

SUMMARY OF CONTENTS

VOLUME 1

- Chapter 1** Overview of Bank Security
- Chapter 2** Crimes Against Financial Institutions and Relevant Criminal Laws
- Chapter 3** Security Department: Structure and Function
- Chapter 4** Physical Security for the Institution
- Chapter 5** Computer Security for Financial Institutions
- Chapter 6** Contingency Planning for Financial Institutions
- Chapter 7** Security for the Human Resources Department
- Chapter 8** Data Security and the Internet
- Chapter 9** Security Training for Bank Employees
- Chapter 10** Investigation of White-Collar Crime
- Chapter 11** Automated Teller Machine Security
- Chapter 12** Safe-Deposit Security
- Chapter 13** Controlling Money Laundering
- Chapter 14** Check Fraud Prevention
- Chapter 15** Protecting Consumer and Proprietary Information

VOLUME 2—APPENDIXES

- 1** Bank Protection Act of 1968: Implementing Regulations
- 2** Reporting Requirements and Regulations
- 3** Securities and Exchange Commission Rules
- 4** [Reserved]
- 5** Sources of Information for Background Check
- 6** Regulations Concerning Employment of Criminal Offenders
- 7** Consumer Protection
- 8** Foreign Corrupt Practices Act of 1977
- 9** Federal Criminal Laws and Prosecution Policies
- 10** Regulation CC: Implementing the Expedited Funds Availability Act
- 11** Employee Polygraph Protection Act of 1988
- 12** Selected FDIC Statements of Policy
- 13** Foreign Assets Control Regulations
- 14** Electronic Signatures in Global and National Commerce Act

15 Private Security Officer Employment Authorization Act
Index

TABLE OF CONTENTS

About the Author.....	iii
Preface	v
Summary of Contents.....	vii

VOLUME 1

Chapter 1

Overview of Bank Security

§ 1.01	The Nature of Private Security	1-1
	[1] A Brief History of Bank Security	1-1
	[2] The Growing Role of Private Security	1-1
§ 1.02	The Bank Protection Act of 1968	1-2
	[1] Regulations Under the Act	1-3
	[a] Security Officer	1-3
	[b] Security Devices	1-3
	[c] Security Procedures	1-3
	[d] Filing of Reports	1-3
	[2] The May 1991 Revision	1-4
	[a] Designation of Security Officer	1-4
	[b] Security Program	1-4
	[c] Report	1-5
	[d] Bank Secrecy Act Compliance	1-6
§ 1.03	Industry Compliance With the Bank Protection Act of 1968	1-6
§ 1.04	SEC Rule 17F-1: Reporting of Missing, Lost, Counterfeit, or Stolen Securities	1-6
	[1] Institutions Covered Under the Program	1-6
	[2] Reporting Requirements	1-7
	[3] Inquiry Requirements	1-8
	[4] Securities Information Center, Inc.	1-8
	[a] Access Codes	1-8
	[b] Responses to Hits	1-9
	[c] Inquiries	1-9
§ 1.05	SEC Rule 17F-2: Fingerprinting Requirements	1-9
	[1] Persons to Be Fingerprinted	1-10
	[2] Exceptions to the Rule	1-10
	[3] Records and Reporting	1-11
	[4] Fingerprinting Pursuant to Other Law	1-11
	[5] Fingerprinting Plans of Self-Regulatory Organizations	1-11
§ 1.06	The Bank Secrecy Act	1-11
	[1] Compliance Procedures	1-11
	[2] Department of Treasury Regulation	1-11
Exhibit 1.1:	Form X-17F-IA: Missing/Lost/Stolen/Counterfeit Securities Report	1-13

