

PRINCIPLES OF FRAUD EXAMINATION

FOURTH EDITION



JOSEPH T. WELLS

WILEY

*PRINCIPLES OF
FRAUD EXAMINATION*

*PRINCIPLES OF FRAUD
EXAMINATION*

FOURTH EDITION

JOSEPH T. WELLS, CFE, CPA

WILEY

VICE PRESIDENT AND PUBLISHER	George Hoffman
EXECUTIVE EDITOR	Joel Hollenbeck
CONTENT EDITOR	Brian Kamins
EDITORIAL ASSISTANT	Rebecca Costantini
Sr. MARKETING MANAGER	Karolina Zarychta Honsa
SENIOR PRODUCTION MANAGER	Janis Soo
ASSOCIATE PRODUCTION MANAGER	Joel Balbin
PRODUCTION EDITOR	Eugenia Lee
COVER DESIGNER	Kenji Ngieng
COVER PHOTO	© Thinkstock/iStock

This book was set in 10/12pt TimesLTStd by Laserwords Private Limited, Chennai, India and printed and bound by Courier Kendallville. The cover was printed by Courier Kendallville.

This book is printed on acid free paper.

Founded in 1807, John Wiley & Sons, Inc. has been a valued source of knowledge and understanding for more than 200 years, helping people around the world meet their needs and fulfill their aspirations. Our company is built on a foundation of principles that include responsibility to the communities we serve and where we live and work. In 2008, we launched a Corporate Citizenship Initiative, a global effort to address the environmental, social, economic, and ethical challenges we face in our business. Among the issues we are addressing are carbon impact, paper specifications and procurement, ethical conduct within our business and among our vendors, and community and charitable support. For more information, please visit our website: www.wiley.com/go/citizenship.

Copyright © 2014, 2011, 2008, 2005 Association of Certified Fraud Examiners, Inc. All rights reserved. Published by John Wiley & Sons, Inc., Hoboken, New Jersey. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc. 222 Rosewood Drive, Danvers, MA 01923, website www.copyright.com Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774, (201)748-6011, fax (201)748-6008, website <http://www.wiley.com/go/permissions>

Evaluation copies are provided to qualified academics and professionals for review purposes only, for use in their courses during the next academic year. These copies are licensed and may not be sold or transferred to a third party. Upon completion of the review period, please return the evaluation copy to Wiley. Return instructions and a free of charge return shipping label are available at www.wiley.com/go/returnlabel. If you have chosen to adopt this textbook for use in your course, please accept this book as your complimentary desk copy. Outside of the United States, please contact your local representative.

To order books or for customer service, please call 1-800-CALL WILEY (225-5945).

ISBN-13: 978-1-118-92234-7 (pbk.)

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

*To the memory of my father,
Coyle A. Wells (1906–1962),
and my mother,
Vola D. Wells (1910–1990).*

FOREWORD

It is a pleasure to write the foreword for *Principles of Fraud Examination*, a book authored by my friend, Dr. Joseph T. Wells. I have known Joe for over 20 years. While most students, practitioners, and academics know him as the founder and chairman of the Association of Certified Fraud Examiners, I know Joe as a friend, as one who has influenced my thinking, knowledge, and research about fraud, and as a person who is one of the most thorough, ambitious, and thoughtful fraud researchers I have ever met. And, as you will see from reading this book, Dr. Wells is an excellent communicator who can make numerous fraud theories and schemes easy to understand.

Joe is a prolific writer. For several years, he authored a fraud-related article in nearly every issue of the *Journal of Accountancy*, and he has written many other books and articles. Dr. Wells' work has won numerous awards. He has also written and produced more than a dozen fraud-related videos that are an integral part of nearly every accounting, auditing, and fraud curriculum in the United States.

It is my opinion that Joseph T. Wells has made a greater contribution to the prevention, detection, and investigation of fraud than any person in the world. Because of his work in fraud education and research and his vision in organizing the ACFE, there are tens of thousands of people who have a better understanding of fraud and who are working to reduce its cost and occurrence.

Principles of Fraud Examination provides an excellent description of the behavioral and social factors that motivate occupational offenders. It also provides an analysis and taxonomy of various kinds of frauds and cases that illustrate and help readers understand each type of fraud. The concepts described in the book are sound and are based on the most extensive empirical research ever conducted on the subject. This book is a must read for any student interested in the study of fraud.

Reading *Principles of Fraud Examination* will help you better understand the various ways fraud and occupational abuse occur, thus helping you identify exposures to loss and appropriate prevention, detection, and investigation approaches. And, as you will see, the book is written in a way that will capture and hold your attention. The numerous fraud stories and personal insights provided by Joe will have you believing you are reading for enjoyment, while in fact, you will be learning from one of the true master educators. I believe this book is destined to become one of the real classics and definitive works on the subject of fraud.

W. Steve Albrecht, PhD
Brigham Young University

PREFACE

The numerous headline-grabbing accounting scandals of recent years—Enron, WorldCom, Tyco, HealthSouth, Bernie Madoff, Lehman Brothers, and Olympus, among others—would be reason enough to study the serious issue of fraud. But the methods used in these cases are not new; they are merely variations of tried-and-true scams.

Pliny the Elder first wrote of fraud over two thousand years ago when he described the adulteration of wine by crooked merchants in Rome. Since that time, fraud has become an increasingly serious issue. Now, in the information age, it can threaten the very underpinnings of our economy.

Accountants have historically had an important role in the detection and deterrence of fraud. But fraud, as you will read in the following pages, is much more than numbers. It involves complex human behaviors such as greed and deception, factors that are difficult to identify and quantify. In short, books, records, and computers don't commit fraud—people do.

Understanding why and how “ordinary” people engage in fraudulent behavior has been my life's work. Like many readers of this book, I began my professional career as an accountant. But after two years toiling in the ledgers of one of the large international accounting firms, I realized that auditing was not my calling. In search of adventure, I became a real-life, gun-toting FBI agent.

The truth is that I was more often armed with my Sharp model QS-2130 calculator than my trusty Smith & Wesson model 60 five-shot stainless-steel revolver. Sure, there were the occasional gun battles. But most of the time I was waging war against corporate titans and crooked politicians. In the decade I spent with the Federal Bureau of Investigation, I learned a difficult and humbling lesson: My accounting education and training had not adequately prepared me for fighting fraud. But the status of antifraud education since then has begun to change, little by little.

