subsequently delete those records after being entered into the system. Medical practices are particularly vulnerable to this type of fraud, as small amounts of copayments are collected in cash, and the patients are not that particular about obtaining receipts as there isn't an opportunity for a refund. Instituting proper internal control systems that mandate giving receipts to the customers or installing surveillance equipment can mitigate the risk of fraud caused by skimming.

Even for retailers that sell merchandise for cash, theft through skimming is quite prevalent. In some cases, the employees keep the store open beyond regular business hours and pocket the sales made at those times instead of properly recording the sales in the accounting records. For merchandising companies, because a sale involves the exchange of goods, skimming results in inventory shrinkage. That is, there is reduction in inventory totals without corresponding sales. In these instances, a pattern of inventory shrinkage is generated.

Another type of business that is vulnerable to skimming is off-location rental services, in which the on-site manager usually has much autonomy. The manager may rent out property for cash without making the necessary accounting entry or without reporting the rental revenue to the organization. Random on-site inspections and correlating maintenance expenses with rental revenue are two approaches to ensure early detection of such schemes. The statistical technique of correlation, developed in a subsequent chapter, can be applied to identify the pattern between rental revenue and maintenance costs. The application of this procedure enables the identification of locations that are anomalous and perhaps need to be visited.

Lapping or Fraudulent Write-offs

Another common form of skimming is undertaken by mail room employees who are responsible for receiving payments and can therefore skim the checks received. That is, instead of depositing the checks in the company account and logging the payment into the accounting system, the employees would deposit checks into their accounts and steal the funds. This kind of scheme requires a cover-up or falsification of records. Without a cover-up the scheme is unraveled quickly when the company sends a second bill and the customer furnishes a cancelled check as proof of payment. Hence perpetrators of such crimes also need to conceal the theft of the checks. Two common ways to conceal the theft are *lapping* and *fraudulent write-offs*. In a lapping scheme, one customer's payment is posted on another customer's account.[7] For example, assume the perpetrator stole Mr. Smith's payment; next, when Mr. Jones makes his payment, it is applied to Mr. Smith's account, and later when Mr. Wells makes a payment, it is applied to Mr. Jones's account, and so on. Thus, when the perpetrator laps customers' accounts, he repeatedly alters accounting records, even though the theft of funds occurred only at the outset.

The fraudulent write-off of a customer's account is another way to bring the account up-to-date without the organization receiving the payment. As noted earlier, the customer is going to complain after receiving a second bill for the amount he or she has already paid. This can provoke internal investigation of the missing funds. To prevent customers' complaints, the perpetrator of the crime has to keep the second bill from being sent to the customer. The customer will not be billed by the organization if the account is written off. The perpetrator would therefore try to write-off the customer account and steal the funds that the customer sent as payment. This way the funds are stolen, the customer isn't billed repeatedly, and the accounting records balance. Because most large organizations segregate the duties of receiving cash, maintaining accounts receivables records, and authorizing write-offs, collusion between employees has to occur for this scheme to be successful. Chapter 5, "Data Mining," shows how such collusion can be unraveled through the use of association mining.

With the increased popularity of online payments, skimming of receivables is a diminishing threat in most modern organizations. However, for organizations still employing traditional methods of receiving payment by checks or cash, institution of proper internal controls can prevent or lead to early detection of such schemes. In subsequent audits, identifying unusual patterns on customer accounts could also unravel such schemes.

Use of a Shell Company

High-level employees within an organization with authority over disbursements may create shell companies that they control. These shell companies then bill the organization for fictitious goods and services. The perpetrator usually is in a position to approve charges or has authority over personnel who approve payments on behalf of the organization. As the payment is made to the shell company, the perpetrator has effectively stolen funds from the organization.

Fraudulent shell companies often will use a P.O. box or residential address as a business address. Sometimes the owner of the shell company could be the spouse or other close relative of the perpetrator, and their names or addresses could be used to set up the shell company. Often the billing documents from these shell companies lack the authenticity of legitimate companies. For example, use of a shell company was discovered when a secretary noticed that the street address of a vendor was the home address of her supervisor. In another instance, fraud was revealed when it was observed that invoices from a vendor that were months apart were sequentially numbered. The implication therefore was that the victim organization was the only customer for this vendor. On further investigation, the fictitious vendor was revealed.

Shell companies can at times sell legitimate goods to the company but at an inflated price. The shell company purchases the goods needed by the organization from legitimate vendors and then resells to the organization at an inflated price. The individual(s) who own the shell company pocket the difference. Such schemes are known as pass-through schemes.

Verifying the list of vendors and ascertaining their legitimacy is an effective way of uncovering the use of a shell company. Data analytic techniques could be effectively employed to analyze large amounts of vendor data to identify anomalies and suspicious activities.