Chapter 2

Crimes Against Financial Institutions and Relevant Criminal Laws

§ 2.01	Growth and Impact of Crimes Against Financial Institutions	2-1
[1]	Growth of Violent Crimes	2-1
[2]	Growth of White-Collar Crimes	2-1
[a]	Impact on Banks	2-2
[b]	FDIC Improvement Act of 1991	2-3
[c]	Increased Prosecution Efforts	2-5
[d]	FDIC Bank Failure Analysis 1985–1995	2-5
[e]	Civil Actions Against Directors, Officers, and Institution-Affiliated Parties	2-5
§ 2.02	Violent Crimes	2-5
[1]	Bank Robbery	2-6
[a]	Profile of Bank Robbers	2-6
[b]	Bank Robbery Prosecutions	2-7
[c]	Bank Robbery Statistics	2-7
[2]	Burglary	2-8
[3]	Kidnapping and Extortion	2-9
[4]	Attacks on Customers	2-9
[a]	ATM Violent Crime	2-9
[b]	Night Depository Violent Crime	2-10
[c]	Civil Liability Considerations	2-10
§ 2.03	White-Collar Crime	2-12
[1]	Causes for Increase in White-Collar Crime	2-13
[a]	Less Stringent Punishment Through the Courts	2-13
[b]	Insufficient Preemployment Screening	2-14
[c]	Diminishing Role of Federal Law Enforcement Officials	2-14
[d]	Changing Morality	2-14
[e]	Expanding International Technology	2-14
[2]	Embezzlement, Theft, or Misapplication of Bank Funds	2-15
[a]	Embezzlement and Misapplication Statutes	2-16
[b]	Bank Fraud Statute	2-18
[c]	False Bank Entries	2-19
[d]	Embezzler Traits	2-20
[3]	Loan Fraud	2-20
[a]	Commercial and Consumer Loans	2-21
[b]	Mortgage Loans	2-21
[c]	“Prime Bank” Notes	2-22.1
[4]	Check Fraud	2-23
[a]	Check Forgery	2-23
[b]	Check Kiting	2-24
[5]	Card Fraud	2-24
[a]	Credit Card	2-24
[b]	Debit (ATM and POS) Card	2-26
[c]	Credit and Debit Card Criminal Laws	2-27
[6]	Advance-Fee Schemes	2-28
[7]	Shell Corporations	2-28
[a]	Offshore Shell Banks	2-29
[8]	Brokered-Loan Fraud	2-30
[9]	Computer Crime	2-32

	[a] Computer Fraud Laws	2-34
	[b] Computer Crime Surveys	2-35
[10]	Traveler's Check Fraud	2-35
[11]	Counterfeiting	2-36
	[a] U.S. Currency	2-36
	[b] Securities	2-37
	[c] Commercial Instruments	2-37
[12]	Theft of Securities	2-37
[13]	Wire Fraud	2-38
[14]	Bank Bribery	2-38
[15]	Interstate Commerce of Stolen Property	2-39
[16]	Telemarketing Fraud	2-40
[17]	Mail Fraud	2-41
[18]	Racketeer Influenced and Corrupt Organizations Act (RICO)	2-41
[19]	OFAC Laws, Embargoed Countries, Penalties	2-42
	[a] Trading With the Enemy Act (TWEA)	2-42
	[b] International Emergency Economic Powers Act (IEPPA)	2-42
	[c] Iraq Sanctions Act	2-42
	[d] United Nations Participation Act (UNPA)	2-42
	[e] International Security and Development Corporation Act (ISDCA)	2-42
	[f] Title 18 of the U.S. Criminal Code	2-42
[20]	Identity Theft	2-42
[21]	Money Laundering	2-43
[22]	The Economic Espionage Act of 1996	2-43
[23]	Telephone Records and Privacy Protection Act of 2006	2-43
[24]	Financial Institutions Preventing Child Pornography	2-43
[25]	Catastrophe Relief Schemes	2-44
¶ 2.04	Suspicious Activity Reporting	2-44
	[1] Federal Reserve Board	2-46
	[2] Comptroller of the Currency	2-46
	[3] Federal Deposit Insurance Corporation	2-46
	[4] Office of Thrift Supervision	2-46
	[5] National Credit Union Administration	2-46
	[6] Preparation Guidelines for Suspicious Activity Report	2-46
	[a] FinCEN Guidelines	2-46
	[b] FBI Guidelines	2-47
Exhibit 2.1:	Bank Robbery Attacks (2005 through 2010) (Violations Reported by the FBI Under the Federal Bank Robbery and Incidental Crimes Statute (18 USC 2113))	2-49
Exhibit 2.2:	FBI Analysis of Victimized Banks and Credit Unions (2010)	2-50
Exhibit 2.3:	FBI Analysis of Acts of Violence at Victimized Banks and Credit Unions (2010)	2-51
Exhibit 2.4:	Bank Burglary Attacks (2005 through 2010) (Violations Reported by the FBI Under the Federal Bank Robbery and Incidental Crimes Statute (18 USC 2113))	2-52
Exhibit 2.5:	FBI Analysis of Kidnapping and Extortion (2008 through 2010) (Violations Investigated by the FBI Under the Federal Bank Robbery and Incidental Crimes Statute (18 USC 2113))	2-53
Exhibit 2.6:	Financial Crimes Enforcement Network (FinCEN) Rule Confidentiality of Suspicious Activity Reports	2-54
Exhibit 2.7:	Suspicious Activity Report	2-56