To assist today's accounting students, *Principles of Fraud Examination* is written to provide a broad understanding of fraud—what it is and how it is committed, prevented, detected, and resolved.

Understanding how fraud is committed is paramount to preventing and detecting it. I've learned that in the 30-plus years since I carried a badge and gun. After I left the FBI in the early 1980s, I offered fraud investigation services to major corporations. Then, in 1988, I became the chairman of the Association of Certified Fraud Examiners, the world's largest antifraud organization. It is a position I still hold. In that capacity, I write, educate, and research fraud issues.

This work has its genesis in my fifth book, *Occupational Fraud and Abuse*, first published in 1997. At the time, I was intrigued by the definition of *fraud* as classically set forth in *Black's Law Dictionary*:

All multifarious means which human ingenuity can devise, and which are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth. It includes all surprise, trick, cunning or dissembling, and any unfair way which another is cheated.

The definition implied to me that there was an almost unlimited number of ways people could think up to cheat one another. But my experience told me something else: After investigating and researching thousands of frauds, they seemed to fall into definite patterns. If we could somehow determine what those patterns were and in what frequency they occurred, it would aid greatly in understanding and ultimately preventing fraud. And since so much fraud occurs in the workplace, this particular area would be the starting point.

So I began a research project with the aid of more than 2,000 Certified Fraud Examiners. They typically work for organizations in which they are responsible for aspects of fraud detection and deterrence. Each CFE provided details on exactly how their organizations were being victimized from within. That information was subsequently summarized in a document for public consumption, the *Report to the Nation on Occupational Fraud and Abuse*. The first Report was issued in 1996. Since then, it has been updated six times, the most recent being in 2012.

Rather than an unlimited number of schemes, the reports have concluded that occupational fraud and abuse can be divided into three main categories: asset misappropriation, corruption, and fraudulent statements. From the three main categories, several distinct schemes were identified and classified; they are covered in detail herein.

Principles of Fraud Examination begins by providing an understanding of fraud examination methodology. Thereafter, it sets forth the schemes used by executives, managers, and employees to commit fraud against their organizations. This 4th edition of the text also includes a chapter on frauds perpetrated against organizations by individuals outside their staff—a growing threat for many entities as commerce increasingly crosses technological and geographical borders.

Each chapter is organized similarly. The major schemes are illustrated and detailed. Statistics are provided and the schemes are flowcharted. Case studies are provided for each chapter. Prevention, detection, and investigation strategies are outlined. Finally, the chapters have essential terms, questions, and discussion issues to help you understand and retain the material you have learned.

Writing this book is not a solo venture, even though I accept responsibility for every word—right or wrong. I am deeply indebted to John Warren, JD, CFE. Without his assistance, this undertaking would have been a nearly impossible task. John is responsible for major areas, including the statistical information and analysis, writing, and editing. Special thanks are due to several key ACFE staffers who assisted me: John Gill, Andi McNeal, Catherine Lofland, Jeanette LeVie, Jim Ratley, and Jenny Carnahan.

For their assistance in helping prepare learning objectives, chapter summaries, essential terms, and discussion issues and questions, I am indebted to Linda Chase, Scarlett Farr, Kristy Holtfreter, Robert Holtfreter, Bonita Peterson, Zabiollah Rezaee, Nazik Roufaiel, and Matthew Samuelson. Mary-Jo Kranacher provided invaluable assistance in her work on Chapters 10, 11, 12, and 17.

Finally, I must thank my wife, Judy. Since I've authored 21 books, she has learned well that this endeavor is a solitary pursuit. Without her unconditional love, encouragement, and patience, these pages could not have been written.

Joseph T. Wells
Austin, Texas
March 2013

BRIEF CONTENTS

CHAPTER 1	<i>INTRODUCTION</i>	3
CHAPTER 2	<i>SKIMMING</i>	51
CHAPTER 3	<i>CASH LARCENY</i>	75
CHAPTER 4	<i>BILLING SCHEMES</i>	93
CHAPTER 5	<i>CHECK TAMPERING</i>	121
CHAPTER 6	<i>PAYROLL SCHEMES</i>	155
CHAPTER 7	<i>EXPENSE REIMBURSEMENT SCHEMES</i>	179
CHAPTER 8	<i>REGISTER DISBURSEMENT SCHEMES</i>	197
CHAPTER 9	<i>NONCASH ASSETS</i>	213
CHAPTER 10	<i>CORRUPTION</i>	239
CHAPTER 11	<i>ACCOUNTING PRINCIPLES AND FRAUD</i>	273
CHAPTER 12	<i>FINANCIAL STATEMENT FRAUD SCHEMES</i>	301
CHAPTER 13	<i>EXTERNAL FRAUD SCHEMES</i>	349
CHAPTER 14	<i>FRAUD RISK ASSESSMENT</i>	367
CHAPTER 15	<i>CONDUCTING INVESTIGATIONS AND WRITING REPORTS</i>	391
CHAPTER 16	<i>INTERVIEWING WITNESSES</i>	417
CHAPTER 17	<i>OCCUPATIONAL FRAUD AND ABUSE: THE BIG PICTURE</i>	443
APPENDIX A	<i>ONLINE SOURCES OF INFORMATION</i>	457
APPENDIX B	<i>SAMPLE CODE OF BUSINESS ETHICS AND CONDUCT</i>	467
APPENDIX C	<i>FRAUD RISK ASSESSMENT TOOL</i>	481
BIBLIOGRAPHY	511
INDEX	513

CONTENTS

CHAPTER 1 INTRODUCTION 3

Fraud Examination Methodology	5
Predication	5
Fraud Theory Approach	5
Tools Used in Fraud Examinations	6
Defining Occupational Fraud and Abuse	8
Defining Fraud	8
Defining Abuse	10
Research in Occupational Fraud and Abuse	12
Edwin H. Sutherland	12
Donald R. Cressey	13
Dr. W. Steve Albrecht	21
Richard C. Hollinger	24
The 2012 Report to the Nations on Occupational Fraud and Abuse	30
Summary	45
Essential Terms	46
Review Questions	46
Discussion Issues	47
Endnotes	47

CHAPTER 2 SKIMMING 51

Case Study: Shy Doc Gave Good Face	51
Overview	53
Skimming Data from the ACFE 2011 Global Fraud Survey	54
Skimming Schemes	55
Sales Skimming	55
Receivables Skimming	63
Case Study: Beverage Man Takes the Plunge	63
Proactive Computer Audit Tests Detecting Skimming	69
Summary	72
Essential Terms	72
Review Questions	72
Discussion Issues	73
Endnotes	73