The Enron financial scandal increased the public's awareness of the use of shell companies to commit fraud. Even though shell companies were used by Enron for fraudulent purposes, they were not used to embezzle from the company, but rather to falsify their financial statements. Enron's use of shell companies is an example of management fraud where the victim was not the organization but the investors and other third parties.

Ghost Employees

A common fraudulent scheme involving payroll is for Human Resource managers or Payroll managers to create *ghost employees*. The ghost employee, while on the payroll of the company, collects wages periodically but does not actually work for the company. This could be a fictitious person or a family member of the perpetrator. By means of falsifying personnel and payroll records, a ghost employee is added to the payroll and hence collects monthly wages. The potential loss to the victim organization of a ghost employee scheme could be enormous due to the recurring nature of the theft. After the perpetrator has successfully created a ghost employee in the payroll system, the regular process of issuing paychecks ensures a steady stream of funds to the perpetrator. When successfully instituted, unlike the schemes of a shell company or skimming, the perpetrator of a ghost employee scheme does not have to engage in any further maintenance of the fraudulent scheme. As there are no recurring actions on the part of the perpetrator, the data shows no unusual patterns.

The existence of ghost employees is difficult to detect by performing trend analysis or investigating unusual patterns; instead, they can be identified by comparing different databases. The perpetrator could have access to a couple of databases and thus might be able to alter them. However, she will not be able to include the ghost employee in other essential databases to which she has no access. Because the ghost employee doesn't really work at the company, there is no documentation of work performed by this employee, no vacation days taken, no performance evaluation report, and so on. Reconciling employee data across various functions of the organization can help to detect ghost employees. Data mining and statistical techniques are helpful in identifying the handful of employees who are outliers across various organizational functions so the investigation can focus on them.

Inventory Shrinkage

When inventory is sold and the corresponding sale is not recorded (as in skimming discussed earlier) or when inventory is stolen, the perpetrator has to amend the unaccounted decrease in inventory balance. Inventory shrinkage is the reduction in the inventory balance due to theft or waste. Investigating the causes of inventory shrinkage can help unravel fraud schemes. Although some amount of inventory shrinkage is routine and expected in the normal course of business, abnormal shrinkage or a pattern of shrinkage are red flags. Normal inventory shrinkage, a random event, should affect all items of the inventory and not just a particular item. Moreover, there should not be any detectable pattern or trend of inventory shrinkage. Such patterns and trends, if identified through statistical procedures, require further investigation.

Documenting inventory shrinkage can be difficult for many organizations due to their accounting systems for inventory. There are two common methods to account for inventory: the perpetual system and the periodic system. In the perpetual method, every transfer-in and sale of inventory is recorded. On the other hand, in the periodic method, the inventory balance is estimated or computed at periodic intervals. Usually only one of the two inventory systems is used in an organization. To effectively detect inventory shrinkage, a perpetual system has to be implemented to maintain running totals of the inventory that can be verified periodically through physical observation. Discrepancies between the two balances indicate the amount of inventory shrinkage.

Perpetrators have been known to conceal inventory shrinkage by altering either the perpetual inventory records or managing the physical count. A critical internal control procedure, segregation of duties, prevents the perpetrator from altering records to conceal the theft of inventory. For example, an item could be reported as broken or perished prior to its theft by the perpetrator, thus the records are adjusted prior to the actual theft of the inventory item. In the most egregious cases, the inventory items are replaced by empty boxes, giving the illusion of inventory. The fraud case of Crazy Eddie, an electronics superstore in the New York metro area, was an infamous occurrence of inventory padding (see Exhibit 1.1).

Exhibit 1.1 Fraud at Crazy Eddie

Crazy Eddie was an electronic store chain that operated in the New York metro area. It started as a private company in the 1970s and went public in 1984. Although fraud was rampant from its inception, the schemes were modified when the company decided to raise public capital. As a private company it committed insurance fraud and payroll tax fraud. However, in preparation for going public, it primarily exploited timing differences to overstate revenue, inflated inventory to understate cost of goods sold, concealed liabilities and other expenses to understate operating expenses, and resorted to inaccurate disclosures in its financial statements for cover up. As a result of overstating revenue and understating cost of goods sold and other operating expenses, the company reported much higher income than it actually earned. On the flip side, by overstating inventory and understating liabilities, it presented a much more appealing financial position on the balance sheet.

One of the many ways that Crazy Eddie was able to conceal the massive fraud for so long was by developing a tightly knit company culture where most senior employees were either family or friends of the family. Every employee was considered part of the extended family. The initial motivation for fraud, when the company was private, was to pay the employees off the books so that they could evade income and payroll taxes. However, to be able to pay cash off the books, the company needed cash off the books. This was achieved by skimming cash sales and thereby also avoiding paying the sales tax. Thus, by skimming sales to pay employees off the books, Crazy Eddie was able to pocket the 8% sales tax he collected from customers and keep his labor cost lower than his competitions' by paying less to his employees and assisting them to avoid paying income and Social Security taxes.