Chapter 3

Security Department: Structure and Function

¶ 3.01	Responsibilities and Duties of the Security Department	3-1
	[1] Physical Security	3-1
	[2] Personnel Security	3-3
	[3] Information Security	3-4
	[4] Crime Prevention and Detection	3-4
	[5] Investigations	3-5
¶ 3.02	Structure of the Security Department Staff	3-6
	[1] Position Description	3-6
	[a] Security Officer	3-6
	[b] Physical Security Manager	3-6
	[c] Investigations Manager	3-8
	[2] Stress in the Security Operation	3-8
	[3] Security Officer Designation	3-8
	[a] Security Officer Qualifications	3-9
	[b] Psychological Screening for Bank Security Officers	3-9
	[c] Certification for Bank Security Officers	3-9
	[4] Reporting Level	3-11
¶ 3.03	Risk Management	3-11
	[1] Security Officer's Role	3-12
	[a] Asset Identification	3-12
	[b] Team Approach	3-12
	[2] Special Considerations for Identification of Information and Information Systems	3-12
	[a] Classify and Rank Sensitive Data, Systems, and Applications	3-13
	[b] Assess Threats and Vulnerabilities	3-13
	[c] Evaluate Control Effectiveness	3-14
	[d] Assign Risk Ratings	3-14
	[3] Types of Insurance Coverage	3-14
	[a] Financial Institution Bond	3-14
	[b] Financial Institution Bond Deductibles	3-16
	[c] Master Trust Policies	3-16
	[d] Miscellaneous Policies	3-16
	[4] Environmental Risk	3-17
	[a] Environmental Risk Analysis	3-17
	[b] Loan Documentation	3-17
	[c] Monitoring	3-17
	[d] Training	3-18
	[5] Standards for Safety and Soundness	3-18
¶ 3.04	Role of the Security Department in Corporate Planning	3-18
	[1] Bank Profitability and the Security Function	3-18
	[2] Auditing the Performance of the Security Department	3-18
	[3] The Security Officer's Role in the Audit	3-20
¶ 3.05	Use of Outside Security Consultants	3-20
	[1] Selecting the Consultant	3-21
	[2] Working With the Consultant	3-21
	[3] A Word About Fees	3-22
¶ 3.06	Code of Ethics for Security Personnel	3-22

[1]	ASIS Code of Ethics	3-22
§ 3.07	Written Security Procedures	3-23
[1]	Model Security Procedure	3-28
Exhibit 3.1:	Banking Office Security Procedures	3-29
Exhibit 3.2:	Banking Office Opening Procedure	3-30