CHAPTER 3 CASH LARCENY 75

Case Study: Bank Teller Gets Nabbed for Theft	75
Overview	77
Cash Larceny Data from the ACFE 2011 Global Fraud Survey	78

Cash Larceny Schemes	78
Larceny at the Point of Sale	78
Larceny of Receivables	81
Cash Larceny from the Deposit	82
Case Study: The Ol' Fake Surprise Audit Gets 'Em Every Time	86
Proactive Computer Audit Tests for Detecting Cash Larceny	87
Summary	88
Essential Terms	89
Review Questions	89
Discussion Issues	90
Endnotes	90

CHAPTER 4 BILLING SCHEMES 93

Case Study: Medical School Treats Fraud and Abuse	93
Overview	95
Billing Scheme Data from the ACFE 2011 Global Fraud Survey	96
Billing Schemes	97
Shell Company Schemes	97
Billing Schemes Involving Nonaccomplice Vendors	104
Pay-and-Return Schemes	104
Overbilling with a Nonaccomplice Vendor's Invoices	105
Case Study: Cover Story: Internal Fraud	106
Preventing and Detecting Fraudulent Invoices from a Nonaccomplice Vendor	108
Personal Purchases with Company Funds	108
Personal Purchases through False Invoicing	109
Personal Purchases on Credit Cards or Other Company Accounts	112
Preventing and Detecting Personal Purchases on Company Credit Cards and Purchasing Cards	114
Proactive Computer Audit Tests for Detecting Billing Schemes	114
Summary	117
Essential Terms	117
Review Questions	117
Discussion Issues	118
Endnotes	118

CHAPTER 5 CHECK TAMPERING 121

Case Study: A Wolf in Sheep's Clothing	121
--	-----

xiv CONTENTS

Overview	123
Check Tampering Data from the ACFE 2011 <i>Global Fraud Survey</i>	123
Check Tampering Schemes	123
Forged Maker Schemes	125
Forged Endorsement Schemes	130
Altered Payee Schemes	134
Concealed Check Schemes	138
Authorized Maker Schemes	139
Concealing Check Tampering	142
The Fraudster Reconciling the Bank Statement	143
Case Study: What are Friends For?	144
Re-Altering Checks	145
Falsifying the Disbursements Journal	146
Reissuing Intercepted Checks	146
Bogus Supporting Documents	147
Electronic Payment Tampering	148
Prevention and Detection	148
Proactive Computer Audit Tests for Detecting Check Tampering Schemes	149
Summary	151
Essential Terms	152
Review Questions	152
Discussion Issues	153
Endnotes	153

CHAPTER 6 PAYROLL SCHEMES 155

Case Study: Say Cheese!	155
Overview	157
Payroll Scheme Data from the ACFE 2011 <i>Global Fraud Survey</i>	157
Payroll Schemes	157
Ghost Employees	157
Falsified Hours and Salary	163
Commission Schemes	167
Case Study: The All-American Girl	169
Proactive Computer Audit Tests for Detecting Payroll Fraud	171
Summary	175
Essential Terms	176
Review Questions	176
Discussion Issues	176
Endnotes	176

CHAPTER 7 EXPENSE REIMBURSEMENT SCHEMES 179

Case Study: Frequent Flier's Fraud Crashes	179
Overview	181
Expense Reimbursement Data from the ACFE 2011 <i>Global Fraud Survey</i>	181
Expense Reimbursement Schemes	181
Mischaracterized Expense Reimbursements	182

Preventing and Detecting Mischaracterized Expense Reimbursements	184
Overstated Expense Reimbursements	185
Fictitious Expense Reimbursement Schemes	187
Multiple Reimbursement Schemes	189
Case Study: The Extravagant Salesman	190
Proactive Computer Audit Tests for Detecting Expense Reimbursement Schemes	192
Summary	193
Essential Terms	193
Review Questions	193
Discussion Issues	193
Endnotes	194

CHAPTER 8 REGISTER DISBURSEMENT SCHEMES 197

Case Study: Demotion Sets Fraud in Motion	197
Overview	199
Register Disbursement Data from the ACFE 2011 <i>Global Fraud Survey</i>	199
Register Disbursement Schemes	199
False Refunds	200
Case Study: A Silent Crime	202
False Voids	204
Concealing Register Disbursements	205
Small Disbursements	206
Destroying Records	206
Preventing and Detecting Register Disbursement Schemes	207
Proactive Computer Audit Tests for Detecting Register Disbursement Schemes	207
Summary	209
Essential Terms	209
Review Questions	209
Discussion Issues	209
Endnotes	210

CHAPTER 9 NONCASH ASSETS 213

Case Study: Chipping Away at High-Tech Theft	213
Overview	215
Noncash Misappropriation Data from the ACFE 2011 <i>Global Fraud Survey</i>	215
Noncash Misappropriation Schemes	217
Misuse of Noncash Assets	217
Unconcealed Larceny Schemes	218
Asset Requisitions and Transfers	222
Purchasing and Receiving Schemes	223
False Shipments of Inventory and Other Assets	224
Case Study: Hard Drives and Bad Luck	225
Other Schemes	228
Concealing Inventory Shrinkage	228
Altered Inventory Records	229

Fictitious Sales and Accounts Receivable	229
Write Off Inventory and Other Assets	229
Physical Padding	230
Preventing and Detecting Thefts of Noncash Tangible Assets That are Concealed by Fraudulent Support	230
Misappropriation of Intangible Assets	231
Misappropriation of Information	231
Misappropriation of Securities	232
Proactive Computer Audit Tests for Detecting Noncash Misappropriations	232
Summary	234
Essential Terms	235
Review Questions	235
Discussion Issues	236
Endnotes	236

CHAPTER 10 *CORRUPTION* 239

Case Study: Why is this Furniture Falling Apart?	239
Overview	241
Corruption Data from the ACFE 2011 <i>Global Fraud Survey</i>	241
Corruption Schemes	241
Bribery	244
Kickback Schemes	244
Overbilling Schemes	246
Bid-Rigging Schemes	249
Something of Value	255
Illegal Gratuities	256
Economic Extortion	256
Conflicts of Interest	256
Case Study: Working Double Duty	257
Purchasing Schemes	259
Sales Schemes	261
Other Conflict of Interest Schemes	262
Preventing and Detecting Conflicts of Interest	263
Anti-Corruption Legislation	263
Foreign Corrupt Practices Act	263
The United Kingdom Bribery Act	265
Scope	266
Proactive Computer Audit Tests for Detecting Corruption	267
Summary	270
Essential Terms	270
Review Questions	271
Discussion Issues	271
Endnotes	272