After the company went public, the objective for committing fraud changed.[8] The family was no longer interested in tax evasion by skimming sales and reporting lower income. Instead they wanted to sell millions of dollars of stock at inflated share prices. To support a high stock price, the company had to find ways to inflate earnings. So the nature of the fraud adapted from understating revenue and income to overstating revenue and income. To inflate reported income, the company not only overstated revenue but understated cost of sales and other operating expenses. The management exploited the auditor's usage of sampling to inflate inventory counts. The employees of the company volunteered to do the auditor's tedious job of counting inventory items, which were stacked high and deep in the warehouse. As a result, even though the physical count of inventory was technically being taken, the inventory padding schemes of management were still effective in concealing the massive fraud.

Inventory shrinkage, even when carefully concealed, can be detected by comparing gross margin percentages across various stores. The location that is stealing inventory and reporting it as either sold or spoiled would have an unusually lower gross margin percentage relative to other stores. Furthermore, conducting a trend analysis over multiple periods would lead to early detection of changes in patterns due to inventory theft. Statistical methods, discussed later in the book, can be used to conduct such analysis.

Embezzlement by Management

Three senior officers at Tyco International were convicted of embezzling millions of dollars from the company. The CEO and two other top officials manipulated two corporate loan programs to obtain funds to sponsor their lavish lifestyles and to give themselves unauthorized bonuses. Subsequently, in order to conceal their theft, they would forgive each other's loans and thereby steal the funds from the company.

The formal charges filed against the officers by prosecutors were for stealing $170 million in company loans and other funds and obtaining more than $430 million through the fraudulent sales of securities. The SEC filed a separate but related charge for their failing to disclose the multi-million dollar low interest or interest-free loans they took from the company and in some cases never repaid. It charged the officers with "treating Tyco as their private bank, taking out hundreds of millions of dollars of loans and compensation without ever telling investors."

1.5 Cyber-crime

In a speech delivered at the American Institute of Certified Public Accountants National Conference on Fraud and Litigation Services in 2007, an Associate Deputy Director of the FBI, Mr. Joseph Ford best described the increased threat of financial crimes in the age of globalization and the Internet. He characterized the Internet "as much a conduit for crime as it is for commerce." While opening up new avenues of crime in computer hacking, the Internet facilitates a wide range of traditional criminals that include mobsters, drug traffickers, corporate fraudsters, spies, and terrorists.

The critical challenge that cyber-crime imposes is that unlike traditional crime, the physical presence of the criminal at the scene of the crime is not necessary. In the traditional days of bank robbery, the robber had to be present at the heist and took the risk of being caught and dragged away in cuffs. However, in the age of the Internet, a bank robber could commit a crime of much greater magnitude without ever even having to set foot in the bank. They usually operate from remote locations, under the umbrella of legal protection provided by a different jurisdiction than where the crime is being committed. These criminals exploit the weaknesses in internal controls to commit their crimes. The risk they face is that their plans might be thwarted, but usually the identification, prosecution, or incarceration of such criminals is complicated due to the involvement of multiple jurisdictions. According to the FBI, a significant percentage of cyber-crimes originate in Romania, but the victims are in the United States or in other western nations. These criminals, formerly employed by the now defunct intelligence apparatus of Romania, have targeted money transmission agencies. Additionally, one type of securities fraud, known as a "pump and dump" scheme, has been traced back to criminals in Latvia and Estonia who hack into accounts of online brokerage companies. Although these crimes originate and are committed overseas, the consequences are felt in the United States and adversely impact U.S. investors.

Consequently, the significant threat encountered by banks and other financial institutions is no longer that of an armed robber engaging in a heist, but that of a cyber-criminal sitting in the comfort of his home at a remote location. The weapon of choice for such criminals is not a firearm as used in traditional bank robberies, but a few keystrokes on their computers. Consequently, the analysis of evidence of such crime doesn't require evaluation of fingerprints or ballistics experts. They require a financial analysis of the money trail and hence the expertise of accountants.

1.6 Chapter Summary

Our collective knowledge of fraud schemes and occurrences is limited by those that have been detected and prosecuted with success. Hence, sophisticated fraud schemes currently undetected by auditors, regulators, or law enforcement officials, might be rampant in society, but our current technology and methods are not sufficiently calibrated to detect them. Because we operate under limited knowledge and fraud perpetrators are a step ahead in conniving new schemes, it is imperative for fraud examiners to be fully cognizant of the schemes that have been unraveled and be equipped with tools to prevent and detect such instances in the future. That is, after a fraud scheme has been discovered, the information should be disseminated as widely as possible so that others can take precautionary steps and reduce their vulnerability to such threats. It is toward this objective that this book began with a brief description of commonly used fraudulent schemes by employees, management, and third parties.