Chapter 4

Physical Security for the Institution

§ 4.01	Security Officer Responsibilities.....	4-1
[1]	Physical Security Equipment Inventory.....	4-2
[2]	UL-Approved Security Equipment.....	4-2
§ 4.02	Alarm Systems	4-3
[1]	Alarm System Definitions	4-3
[2]	Burglar Alarm Systems	4-5
[a]	Local Alarm Systems	4-6
[b]	Police Station-Connected Systems.....	4-6
[c]	Central Station Alarm Systems	4-7
[d]	Proprietary Systems.....	4-10
[e]	Transmission Line Security.....	4-10
[3]	Protection of Building's Perimeter and Interior.....	4-11
[4]	Vault, Safe, ATM, and Night Depository Alarms	4-11
[a]	Vaults	4-12
[b]	Safes.....	4-12
[c]	Night Depositories and ATMs	4-12
[5]	Holdup Alarms	4-13
[a]	Holdup Buttons	4-13
[b]	Holdup Footrails.....	4-14
[c]	Money Clips	4-14
[6]	Fire Alarms.....	4-14
[7]	Importance of Maintaining an Up-to-Date System	4-14
§ 4.03	Camera Surveillance Equipment.....	4-15
[1]	Selecting Equipment	4-16.1
[a]	Closed-Circuit Television	4-17
[b]	Sequence Bulk Film Cameras	4-19
[c]	Demand Bulk Film Cameras	4-20
[d]	Lens Selection	4-20
[2]	Positioning Surveillance Camera Equipment.....	4-20
§ 4.04	Protective Lighting.....	4-21
[1]	Applications for Financial Institutions.....	4-21
[a]	Vault Illumination.....	4-22
[b]	High-Exposure Area Illumination	4-22
[c]	Customer-Service Area Illumination.....	4-22
[d]	Parking Lot Illumination.....	4-22
[2]	Selecting Equipment	4-23
[a]	Types of Protective Lighting	4-23
[b]	Sources of Light	4-23
[3]	Positioning of Lighting.....	4-24

§ 4.05	Locks	4-24
	[1] Key Locks	4-24
	[2] Combination Locks	4-25
	[3] New Key Technology	4-27
	[4] Delayed-Action Time Locks	4-27
	[5] Electromechanical Locks	4-28
	[6] Developing a Control System.....	4-28
	[a] Keylock Control.....	4-28
	[b] Combination Control	4-29
	[7] Lock Installation	4-30
§ 4.06	Safes: Physical Specifications	4-30
	[1] UL-Approved Chests.....	4-30
	[a] UL-Approved Safes	4-30
	[b] Night Depositories	4-32
	[2] Previously Approved Chests	4-33
	[a] Auxiliary Safes	4-33
	[b] Night Depositories	4-33
	[c] ATMs.....	4-34
	[3] Selection of Equipment—Safes and Night Depositories	4-34
§ 4.07	Vaults	4-34
	[1] Vault Standards Formerly Required by the Bank Protection Act	4-35
	[2] Insurance Service Office Standards	4-35
	[3] ASTM Standard.....	4-35
	[4] Modular Vaults	4-36
	[5] Vault Doors.....	4-37
§ 4.08	Access Control and Identification Systems	4-37
	[1] Access Control	4-37
	[2] Identification	4-37
	[3] Biometric Personal Identification Systems	4-38
	[a] Fingerprints.....	4-39
	[b] Eye Scan.....	4-40
	[c] Hand Geometry	4-40
	[d] Finger Vein.....	4-40
	[e] Voice Patterns.....	4-40
	[f] Signature	4-40
	[g] Face Image	4-40
	[h] Facial Thermogram.....	4-40
	[i] Biometric Examples.....	4-40.1
	[4] Radio-Frequency Identification (RFID) Systems	4-40.1
§ 4.09	Banking Office Design	4-41
	[1] Visibility	4-43
	[2] Design and Layout	4-43
	[a] Customer Entrance	4-44
	[b] Teller Counter.....	4-44
	[c] Bullet-Resistant Barriers	4-45
	[d] Window Film.....	4-46
	[3] Landscaping Safety Considerations	4-46
§ 4.10	Counter Audio	4-46.1
	[1] Listening Devices	4-46.1
	[2] Countermeasures	4-47

¶ 4.11	Use of Guards	4-48
	[1] Justifying Guards	4-48
	[a] Research Phase	4-48
	[b] Risk Checklist	4-49
	[c] Implementing the New Approach	4-49
	[2] Choosing a Contract Guard Service	4-50
	[3] Using Public Police as Guards	4-51
	[a] Liability for Actions.....	4-52
	[b] Control of Work	4-52
	[c] Deep Pockets.....	4-53
	[4] Using Bullet-Proof Vests.....	4-53
	[a] Concealability and Comfort.....	4-53
	[b] Construction of the Vest.....	4-54
	[5] Armed vs. Unarmed Guards.....	4-54
	[6] Private Security Officer Employment Authorization Act.....	4-55
¶ 4.12	Dye Packs	4-56