CHAPTER 11 *ACCOUNTING PRINCIPLES AND FRAUD* 273

Fraud in Financial Statements	273
Who Commits Financial Statement Fraud?	274

Why Do People Commit Financial Statement Fraud?	274
How Do People Commit Financial Statement Fraud?	275
Conceptual Framework for Financial Reporting	276
Economic Entity	277
Going Concern	277
Monetary Unit	278
Periodicity	278
Historical Cost	278
Revenue Recognition	278
Matching	278
Full Disclosure	278
Cost-Benefit	279
Materiality	279
Industry Practice	279
Conservatism	279
Relevance and Reliability	280
Comparability and Consistency	280
Responsibility for Financial Statements	280
Users of Financial Statements	281
Types of Financial Statements	281
The Sarbanes–Oxley Act of 2002	283
Public Company Accounting Oversight Board	287
Certification Obligations for CEOs and CFOs	289
Standards for Audit Committee Independence	290
Standards for Auditor Independence	291
Enhanced Financial Disclosure Requirements	292
Protections for Corporate Whistleblowers under Sarbanes–Oxley	293
Enhanced Penalties for White-Collar Crime	294
Financial Statement Fraud Data from the ACFE 2011 <i>Global Fraud Survey</i>	296
Frequency and Cost	296
Types of Financial Statement Fraud Schemes	296
Summary	297
Essential Terms	297
Review Questions	298
Discussion Issues	298

CHAPTER 12 *FINANCIAL STATEMENT FRAUD SCHEMES* 301

Case Study: That Way Lies Madness	301
Overview	304
Defining Financial Statement Fraud	305
Costs of Financial Statement Fraud	305
Fictitious Revenues	308
Sales with Conditions	309
Pressures to Boost Revenues	310
Red Flags Associated with Fictitious Revenues	310
Timing Differences	311
Matching Revenues with Expenses	311
Premature Revenue Recognition	312

xvi CONTENTS

Long-Term Contracts	314
Channel Stuffing	314
Recording Expenses in the Wrong Period	315
Red Flags Associated with Timing Differences	315
Case Study: The Importance of Timing	316
Concealed Liabilities and Expenses	316
Liability/Expense Omissions	317
Capitalized Expenses	318
Expensing Capital Expenditures	319
Returns and Allowances and Warranties	320
Red Flags Associated with Concealed Liabilities and Expenses	320
Improper Disclosures	320
Liability Omissions	321
Subsequent Events	321
Management Fraud	321
Related-Party Transactions	321
Accounting Changes	322
Red Flags Associated with Improper Disclosures	323
Improper Asset Valuation	323
Inventory Valuation	324
Accounts Receivable	325
Business Combinations	325
Fixed Assets	326
Red Flags Associated with Improper Asset Valuation	328
Detection of Fraudulent Financial Statement Schemes	329
AU 240—Consideration of Fraud in a Financial Statement Audit	329
Financial Statement Analysis	337
Deterrence of Financial Statement Fraud	342
Reduce Pressures to Commit Financial Statement Fraud	343
Reduce the Opportunity to Commit Financial Statement Fraud	343
Reduce Rationalization of Financial Statement Fraud	343
Case Study: All on the Surface	344
Summary	346
Essential Terms	346
Review Questions	347
Discussion Issues	347

CHAPTER 13 EXTERNAL FRAUD SCHEMES 349

Case Study: A Computer Hacker Turned Informant . . . Turned Hacker	349
Overview	351
Threats from Customers	352
Check Fraud	352
Credit Card Fraud	353
Threats from Vendors	354
How Prevalent Is Vendor Fraud?	355
Collusion among Contractors	355

Contract Performance Schemes	356
Preventing and Detecting Vendor Fraud	357
Threats from Unrelated Third Parties	357
Computer Fraud	358
Corporate Espionage	361
Why Do Companies Resort to Corporate Espionage?	361
Favorite Targets of Corporate Espionage	361
How Spies Obtain Information	362
Preventing and Detecting Corporate Espionage	363
Summary	364
Essential Terms	364
Review Questions	365
Discussion Issues	365
Endnotes	366

CHAPTER 14 FRAUD RISK ASSESSMENT 367

Overview	367
What Is Fraud Risk?	367
Why Should an Organization Be Concerned about Fraud Risk?	368
Factors That Influence Fraud Risk	368
What is a Fraud Risk Assessment?	369
What Is the Objective of a Fraud Risk Assessment?	369
Why Should Organizations Conduct Fraud Risk Assessments?	369
Improve Communication and Awareness about Fraud	370
Identify What Activities Are the Most Vulnerable to Fraud	370
Know Who Puts the Organization at the Greatest Risk	370
Develop Plans to Mitigate Fraud Risk	370
Develop Techniques to Determine Whether Fraud Has Occurred in High-Risk Areas	370
Assess Internal Controls	370
Comply with Regulations and Professional Standards	371
What Makes a Good Fraud Risk Assessment?	371
Collaborative Effort of Management and Auditors	371
The Right Sponsor	372
Independence and Objectivity of the People Leading and Conducting the Work	372
A Good Working Knowledge of the Business	372
Access to People at All Levels of the Organization	373
Engendered Trust	373
The Ability to Think the Unthinkable	373
A Plan to Keep It Alive and Relevant	373
Considerations for Developing an Effective Fraud Risk Assessment	374
Packaging It Right	374
One Size Does Not Fit All	374
Keeping It Simple	374