Although extant literature and books on forensic accounting have focused on detecting and preventing employee and management fraud in an organization, cyber-crime is a growing threat. Businesses, especially financial institutions, are increasingly vulnerable to cyber-crime. As computing technology makes advances and the use of Internet for legitimate business purposes explodes, it becomes increasingly difficult to monitor Internet traffic and identify suspicious activities. Additionally, though precautionary measures can prevent loss, the perpetrators of cyber-crime are rarely prosecuted with success and therefore are free to continue to devise new schemes to defraud victims. That is, while the perpetrators of a failed robbery would be prosecuted and incarcerated (thereby limiting their ability to perfect their crime), the foiled attempts of cyber-criminals are not prosecuted due to jurisdictional constraints, and these criminals gain valuable knowledge about the cyber-security systems and potentially use it to beat the system. Thus there is now a more critical need to be proactive in developing better and impregnable *cyber-shields* to protect against cyber-crime. The statistical techniques presented in subsequent chapters provide the necessary foundation to develop sophisticated investigative tools to prevent and detect not just employee and management fraud but also to deter cyber-crime.

1.7 Endnotes

1. In its *Financial Crimes Report to the Public*, the FBI summarizes its operations for the two-year period ending on September 2011. The entire report is available at http://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011.
2. *Washington Post* in July 2010 estimated the losses to be $21.2 billion, http://voices.washingtonpost.com/economy-watch/.
3. The U.S. Securities and Exchange Commission describes the warning signs of a Ponzi scheme at http://www.sec.gov/answers/ponzi.htm#RedFlags.
4. For a detailed discussion of Lehman's use of Repo 105 transactions, see Caplan, Dennis H., Saurav K. Dutta and David J. Marcinko, "Lehman on the Brink of Bankruptcy: A Case about Aggressive Application of Accounting Standards." *Issues in Accounting Education* 27, no. 2 (2012): 441-459; or Dutta, Saurav K., Dennis Caplan and Raef Lawson, "Lehman's Shell Game: Poor Risk Management." *Strategic Finance*, 2010 (August).

5. Available at http://lehmanreport.jenner.com/. Volume III of the Examiner's Report is particularly relevant to the issues raised in this case.
6. *Principles of Fraud Examination,* Joseph T. Wells, 2010, John Wiley and Sons Publishing.
7. Lapping is one of the most common concealment techniques (*Principles of Fraud Examination* by J. Wells, p. 66).
8. A thorough discussion of the fraudulent scheme at Crazy Eddie is presented in *Contemporary Auditing: Real Issues and Cases* by Michael Knapp, Southwestern Publishing.

This page intentionally left blank

Index

A

a-priori probability, 111

acceptance sampling, 191

accounting rules, internal controls to ensure adherence to, 42

ACFE (Association of Certified Fraud Examiners), 11

Adelphia, 25

ADRs (American Depository Receipts), 36

adverse selection, 31

AEP Energy Services, 25

agency theory, 31

AICPA (American Institute of Certified Public Accountants), 27-28, 67

Albrecht, Steve, xvi

alternative hypothesis, 237

Ambani, Anil, 37

Ambani, Dhirubhai, 37

Ambani, Mukesh, 37

anticipated error rates, 226-228

application controls, 43

AS 5 (Auditing Standard No. 5), 67

assets
  internal controls for safeguarding of organizational, 41
  misappropriation of, 80

association analysis, 93-95

association rules, 94

AU (Audit Sampling) 350, 188

audit committee
  financial reporting process, role and responsibilities in, 70-75
  international guidelines, 72-73
  oversight function, 74-75
  overview, 34
  tips for, 75

auditors
  external auditors, role and responsibilities in financial reporting process of, 66-68
  hypergeometric distribution, use of, 145
  internal auditors, role and responsibilities in financial reporting process of, 78-80

audits
  expectations gap in, 65-66
  for public companies, history of requirement for, 61-62
  sampling
    acceptance, 191
    discovery, 190
    DUS (dollar unit sampling), 191
    overview, 188-190
    PPS (probability proportional to size), 191

B

back-up procedures, 44

balance sheet fraud, 8-9

batch control totals, 43

Bayes' rule, 116-122

belief system, 40

Bingham, James, 83

binomial distribution
- Excel used for statistical computations, 147
- mean (expected value), 130-131
- normal distribution, expressed as, 171
- overview, 128-132
- standard deviation, 131-132
- symmetrical, 132

Blue Ribbon Panel, 34

BOD (Board of Directors)
- audit committee, 34
- ethics of, 70
- financial reporting process, role and responsibilities in, 68-71
- oversight function, 68-69
- overview, 32-34