Chapter 5

Computer Security for Financial Institutions

¶ 5.01	Computer Exposure	5-1
	[1] Risk Assessment	5-1
	[a] Lessons Learned From the Year 2000 Project.....	5-2
	[2] Safety and Soundness	5-4
	[a] GAO Concerns About Safety and Soundness	5-5
	[3] Legal	5-6
	[4] Data Processing Terms	5-6
	[5] Computer Risks	5-6
	[a] Theft of Currency and Other Financial Assets	5-7
	[b] Theft or Destruction of Computer Hardware or Software	5-7
	[c] Loss of Data Processing Capability	5-7
	[d] Theft of Customer or Institutional Data.....	5-8
	[e] Computer Viruses	5-9
	[f] Service Contracts.....	5-11
	[g] Vulnerabilities on the Internet.....	5-11
¶ 5.02	Computer Fraud Legislation	5-11
	[1] Federal Laws	5-12
	[a] Computer Fraud and Abuse Act of 1986.....	5-12
	[b] Telecommunications Law	5-12
	[c] Federal Computer Crime Law—Statute and OCC Guidance.....	5-12
	[2] State Computer Crime Laws	5-13
¶ 5.03	Computer Security Program	5-14
	[1] Architectural Guidelines.....	5-15
	[2] Organization Principles.....	5-15
	[a] Control Domains	5-15
	[b] Levels of Understanding.....	5-16
	[3] Baseline Security Controls.....	5-16
	[a] The Baseline Concept.....	5-16
	[b] Control Objectives	5-17

	[c]	Baseline Control Benefits	5-17
	[4]	Security Monitoring.....	5-18
§ 5.04		Computer Security Program Control Domains	5-18.1
	[1]	Management Control.....	5-18.1
		[a] Assignment of Responsibility.....	5-18.1
		[b] Users	5-18.1
		[c] Data Processing Management.....	5-18.1
		[d] Auditor.....	5-19
		[e] Data Security Officer.....	5-20
		[f] FDIC Auditing Checklist	5-21
	[2]	Communications Control	5-22
		[a] Communications Networks.....	5-22
		[b] Information Integrity	5-23
	[3]	Systems and Applications Controls	5-24
		[a] Authorized Access.....	5-24
		[b] Information Integrity	5-26
		[c] Privacy	5-26
		[d] Viruses	5-27
	[4]	Operational Controls	5-27
		[a] Authorized Usage	5-27
		[b] Process Integrity	5-28
		[c] Verification.....	5-28
		[d] Change Management	5-29
	[5]	Personnel Security	5-29
		[a] Systems Access.....	5-29
		[b] Systems Logging.....	5-30
	[6]	Physical Security	5-31
		[a] Site Selection.....	5-31
		[b] Design and Construction Characteristics.....	5-31
		[c] Fire Protection.....	5-32
		[d] Access Control	5-33
		[e] Physical Security in Distributed Environments.....	5-34
	[7]	Contingency Controls.....	5-35
		[a] Corporate Business Resumption and Contingency Planning	5-35
		[b] Federal Financial Institutions Examination Council Policy.....	5-36
§ 5.05		End-User Computing.....	5-37
	[1]	Risks Involved.....	5-38
	[2]	Controls at the End-User Level	5-38

Chapter 6

Contingency Planning for Financial Institutions

§ 6.01		The Need for Contingency Planning	6-1
	[1]	The 9/11 Commission Report	6-2
		[a] A Nation at War	6-2
		[b] Knowing Your Enemy's Beliefs	6-2
		[c] Islamic Fundamentalism	6-2
		[d] Osama bin Laden	6-3
		[e] Al Qaeda—An International Organization	6-3