Preparing the Company for the Fraud Risk Assessment	374	Surveillance	396
Assembling the Right Team to Lead and Conduct the		Informants	396
Fraud Risk Assessment	375	“Dumpster-Diving”	396
Determining the Best Techniques to Use in Conducting the		Subpoenas	396
Fraud Risk Assessment	375	Search Warrants	397
Obtaining the Sponsor’s Agreement on the Work to Be		Voluntary Consent	397
Performed	376	Preserving Documentary Evidence	397
Educating the Organization and Openly Promoting the		Chain of Custody	398
Process	376	Preserving the Document	398
Executing the Fraud Risk Assessment	377	Organizing Documentary Evidence	398
Identifying Potential Inherent Fraud Risks	377	Chronologies	399
Assessing the Likelihood of Occurrence of the Identified		To-Do Lists	399
Fraud Risks	380	Using Computer Software to Organize Documents and	
Assessing the Significance to the Organization of the		Other Data	399
Fraud Risks	380	Sources of Information	399
Evaluating Which People and Departments Are Most		In-House Sources	400
Likely to Commit Fraud, and Identifying the Methods		Public Information	400
They Are Likely to Use	381	Report Writing	408
Identifying and Mapping Existing Preventive and		Purpose of the Report	408
Detective Controls to the Relevant Fraud Risks	381	Know the Reader	408
Evaluating Whether the Identified Controls Are Operating		Format	409
Effectively and Efficiently	382	Opinions or Conclusions in Report	414
Identifying and Evaluating Residual Fraud Risks Resulting		Summary	414
from Ineffective or Nonexistent Controls	382	Essential Terms	414
Addressing the Identified Fraud Risks	382	Review Questions	415
Establishing an Acceptable Level of Risk	382	Discussion Issues	415
Ranking and Prioritizing Risks	382	CHAPTER 16 INTERVIEWING WITNESSES	417
Responding to Residual Fraud Risks	384	Overview	417
Reporting the Results of the Fraud Risk Assessment	385	Introductory Questions	418
Considerations When Reporting the Assessment		General Rules for the Introductory Phase of the	
Results	385	Interview	418
Making an Impact with the Fraud Risk Assessment	386	Informational Questions	420
Beginning a Dialogue across the Company	386	Closing Questions	423
Looking for Fraud in High-Risk Areas	386	Assessment Questions	424
Holding Responsible Parties Accountable for		Verbal Clues to Deception	425
Progress	386	Nonverbal Clues	426
Keeping the Assessment Alive and Relevant	386	Typical Attitudes Displayed by Respondents	427
Monitor Key Controls	387	Admission-Seeking Questions	430
The Fraud Risk Assessment and the Audit Process	387	Steps in the Admission-Seeking Interview	431
Fraud Risk Assessment Tool	387	Summary	441
Summary	388	Essential Terms	441
Essential Terms	388	Review Questions	442
Review Questions	388	Discussion Issues	442
Discussion Issues	389	CHAPTER 17 OCCUPATIONAL FRAUD AND ABUSE:	THE BIG PICTURE
Endnotes	389	Defining Abusive Conduct	443
CHAPTER 15 CONDUCTING INVESTIGATIONS	391	Measuring the Level of Occupational Fraud and Abuse	445
AND WRITING REPORTS	391	The Human Factor	445
When is an Investigation Necessary?	391	Understanding Fraud Deterrence	447
Planning the Investigation	392	The Impact of Controls	447
Selecting the Investigation Team	392	The Perception of Detection	447
Developing Evidence	394		
Covert Operations	395		

xviii CONTENTS

The Corporate Sentencing Guidelines **450**
 Definition of Corporate Sentencing **450**
 Vicarious or Imputed Liability **451**
 Requirements **451**
The Ethical Connection **452**
Concluding Thoughts **453**
Summary **454**
Essential Terms **454**
Review Questions **455**
Discussion Issues **455**
Endnotes **455**