Boolean vectors, 94

boundary system, 40

Bush, George W., 24

C

Cadbury Report, 33

Cendant, 25

census, 180-181

Center of Audit Quality, 65, 77

Central Limit Theorem, 158, 199-200

CEO (Chief Executive Officer)
- BOD, influence on, 34
- perquisites and related party transactions, 56

certifications for forensic accountants, 26

Certified Public Accountant (CPA), 26

CFE (Certified Fraud Examiner), 26

CFF (Certified in Financial Forensics), 26

Chebycheff's inequality, 169

CIA (Certified Internal Auditor), 26

Citigroup, 2

cluster analysis, 96-97

cluster sampling, 185

coefficient of determination, 236, 241

combinatorial probability, 141

complement of event, 111

Comverse, 25

conditional probability, 111-117. *See also* Bayes' rule

confidence intervals
- for large sample when population standard deviation is known, 205-209
- for large sample when population standard deviation is unknown, 209-211
- overview, 203-205, 238-239
- for proportions, 212-214
- scientific calculator used to compute, 217
- for small samples, 211-212

  - steps for constructing, 215-216
  - tolerable error, 220-221

confidence levels and determining sample size, 223, 226-228

confidentiality for whistleblowers, 82

confirming evidence, 108-109

consistent estimators, 202

continuous probability distributions
  - binomial distribution expressed as a normal distribution, 171
  - Chebycheff's inequality, 169
  - cumulative distribution function, 150-156
  - exponential distribution, 172-173
  - joint distribution of continuous random variables, 173-176
  - normal probability distribution, 157-170
  - overview, 149-156
  - probability distribution function, 150-153
  - uniform (rectangular) probability distribution, 151-153, 156-157

control activities, 47, 50

control environment, 47, 49-50

Cooper, Cynthia, 78

corporate fraud
  - earliest instance of, 61-62
  - FBI's role in detecting, 26
  - investigations, 5
  - overview, 5
  - whistleblowers, groups who have been, 81

corporate governance
  - agency theory, 31
  - BOD (Board of Directors), 32-34
  - in developed economies, 33-34
  - in emerging economies, 35-39
  - organizational controls, 39-41
  - overview, 31-33

corrective controls, 42

correlation
  - overview, 233-234
  - sampling error, 242

correlation coefficient, 234

corruption, 80

COSO (Treadway Commission's Committee of Sponsoring Organization) framework on internal controls, 45-52, 57-58

CPA (Certified Public Accountant), 26

Crazy Eddie, 17

Cressey, Donald, xvi

cumulative distribution function, 150-156

curvilinear relationships, 233, 243

cyber-crime, 16-18

cyber-security, use of Poisson distribution in, 140

D

data classification, 92

data encryption, 44

data mining
  - association analysis, 93-95
  - cluster analysis, 96-97

  - data classification, 92
  - money laundering, detection of, 100-103
  - outlier analysis, 98-100
  - overview, 89-91

deficiency in internal controls, 51

Deloitte Forensic Center, 75

detective controls, 42

determining sample size
  - anticipated error rates, for differing, 226-228
  - confidence, for differing levels of, 223, 226-228
  - overview, 219
  - precision, for differing levels of, 223, 226-228
  - for proportions, 225-228
  - when population deviation is known, 220-221
  - when population deviation is unknown, 222-225

developed economies, corporate governance in, 33-34

diagnostic control system, 41

discovery sampling, 190

discrete probability distributions
  - binomial distribution
    - *Excel used for statistical computations, 147*
    - *mean (expected value), 130-131*
    - *overview, 128-132*
    - *standard deviation, 131-132*
    - *symmetrical, 132*
  - hypergeometric distribution
    - *auditors' use of, 145*
    - *Excel used for statistical computations, 147*
    - *mean (expected value), 142*
    - *multilocation inventory audit example, 142-145*
    - *overview, 140-142*
    - *standard deviation, 142*
  - mean (expected value), 126-127
  - overview, 126
  - Poisson distribution
    - *application of, 137*
    - *cyber-security, use in, 140*
    - *Excel used for statistical computations, 147*
    - *mean (expected value), 137*
    - *overview, 132-136*
    - *standard deviation, 137*
    - *variance, 137*
  - standard deviation, 127

document matching, 44

Dodd-Frank Wall Street Reform and Consumer Protection Act, 23, 33, 80

DOJ (Department of Justice) and prosecution of criminals committing fraud, 24-25

DUS (dollar unit sampling), 191

Dyck, A., 81

Dynegy, 25

E

earnings management, 77

edit checks, 44

efficiency, internal controls promoting, 42

efficient estimators, 202

embezzlement, 16, 54

emerging economies, corporate governance in, 35-39

employee collusion, 94-95

employee detection of management fraud, 82

employee fraud
  embezzlement, 16, 54
  fraudulent write-offs, 13
  ghost employees, 14-15
  inventory shrinkage, 15-16
  lapping, 13
  overview, 11
  shell companies, 13-14
  skimming, 12