	[f] Key Points for Security Planning	6-4
	[g] 9/11: 10 Years Later	6-4
[2]	Homeland Security Act of 2002	6-5
	[a] U.S. Department of Homeland Security	6-5
[3]	President's Commission on Critical Infrastructure Protection	6-8
	[a] Financial Services Sector Coordinating Council	6-10
	[b] Financial Services Information Sharing and Analysis Center	6-10
	[c] Protected Critical Infrastructure Information Program	6-10
[4]	FFIEC Policy on Contingency Planning	6-11
[5]	International Terrorism	6-12
¶ 6.02	Levels of Responsibility for Contingency Planning	6-12
	[1] U.S. Government Preparedness	6-12
	[2] Financial Institution Responsibility	6-12
	[a] Corporate Capacity for Succession	6-13
	[b] Corporate Policy Statement	6-13
	[c] A Sample Policy Statement	6-13
¶ 6.03	Risk Assessment In Contingency Planning	6-13
	[1] Assessing Risks	6-14
	[2] Human-Induced Events	6-14
	[a] IT System Intrusions and Systems Failures	6-15
	[b] Kidnapping, Hostage-Taking, and Extortion	6-15
	[c] Bomb Threats and Bombings	6-16
	[d] Terrorism	6-16
	[e] Sabotage	6-17
	[f] Nuclear War	6-17
	[g] Riots and Civil Disturbances	6-18
	[h] Electrical Blackouts and Brownouts	6-18
	[i] Fire	6-18
	[3] Natural Events and Pandemics	6-18
¶ 6.04	Developing the Contingency Management Plan	6-18
	[1] Contingency Management Planning Officer Responsibility	6-19
	[2] Designation of Contingency Management Team	6-19
	[3] Establishing Command Centers	6-19
	[4] Communications	6-20
	[5] Evaluating Critical Needs	6-20
	[a] Policies and Procedures	6-20
	[b] Key Personnel	6-20
	[c] Temporary Office Facilities	6-21
	[d] Information Technology Systems	6-21
	[e] Medical and HAZMAT Supplies	6-21
	[6] Recovery Priorities	6-21
	[7] Vital Records	6-21
	[8] Electronic Imaging Systems	6-22
¶ 6.05	Developing and Writing the Contingency Plan	6-23
	[1] Bomb Threats and Bombings	6-24
	[a] Intelligence Assessment	6-24
	[b] Precautions in Advance of Any Bomb Threat	6-24
	[c] Procedure if a Bomb Threat Is Received	6-25
	[d] Developing an Evacuation Procedure	6-25
	[e] Bombing Devices in Safe Deposit Boxes	6-26

	[f] Suspected Mail Bombs	6-26
[2]	Kidnapping, Hostage-Taking, and Extortion	6-27
	[a] Employee Training	6-27
	[b] Obtaining Information From the Perpetrator	6-28
	[c] If the Victim Is Brought to the Premises	6-28
	[d] Developing a Ransom Payment Policy	6-28
	[e] Guidelines for Ransom Payment	6-28
	[f] Key Points for the Kidnapping Plan	6-29
	[g] Insurance	6-29
[3]	Riots and Civil Disturbances	6-30
	[a] Legal Considerations	6-30
	[b] Personnel Safety	6-30
[4]	Electrical Failures	6-30
[5]	Fire	6-31
	[a] Fire Wardens	6-31
	[b] Evacuation	6-31
	[c] Training	6-31
[6]	Flooding, Snowstorms, Earthquakes, and Windstorms	6-31
[7]	Nuclear Attack	6-32
	[a] Property Protection	6-32
	[b] Personnel Protection	6-32
	[c] Storing Vital Records	6-32
	[d] Post-Attack Operations	6-33
[8]	Radiological Dispersion Device	6-35
[9]	Biological Weapons	6-35
	[a] Anthrax	6-36
[10]	Pandemics	6-39
	[a] The Federal Government	6-39
	[b] States and Localities	6-40
	[c] The Private Sector and Critical Infrastructure Entities	6-40
[11]	Chemical Weapons	6-41
	[a] Choking Agents	6-41
	[b] Blister Agents	6-41
	[c] Nerve Agents	6-41
	[d] Blood Agents	6-42
[12]	Potential Indicators of Weapons of Mass Destruction (WMD) Threats or Incidents	6-42
[13]	Exercise the Plan	6-42
	[a] Planning an Exercise	6-42
	[b] Performing an Exercise	6-43
	¶ 6.06 Interagency Policy on Contingency Planning for Financial Institutions	6-43
	Exhibit 6.1: Sample Bylaw to Provide for Emergency Operations by Surviving Staff	6-44
	Exhibit 6.2: Sample Bylaw to Provide for Emergency Operations Through Executive Committee Action	6-45
	Exhibit 6.3: Sample Resolution to Provide for Officer Succession	6-46
	Exhibit 6.4: Sample Bylaw to Provide for Alternate Locations	6-47
	Exhibit 6.5: Sample Resolution to Provide for Acting Head Offices	6-48
	Exhibit 6.6: Checklist of Vital Records	6-49
	Exhibit 6.7: Bomb Warning Checklist	6-52
	Exhibit 6.8: Checklist for Evaluating Your Bank's Disaster Readiness	6-53