APPENDIX A *ONLINE SOURCES
OF INFORMATION* **457**

APPENDIX B *SAMPLE CODE OF BUSINESS ETHICS
AND CONDUCT* **467**

APPENDIX C *RISK ASSESSMENT TOOL* **481**

BIBLIOGRAPHY **511**

INDEX **513**

Occupational Fraud and Abuse

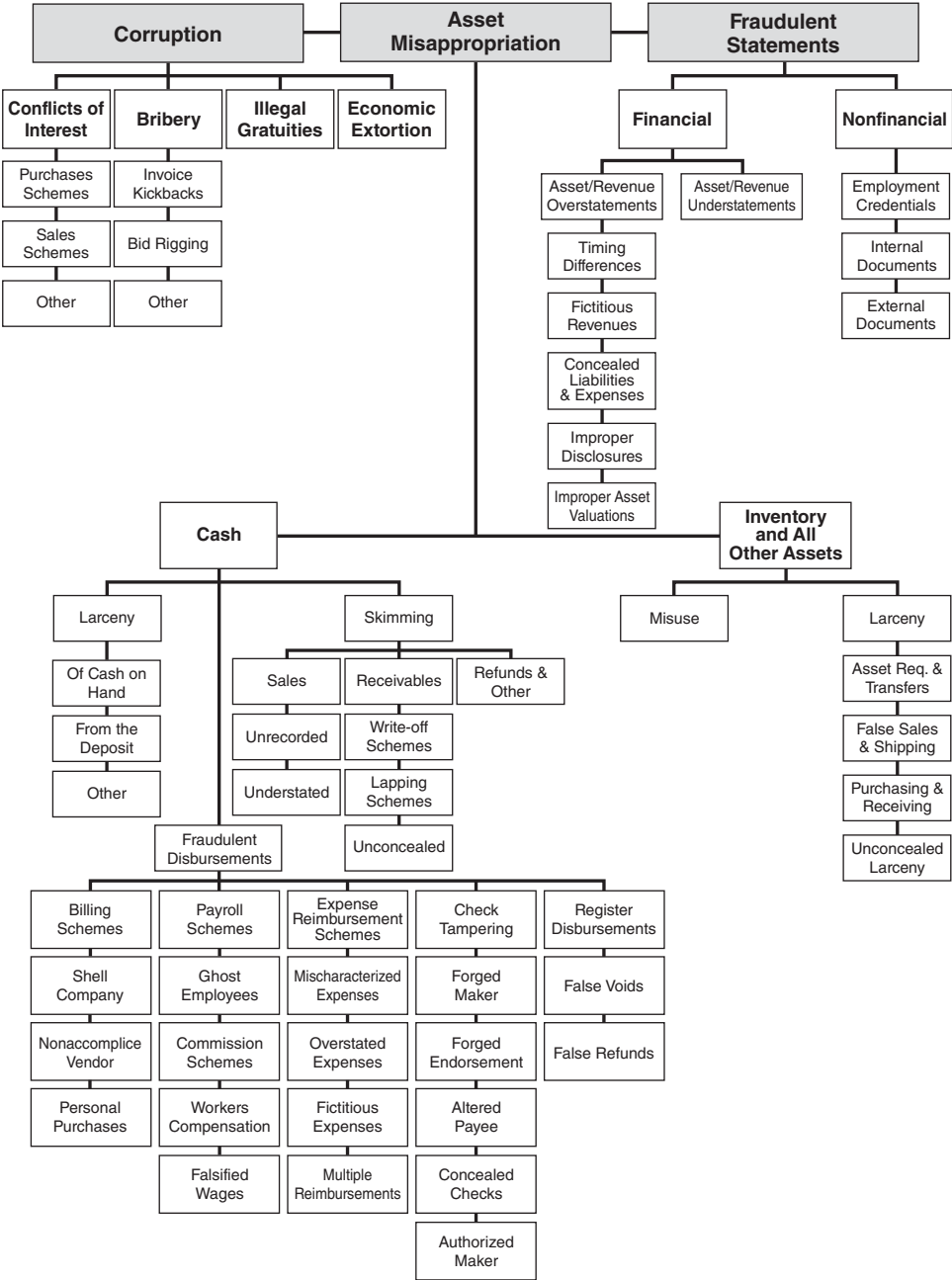


EXHIBIT 1-1

INTRODUCTION

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

- 1-1 Define fraud examination and differentiate it from auditing
- 1-2 Understand the fraud theory approach
- 1-3 Define occupational fraud
- 1-4 Define fraud
- 1-5 Define abuse
- 1-6 Know the difference between fraud and abuse
- 1-7 Describe the criminological contributions of Edwin H. Sutherland
- 1-8 Understand Donald Cressey's hypothesis
- 1-9 Give examples of nonshareable problems that contribute to fraud
- 1-10 Understand how perceived opportunity and rationalization contribute to fraud
- 1-11 Explain W. Steve Albrecht's "fraud scale"
- 1-12 Summarize the conclusions of the Hollinger-Clark study
- 1-13 Summarize the findings of the *2011 Global Fraud Survey*

Assume that you are an auditor for Bailey Books Corporation of St. Augustine, Florida. With \$226 million in annual sales, Bailey Books is one of the country's leading producers of textbooks for the college and university market and of technical manuals for the medical and dental professions.

On January 28, you received a telephone call. The caller advised that he did not wish to disclose his identity. However, he claimed to have been a long-term supplier of paper products to Bailey Books. The caller said that since Linda Reed Collins took over as purchasing manager for Bailey Books several years ago, he was systematically squeezed out of doing business with the company. He hinted that he thought Collins was up to something illegal. You queried the caller for additional information, but he hung up. What do you do now?

This case is fictional, but the situation is a common one in the world of commerce. Organizations incur costs in order to produce and sell their products or services. And such costs run the gamut: labor, taxes, advertising, occupancy, raw materials, research and development—and yes, fraud and abuse. The last cost, however, is fundamentally different from the others—the true expense of fraud and abuse is hidden, even if it is reflected in the profit-and-loss figures. Sometimes these offenses can constitute multibillion-dollar accounting misstatements, but much more frequently, they involve asset misappropriations or corruption, such as the fraud alluded to by the caller in the example above.

Resolving allegations of fraud—whether from tips, complaints, or accounting clues—is the discipline of fraud examination. It involves obtaining documentary evidence, interviewing witnesses and potential suspects, writing investigative reports, testifying to findings, and assisting in the general detection and prevention of fraud. Fraud examination has similarities to the field of *forensic accounting*, but the two terms are not precisely equivalent. Forensic accounting is the use of any accounting knowledge or skill for courtroom purposes and can therefore involve not only fraud, but also bankruptcy, business valuations and disputes, divorce, and a host of other litigation support services. On the other hand, though fraud examinations are typically performed by accountants, they can also be conducted by professionals in other fields, such as law enforcement officials, corporate security specialists, or private investigators.

Similarly, fraud examination and auditing are related, but are not identical. Because most occupational frauds are financial crimes, a certain degree of auditing is necessarily involved. But a fraud examination encompasses much more than just the review of financial data; it also involves techniques such as interviews, statement analyses, public records searches, and forensic document examination. Furthermore, there are significant differences between the two disciplines in terms of their scopes, objectives, and underlying presumptions. The following table summarizes the differences between the two disciplines.

Auditing vs. Fraud Examination

Issue	Auditing	Fraud Examination
Timing	Recurring Audits are conducted on a regular, recurring basis.	Nonrecurring Fraud examinations are nonrecurring. They are conducted only with sufficient predication.
Scope	General The audit is a general examination of financial data.	Specific Fraud examinations are conducted to resolve specific allegations.
Objective	Opinion An audit is generally conducted to express an opinion on financial statements or related information.	Affix blame The fraud examination determines whether fraud has occurred, and if so, who is responsible.
Relationship	Nonadversarial The audit process does not seek to affix blame.	Adversarial Fraud examinations involve efforts to affix blame.
Methodology	Audit techniques Audits are conducted primarily by examining financial data.	Fraud examination techniques Fraud examinations are conducted by (1) document examination, (2) review of outside data such as public records, and (3) interviews.
Presumption	Professional skepticism Auditors are required to approach audits with professional skepticism.	Proof Fraud examiners approach the resolution of a fraud by attempting to establish sufficient proof to support or refute an allegation of fraud.

FRAUD EXAMINATION METHODOLOGY

Fraud examination methodology requires that all fraud allegations be handled in a uniform, legal fashion, and that they be resolved in a timely manner. Assuming there is sufficient reason (predication) to conduct a fraud examination, specific steps are employed in a logical progression that is designed to narrow the focus of the inquiry from the general to the specific, eventually centering on a final conclusion. The fraud examiner begins by developing a hypothesis to explain how the alleged fraud was committed, and by whom. As each step of the fraud examination process uncovers more evidence, that hypothesis is amended and refined.

Predication

Predication is the totality of circumstances that would lead a reasonable, professionally trained, prudent individual to believe that a fraud has occurred, is occurring, or will occur. All fraud examinations must be based on proper predication; without it, a fraud examination should not be commenced. An anonymous tip or complaint, as in the Linda Reed Collins example cited earlier, is a common method for uncovering fraud; such a tip is generally considered sufficient predication. However, mere suspicion, without any underlying circumstantial evidence, is not a sufficient basis for conducting a fraud examination.