Enron, 14, 24, 188-189

Enterasys, 24

errors
  anticipated error rates, 226-228
  random error, 232-233, 239-241
  sampling error, 197, 242
  standard error, 236
  tolerable error, 220-221
  Type I error, 238
  Type II error, 238

estimation of population parameters, 200-203

ethical culture, 27-28

ethics of BOD, 70

events, 111

evidence
  confirming, 108-109
  information and, 110
  probative value of, 113-117
  schematic representation of, 108-109
  smoking gun, 188-189

Excel used for statistical computations
  binomial distribution, 146
  hypergeometric distribution, 146-147
  Poisson distribution, 147

expectations gap in accounting profession, 65-66

exponential distribution, 172-173

external audit of internal controls, 45-46

external auditors, role and responsibilities in financial reporting process of, 66-68

F

family relationships in emerging economies, 35-39

FCPA (Foreign Corrupt Practices Act), 75

Federal Civil False Claims Act, 82

financial firm failures, 63

financial institution fraud, 6

Financial Reporting Council of the U.K., 72

financial reporting process as collective effort
  audit committee, 70-75
  Board of Directors, 68-71
  external auditors, 66-68
  internal auditors, 78-80
  management, 75-77
  overview, 63-66
  whistleblower, role of, 80-84

firewalls, 44

Ford, Joseph, 16

forensic accountants
  certifications, 26
  qualifications required for, 26
  responsibilities of, 26
Forensic Analytics **(Nigrini), xvi**
Fornelli, Cynthia, 65
fraud
  characteristics of, 3
  corporate
    earliest instance of, 61-62
    FBI's role in detecting, 26
    investigations, 5
    overview, 5
    whistleblowers, groups who have been, 81
  cyber-crime, 16-18
  DOJ prosecution of criminals committing, 24-25
  earliest instance of, 61-62
  employee
    embezzlement by management, 16
    fraudulent write-offs, 13
    ghost employees, 14-15
    inventory shrinkage, 15-16
    lapping, 13
    overview, 11
    shell companies, 13-14
    skimming, 12
  financial institution, 6
  health care, 6
  investigations of, 4-5
  management
    balance sheet fraud, 8-9
    employee detection of, 82
    HealthSouth, 9-10
    inflating revenue, schemes for, 7
    Lehman, 10-11
    motivation and opportunity for, 77
    overview, 7-9, 11
    understating expenses, schemes for, 7-8
    WorldCom, 9
  mortgage, 6
  overview, 3-7
  securities, 5
  types of, 3
Fraud Triangle **(Cressey), xvi**
fraudulent write-offs, 13

G

Galleon Management, 71
Gaussian probability distribution. ***See* normal probability distribution**
general internal controls, 43
ghost employees, 14-15
Goldman Sachs, 71, 109
Gosset, W.S., 212
Groupon, 45-46

H

health care fraud, 6
HealthSouth, 9-10
Homestore, 25
HSBC, 100
hypergeometric distribution
  auditors' use of, 145
  Excel used for statistical computations, 147

  - mean (expected value), 142
  - multilocation inventory audit example, 142-145
  - overview, 140-142
  - standard deviation, 142

I

ICFRs (internal controls over financial reporting), 74

inflating revenue, schemes for, 7

information
  - and communication, 48, 50
  - and evidence, 110

infoUSA Inc., 56

inside whistleblowers, 83-82

insider trading, 71, 109

Institute of Internal Auditors, 78

interactive control system, 41

internal auditors, roles and responsibilities in financial reporting process, 78-80

internal controls
  - application, 43
  - benefits of, 52
  - common, 43-44
  - corrective, 42
  - COSO framework on, 45-52
  - costs of, 52-53, 58
  - deficiency in, 51
  - detective, 42
  - external audit of, 45-46
  - general, 43
  - legislation on, 58
  - limitations of, 53-56
  - management override, 55-56
  - outsourcing and, 51
  - overview, 41-42
  - preventive, 42

international guidelines for audit committee, 72-73

interval estimate, 203. ***See also*** **confidence intervals**

inventory shrinkage, 15-16

investigations of fraud, 4-5

J

joint distribution of continuous random variables, 173-176

joint event, 111

joint probability, 106, 112-113, 115

judgment (nonrandom) sampling, 181-182, 187-189

K

Ka-Shing, Li, 38

Koss Corporation, 54

Kreuger and Toll, 62

L

lapping, 13

large sample
  - confidence intervals when population standard deviation is known, 205-209
  - confidence intervals when population standard deviation is unknown, 209-211

Lee, Matthew, 83
legislation
  Dodd-Frank Wall Street Reform and Consumer Protection Act, 23, 33, 80
  on internal controls, 58
  overview, 21
  SOX (Sarbanes-Oxley Act of 2002), 22-23, 33, 76
Lehman Brothers, 10-11, 83
***Levers of Control* (Simons), 39**
Levitt, Arthur, 70
likelihood ratio, 116-117
linear relationship, 233
lockbox system, 44
logarithmic regression model, 243