Exhibit 6.9:	Business Pandemic Influenza Planning Checklist	6-63
Exhibit 6.10:	Department of Homeland Security Organization Chart	6-65
Exhibit 6.11:	Guidance for Financial Institutions on the Use of Foreign-Based Third-Party Service Providers	6-66
Exhibit 6.12:	Implementing 9/11 Commission Recommendations (Available Only on CD)	6-73

Chapter 7

Security for the Human Resources Department

§ 7.01	Applicant Screening	7-1
[1]	Training the Personnel Interviewer	7-1
[2]	The Employment Application	7-1
	[a] Topics That Should Be Questioned	7-2
	[b] Questions Concerning Criminal Records	7-2
	[c] Consent Agreements	7-2
	[d] Applicant's Signature	7-2
[3]	Fingerprinting	7-2
	[a] How to Submit Fingerprint Cards	7-3
[4]	Federal Deposit Insurance Act, Section 19	7-4
	[a] General Guidelines	7-4
	[b] FDIC Consent Application	7-4.1
	[c] Revisions to Consent Applications	7-5
	[d] Persons Covered	7-5
	[e] Exclusions from Section Applicability	7-5
	[f] FDIC Review Process for Consent Applications	7-6
	[g] Pending Employee Criminal Cases	7-6
[5]	Verification Procedures	7-6
	[a] Mail Reference Check	7-7
	[b] Investigative Agencies	7-7
	[c] Polygraph Tests	7-7
	[d] Using Pre-Employment Assessments	7-8
	[e] Computerized Source Records	7-11
[6]	Fair Credit Reporting Act	7-11
	[a] Amendments to the Fair Credit Reporting Act	7-11
	[b] Human Resources Impact	7-12
	[c] Civil Liability for Willful Noncompliance	7-12
	[d] Civil Liability for Negligent Noncompliance	7-13
[7]	Medical History	7-13
	[a] Controlled Substance Testing	7-13
	[b] Urinalysis and Hair Testing Chain of Custody	7-14
	[c] Drug Testing Statistics	7-14
[8]	Private Security Officer Employment Authorization Act	7-15
	[a] Definitions	7-15
	[b] Method for Conducting FBI Criminal History Searches	7-15
	[c] Criminal Penalties	7-16
§ 7.02	Security Aspects of Substance Abuse	7-16
[1]	Suggested Written Policy Regarding Use of Alcohol	7-16
[2]	Suggested Written Policy Regarding Use of Controlled Substances	7-17
[3]	Signs of Alcoholism	7-18