Fraud Theory Approach

In most occupational fraud cases, it is unlikely that there will be direct evidence of the crime. There are rarely eyewitnesses to a fraud, and it is unlikely—at least at the outset of an investigation—that the perpetrator will come right out and confess. Thus a successful fraud examination takes various sources of incomplete circumstantial evidence and assembles them into a solid, coherent structure that either proves or disproves the existence of the fraud.

To solve a fraud without complete evidence, the fraud examiner must make certain assumptions, not unlike a scientist who postulates a theory based on observation and then tests it. When investigating complex frauds, the fraud theory approach is almost indispensable. Fraud theory begins with an assumption, based on the known facts, of what might have occurred. That assumption is then tested to determine whether it can be proven. The fraud theory approach involves the following sequence of steps:

1. Analyze available data
2. Create a hypothesis
3. Test the hypothesis
4. Refine and amend the hypothesis

Let us illustrate using the Linda Reed Collins scenario. When you received the telephone call from a person purporting to be a vendor, you had no idea whether the information was legitimate. There could have been many reasons why a vendor would feel unfairly treated. Perhaps he just lost Bailey's business because another supplier provided inventory at a lower cost. Under the fraud theory approach, you must analyze the available data before developing a preliminary hypothesis about what may have occurred.

Analyzing Available Data If an audit of the entire purchasing function was deemed appropriate, it would be conducted at this time and would specifically focus on the possibility of fraud resulting from the anonymous allegation. For example, a fraud examiner would look at how contracts are awarded and at the distribution of contracts among Bailey Books' suppliers.

Creating a Hypothesis Based on the caller’s accusations, you would develop a hypothesis to focus your efforts. The hypothesis is invariably a “worst-case” scenario. That is, with the limited information you possess, what is the worst possible outcome? In this case, for Bailey Books, it would probably be that its purchasing manager was accepting kickbacks to steer business to a particular vendor. A hypothesis can be created for any specific allegation, such as a bribery or kickback scheme, embezzlement, a conflict of interest, or financial statement fraud.

Testing the Hypothesis After the hypothesis has been developed, it must be tested. This involves developing a “what-if” scenario and gathering evidence to either prove or disprove the proposition. For example, if a purchasing manager like Linda Reed Collins were being bribed, a fraud examiner likely would find some or all of the following:

- A personal relationship between Collins and a vendor
- Ability of Collins to steer business toward a favored vendor
- Higher prices or lower quality for the product or service being purchased
- Excessive personal spending by Collins

In the hypothetical case of Linda Reed Collins, you—using Bailey Books’ own records—can readily establish whether one vendor is receiving a proportionally larger share of the business than other vendors. You can ascertain whether Bailey Books was paying too much for a particular product, such as paper, simply by calling other vendors and determining competitive pricing. Furthermore, purchasing managers don’t usually accept offers of kickbacks from total strangers; a personal relationship between a suspected vendor and the buyer could be confirmed by discreet observation or inquiry. And whether Collins has the ability to steer business toward a favored vendor could be determined by reviewing the company’s internal controls to ascertain who is involved in the decision-making process. Finally, the proceeds of illegal income are not normally hoarded; such money is typically spent. Collins’s lifestyle and spending habits could be determined through examination of public documents such as real estate records and automobile liens.

Refining and Amending the Hypothesis In testing the hypothesis, a fraud examiner might find that the facts do not fit a particular scenario. If this is the case, the hypothesis should be revised and retested. Gradually, as the process is repeated and the hypothesis is continually revised, the examiner works toward the most likely and supportable conclusion. The goal is not to “pin” the crime on a particular individual, but rather to determine, through the methodical process of testing and revision, whether a crime has been committed—and if so, how.

Tools Used in Fraud Examinations

Three tools are available regardless of the nature of a fraud examination. First, the fraud examiner must be skilled in the examination of financial statements, books and records, and supporting documents. In many cases, these will provide the indicia of fraud upon which a complete investigation is based. The fraud examiner must also know the legal ramifications of evidence and how to maintain the chain of custody over documents. For example, if it is determined that Linda Reed Collins was taking payoffs from a supplier, checks and other financial records to prove the case must be lawfully obtained and analyzed, and legally supportable conclusions must be drawn.

The second tool used by fraud examiners is the interview, which is the process of obtaining relevant information about the matter from those who have knowledge of it.

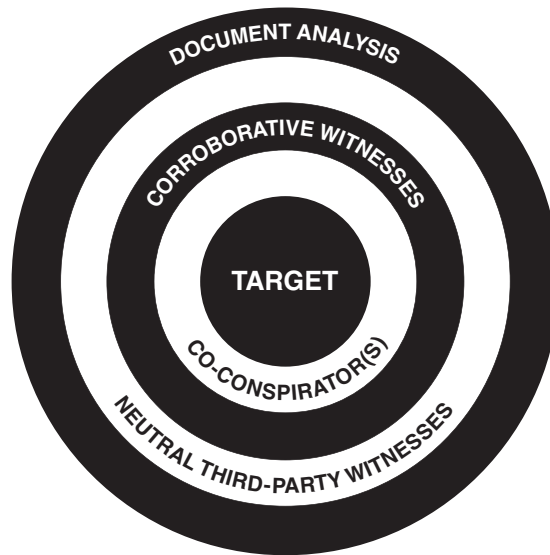


EXHIBIT 1-2 Evidence-Gathering Order in Fraud Examinations

For example, in developing information about Linda Reed Collins, it might be necessary to interview her coworkers, superiors, and subordinates.

In a fraud examination, evidence is usually gathered in a manner that moves from the general to the specific (see Exhibit 1-2). That rule applies both to gathering documentary evidence and taking witness statements. Thus, a fraud examiner would most likely start by interviewing neutral third-party witnesses, persons who may have some knowledge about the fraud but who are not involved in the offense. Next, the fraud examiner would interview corroborative witnesses—those people who are not directly involved in the offense, but who may be able to corroborate specific facts related to the offense.

If, after interviewing neutral third-party witnesses and corroborative witnesses, it appears that further investigation is warranted, the fraud examiner proceeds by interviewing suspected co-conspirators in the alleged offense. These people are generally interviewed in a particular order, starting with those thought to be least culpable and proceeding to those thought to be most culpable. Only after suspected co-conspirators have been interviewed is the person who is suspected of committing the fraud confronted. By arranging interviews in order of probable culpability, the fraud examiner is in a position to have as much information as possible by the time the prime suspect is interviewed. The methodology for conducting interviews will be discussed in Chapter 16.