M

Madoff, Bernie, 2
major nonconformity, 51
management
  financial reporting process, role and responsibilities in, 75-77
  internal controls, override of, 55-56
  policies, internal controls ensuring adherence to, 42
management fraud
  balance sheet fraud, 8-9
  employee detection of, 82
  HealthSouth, 9-10
  inflating revenue, schemes for, 7
  Lehman, 10-11
  motivation and opportunity for, 77
  overview, 7-9, 11
  understating expenses, schemes for, 7-8
  WorldCom, 9
marginal probability, 111, 115
mass marketing fraud, 7
material weakness, 51, 58
mathematical notations and formulae for probability, 111
McKesson and Robbins, 62
mean (expected value)
  binomial distribution, 130-131
  hypergeometric distribution, 142
  normal probability distribution, 158-159
  overview, 126-127
  Poisson distribution, 137
  uniform (rectangular) probability distribution, 157
Mercury Finance, 25
Merrill Lynch, 189
minor nonconformity, 51
money laundering
  detection of, 100-103
  overview, 100
  settlements in money laundering charges, recent, 100
monitoring activities, 48, 51
moral hazard, 33
Morse, A., 81
mortgage fraud, 6
multilocation inventory audit example for hypergeometric distribution, 142-145
multiple regression models, 244-245
mutual exclusivity, 106

N

Nigerian email/letter scheme, 6-7

Nigrini, Mark, xvi

nonparamethic outlier analysis, 99

nonrandom sampling, 181-182, 187-189

normal probability distribution
- binomial distribution expressed as, 171
- mean, 158-159
- overview, 157-170
- scientific calculator used to compute probabilities, 178
- standard deviation, 158-159
- standard normal distribution table, 162
- testing for normality, 168-170

normal probability plot, 169-170

null hypothesis, 237-238

numbered documents, 43

numeric value, 111

O

objective probability, 111

OLS (Ordinary Least Squares) regression, 234-235, 239-241

organizational controls, 39-41

organizational culture, 39

outlier analysis, 98-100

outsourcing and internal controls, 51

oversight function
- audit committee, 74-75
- BOD, 68-69

P

parametric outlier analysis, 99

PCAOB (Public Company Accounting Oversight Board), 22, 63, 67

perquisites and related party transactions, 56

physical security, 44

PNC, 25

point estimate, 203

Poisson distribution
- application of, 137
- cyber-security, use in, 140
- Excel used for statistical computations, 147
- mean (expected value), 137
- overview, 132-136
- standard deviation, 137
- variance, 137

polynomial regression models, 243-244

Ponzi, Charles, 1

Ponzi scheme, 1-2, 62

population deviation is known, determining sample size when, 220-221

population deviation is unknown, determining sample size when, 222-225

population parameters
- estimation of, 200-203
- generalizing sample data to, 196-199
- interval estimate, 203
- point estimate, 203

posterior probability, 121-122

PPS (probability proportional to size) sampling, 191
precision levels, determining sample size for differing, 223, 226-228
prediction intervals, 238-239
President's Corporate Fraud Task Force, 24
preventive controls, 42
principal-agent conflict, 35
principal-principal relationship, 36
probabilistic linear models, 232-233
probability
  a-priori, 111
  Bayes' rule, 116-122
  combinatorial, 141
  concepts and terminology, 106
  conditional, 111-115
  distributions, 125
  information and evidence, 110
  joint, 106, 112-113, 115
  likelihood ratio, 116-117
  marginal, 111, 115
  mathematical notations and formulae, 111
  mutual exclusivity, 106
  numeric value, 111
  objective, 111
  overview, 106
  posterior, 121-122
  probative value of evidence, 113-117
  sample space, 106
  schematic representation of evidence, 108-109
  subjective, 111
  Venn diagrams, 106-109
probability distribution function, 150-153
probative value of evidence, 113-117
Proctor and Gamble, 71
professional guidance for internal auditors, 78-79
proportions
  confidence intervals, 212-214
  determining sample size, 225-228
Public Company Accounting Oversight Board (PCAOB), 22, 63, 67

Q

qualifications required for forensic accountants, 26
Qwest, 25

R

random error, 232-233, 239-241
random sampling
  cluster, 185
  overview, 181-184
  selection with replacement, 182-183
  selection without replacement, 182-184
  stratified, 184-185
  systemic, 184

reconciliation of accounts, 43

recording of business transactions, internal controls for accuracy in, 41

Refco, 25

regression
- alternative hypothesis, 237
- coefficient of determination, 236, 241
- confidence intervals, 238-239
- logarithmic regression model, 243
- multiple regression models, 244-245
- null hypothesis, 237-238
- OLS regression, 234-235, 239-241
- overview, 234-236
- polynomial regression models, 243-244
- prediction intervals, 238-239
- prediction using, 238-239
- random error, 232-233, 239-241
- sampling error, 242
- test of significance, 237-238
- Type I error, 238
- Type II error, 238

regression line, 234-236

regulation
- audits for public companies, history of requirement for, 61-62
- DOJ, fraud prosecution by, 24-25
- internal controls for compliance with, 42
- overview, 21