The third tool that must be used in a fraud examination is observation. Fraud examiners are often placed in a position in which they must observe behavior, search for displays of wealth, and, in some instances, observe specific offenses. For example, a fraud examiner might recommend a video surveillance if it is discovered that Linda Reed Collins has a meeting scheduled with a person suspected of making payoffs.

Fraud examination methodology can be applied to virtually any type of fraud investigation. Although suspected frauds can be categorized by a number of different methods, they are usually referred to as “internal frauds” or “external frauds.” The latter refers to offenses committed by individuals against other individuals (e.g., con schemes), by individuals against organizations (e.g., insurance fraud), or by organizations against individuals (e.g., consumer frauds), but the former refers to offenses committed by the

people who work for organizations; these are the most costly and the most common frauds. A more descriptive term for these crimes, as we shall see, is *occupational fraud and abuse*. This book will concentrate exclusively on occupational fraud and abuse: how it is committed, how it is prevented, and how it is investigated.

DEFINING OCCUPATIONAL FRAUD AND ABUSE

For purposes of this book, *occupational fraud and abuse* is defined as

*The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.*¹

This definition's breadth means that occupational fraud and abuse involves a wide variety of conduct by executives, employees, managers, and principals of organizations, ranging from sophisticated investment swindles to petty theft. Common violations include asset misappropriation, fraudulent statements, corruption, pilferage and petty theft, false overtime, use of company property for personal benefit, and payroll and sick time abuses. Four elements common to these schemes were first identified by the Association of Certified Fraud Examiners in its *1996 Report to the Nation on Occupational Fraud and Abuse*, which stated: "The key is that the activity (1) is clandestine, (2) violates the employee's fiduciary duties to the organization, (3) is committed for the purpose of direct or indirect financial benefit to the employee, and (4) costs the employing organization assets, revenues, or reserves."²

An "employee," in the context of this definition, is any person who receives regular and periodic compensation from an organization for his labor. The employee moniker is not restricted to the rank-and-file, but specifically includes corporate executives, company presidents, top and middle managers, and other workers.

Defining Fraud

In the broadest sense, fraud can encompass any crime for gain that uses deception as its principal modus operandi. Of the three ways to illegally relieve a victim of money—force, trickery, or larceny—all offenses that employ trickery are frauds. Since deception is the linchpin of fraud, we will include *Merriam-Webster's* synonyms: "'Deceive' implies imposing a false idea or belief that causes ignorance, bewilderment, or helplessness; 'mislead' implies a leading astray that may or may not be intentional; 'delude' implies deceiving so thoroughly as to obscure the truth; 'beguile' stresses the use of charm and persuasion in deceiving."³

Although all frauds involve some form of deception, not all deceptions are necessarily frauds. Under common law, four general elements must be present for a fraud to exist:

1. A material false statement
2. Knowledge that the statement was false when it was uttered
3. Reliance of the victim on the false statement
4. Damages resulting from the victim's reliance on the false statement

The legal definition of fraud is the same whether the offense is criminal or civil; the difference is that criminal cases must meet a higher burden of proof.

Let's assume an employee who worked in the warehouse of a computer manufacturer stole valuable computer chips while no one was looking and resold them to a competitor.

This conduct is certainly illegal, but what law has the employee broken? Has he committed fraud? The answer, of course, is that it depends. Let us briefly review the legal ramifications of the theft.

The legal term for stealing is *larceny*, which is defined as “felonious stealing, taking and carrying, leading, riding, or driving away with another’s personal property, with the intent to convert it or to deprive the owner thereof.”⁴ In order to prove that a person has committed larceny, we would need to prove the following four elements: (1) There was a taking or carrying away (2) of the money or property of another (3) without the consent of the owner and (4) with the intent to deprive the owner of its use or possession. In our example, the employee definitely “carried away” his employer’s property, and we can safely assume that this was done without the employer’s consent. Furthermore, by taking the computer chips from the warehouse and selling them to a third party, the employee clearly demonstrated intent to deprive his employer of the ability to possess and use those chips. Therefore, the employee has committed larceny.

The employee might also be accused of having committed a tort known as *conversion*.⁵ Conversion, in the legal sense, is “an unauthorized assumption and exercise of the right of ownership over goods or personal chattels belonging to another, to the alteration of their condition or the exclusion of the owner’s rights.”⁶ A person commits a conversion when he takes possession of property that does not belong to him and thereby deprives the true owner of the property for any length of time. The employee in our example took possession of the computer chips when he stole them, and by selling them he has deprived his employer of that property. Therefore, the employee has also engaged in conversion of the company’s property.

Furthermore, the act of stealing the computer chips also makes the employee an embezzler. According to *Black’s Law Dictionary*, to *embezzle* means “willfully to take, or convert to one’s own use, another’s money or property of which the wrongdoer acquired possession lawfully, by reason of some office or employment or position of trust.”⁷ The key words in that definition are “acquired possession lawfully.” In order for an embezzlement to occur, the person who stole the property must have been entitled to possession of the property at the time of the theft. Remember, “possession” is not the same thing as “ownership.” In our example, the employee might be entitled to possess the company’s computer chips (to assemble them, pack them, store them, etc.), but clearly the chips belong to the employer, not the employee. When the employee steals the chips, he has committed embezzlement.

We might also observe that some employees have a recognized fiduciary relationship with their employers under the law. The term *fiduciary*, according to *Black’s Law Dictionary*, is of Roman origin and means:

*a person holding a character analogous to a trustee, in respect to the trust and confidence involved in it and the scrupulous good faith and candor which it requires. A person is said to act in a “fiduciary capacity” when the business which he transacts, or the money or property which he handles, is not for his own benefit, but for another person, as to whom he stands in a relation implying and necessitating great confidence and trust on the one part and a high degree of good faith on the other part.*⁸

In short, a fiduciary is someone who acts for the benefit of another.

A fiduciary has a duty to act in the best interests of the person whom he represents. When he violates this duty he can be liable under the tort of *breach of fiduciary duty*. The elements of this cause of action vary among jurisdictions, but in general they consist of the following: (1) a fiduciary relationship between the plaintiff and the defendant, (2) breach of the defendant’s (fiduciary’s) duty to the plaintiff, and (3) harm to the plaintiff or