Reliance Industries, 37

Repo 105, 10-11, 83

"Responsibility for Preventing and Detecting Financial Reporting Fraud" (SEC panel discussion), 65-66

revenue, schemes for inflating, 7

risk assessment
- with COSO framework, 57-58
- overview, 47, 50

risk-based approach to audit procedure, 67

Romania, cyber-crime in, 18

round trip transaction, 189

S

sample mean, 198-199

sample space, 106

sample standard deviation, 198-199

sampling
- audit
  - *acceptance, 191*
  - *discovery, 190*
  - *DUS (dollar unit sampling), 191*
  - *overview, 188-190*
  - *PPS (probability proportional to size), 191*
- census compared, 180-181
- determining sample size
  - *anticipated error rates, for differing, 226-228*
  - *confidence, for differing levels of, 223, 226-228*
  - *overview, 219*
  - *precision, for differing levels of, 223, 226-228*

        for proportions, 225-228
        when population deviation is known, 220-221
        when population deviation is unknown, 222-225
    judgment (nonrandom), 181-182, 187-189
    overview, 179-181
    random
        cluster, 185
        overview, 181-184
        selection with replacement, 182-183
        selection without replacement, 182-184
        stratified, 184-185
        systemic, 184
sampling error, 197, 242
SAS (Statement of Auditing Standards) No. 99, 27-28, 67
scatter plot, 233
schematic representation of evidence, 108-109
scientific calculator
    for confidence intervals, 217
    for normal probability distribution, 178
    for OLS regression, 247
SEC (Securities and Exchange Commission)
    overview, 5
    SOX, study and clarification of, 23
Securities and Exchange Act of 1933, 70
securities fraud, 5
segregation of duties, 43
settlements in money laundering charges, recent, 100
shareholders in emerging economies, controlling, 35-39
shell companies, 13-14
shopping cart analysis, 93
significant deficiency, 51
Simons, Robert, 39
simple event, 111
skimming, 12
small samples, confidence intervals for, 211-212
smoking gun evidence, 188-189
SOX (Sarbanes-Oxley Act of 2002), 22-23, 33, 76
SSE (sum of the squared errors), 234
Standard Chartered PLC, 100
standard deviation
    binomial distribution, 131-132
    hypergeometric distribution, 142
    normal probability distribution, 158-159
    overview, 127
    Poisson distribution, 137
    uniform (rectangular) probability distribution, 157
standard error, 236
standard normal distribution table, 162
Stanford International, 2

statistical inference from sample information
- Central Limit Theorem, 199-200
- confidence intervals
  - *for large sample when population standard deviation is known, 205-209*
  - *for large sample when population standard deviation is unknown, 209-211*
  - *overview, 203-205*
  - *for proportions, 212-214*
  - *scientific calculator used to compute, 217*
  - *for small samples, 211-212*
  - *steps for constructing, 215-216*
- overview, 195-196
- population parameters
  - *estimation of, 200-203*
  - *generalizing sample data to, 196-199*
  - *interval estimate, 203*
  - *point estimate, 203*
- sample mean, 198-199
- sample standard deviation, 198-199
- sampling error, 197

stratified sampling, 184-185

Student t-distribution, 212

subjective probability, 111

sufficient estimator, 202

symmetrical binomial distribution, 132

system/process documentation, 43

systemic sampling, 184

T

t-distribution, 212

test of significance, 237-238

testing for normality, 168-170

tolerable error, 220-221

Treadway Commission's Committee of Sponsoring Organization (COSO) framework on internal controls, 45-52, 57-58

Tyco International, 16

Type I error, 238

Type II error, 238

U

unbiased estimators, 202

unbundling, 6

understating expenses, schemes for, 7-8

uniform (rectangular) probability distribution, 151-153, 156-157

V

Valukas, Anton, 10

Vanda Computers, 38

variance
- Poisson distribution, 137
- uniform (rectangular) probability distribution, 157

Venn diagrams, 106-109

W

Wells, Joseph, xvi

whistleblowers

  confidentiality for, 82

  costs to, 83-82

  financial reporting process, role and responsibilities in, 80-84

  groups who have been, 81

  inside, 83-82

"Who Blows the Whistle on Corporate Fraud?" (Dyck, Morse, and Zingales), 81

WorldCom, 9, 25, 78

X

Xerox, 83

Z

Zingales, L., 81