	[4]	Controlled Substance Abuse	7-18
		[a] Types of Controlled Substances	7-18
		[b] Some General Symptoms of Drug Abuse	7-19
		[c] Specific Symptoms	7-20
		[d] Noninvasive Detection	7-21
§ 7.03		Compulsive Gambling	7-21
	[1]	Signs of Gambling	7-22
	[2]	Suggested Written Policy Regarding Gambling	7-22
§ 7.04		Code of Conduct	7-22
	[1]	Elements of a Code of Conduct	7-23
	[2]	Foreign Corrupt Practices Act of 1977	7-25
	[3]	Bank Bribery Law	7-25
		[a] Justice Department Policy	7-26
		[b] Federal Banking Supervisory Guidelines	7-26
	[4]	Implementing an Effective Ethics Program	7-29
§ 7.05		The Americans With Disabilities Act	7-31
	[1]	Disability Defined	7-31
	[2]	Preemployment Screening	7-31
	[3]	Reasonable Accommodation	7-32
§ 7.06		The SAFE Act of 2008	7-33
§ 7.07		Workplace Violence	7-33
	[1]	Situational Example	7-34
	[2]	Historical Violence in America	7-34
	[3]	Violence in the American Workplace	7-34
	[4]	Significant Workplace Problem	7-35
	[5]	Interpersonal Acts of Violence	7-35
		[a] Warning Flags	7-36
	[6]	Written Plan	7-37
	[7]	Prevention Controls	7-38
		[a] Management's Position	7-38
		[b] Policies and Procedures	7-38
		[c] Training of Managers	7-38
		[d] New Employee Screening	7-39
		[e] Communications	7-39
		[f] Employee Input	7-39
	[8]	Employee Assistance Program	7-39
	[9]	Employee Terminations	7-39
	[10]	Security Program Interface	7-39
	[11]	Security Personnel Training	7-40
	[12]	Criminal Justice System	7-40
	[13]	Problem Reaction	7-40
	[14]	Incident Management	7-40
§ 7.08		Vacation Policies	7-40
	[1]	Situational Example	7-41
	[2]	Industry Standard	7-41
	[3]	Exceptions to Industry Standard	7-41
	[4]	FDIC Policy	7-42

Chapter 8

Data Security and the Internet

§ 8.01	Financial Transactions and the Internet	8-1
[1]	The Internet	8-1
[2]	Electronic Data Interchange	8-1
[3]	Federal Criminal Laws and the Internet	8-2
[a]	Procedures for Suspected Computer Crime	8-3
[b]	Types of Computer Crimes Investigated by the FBI	8-3
[c]	CSI Computer Crime Survey	8-3
[4]	Corporate Financial Exposure	8-4
§ 8.02	Security Risks Associated With the Internet	8-4
[1]	Technological Advances	8-4
[2]	Security Concerns	8-4
[a]	Data Privacy and Confidentiality	8-5
[b]	Data Integrity	8-5
[c]	Authentication	8-5
[d]	Nonrepudiation	8-5
[e]	Access Control and System Design	8-5
[3]	The Pitfalls of the Internet	8-6
[a]	Cyber Crime and Terrorism	8-7
[b]	Theft and Denial-of-Service Attacks by Hackers	8-11
[c]	Computer Viruses	8-11
[d]	Foreign Government Threats	8-12
[e]	Competitors and the Theft of Proprietary Information	8-12
[f]	Identity Theft	8-12
[g]	Business Account Takeovers	8-14
[4]	Web-Linking Risks	8-17
[5]	Wireless Technology	8-18
[6]	Software Vulnerabilities	8-19
[7]	Surviving Internet Attacks	8-19
[8]	Voice Over Internet Protocol	8-19
§ 8.03	Security Requirements for Online Financial Transactions	8-19
[1]	Internet Security Policy	8-20
[2]	Data Privacy and Confidentiality	8-20
[3]	Data Integrity	8-20
[4]	Identification and Authentication	8-20
[5]	Nonrepudiation	8-20
[6]	Access Control/System Design	8-21
§ 8.04	Security Controls for Online Financial Transactions	8-21
[1]	Encryption	8-21
[a]	Public Keys	8-21
[b]	Secret Keys	8-22
[c]	Control of Cryptographic Keys	8-22
[d]	Private Sector Cryptographic Systems	8-22
[e]	Quantum Cryptography	8-23
[2]	Digital Signatures	8-23
[a]	Digital Signature Laws	8-24
[b]	ABA Digital Signature Rules	8-24
[3]	Certificates & Certificate Authorities	8-24.1

[4]	Authentication in an Internet Banking Environment	8-24.1
[a]	Passwords	8-24.3
[b]	Tokens	8-24.3
[c]	Password-Generating Token	8-24.3
[d]	Smart Cards	8-24.4
[e]	Biometrics	8-24.4
[f]	One-Time Password Scratch Card	8-26
[g]	Second Channel Authentication	8-26
[h]	Mutual Authentication	8-26
[i]	Procedures to Mitigate Business Account Online Wire Transfer Fraud	8-26
[5]	Firewalls	8-26
[a]	Necessity of Firewalls	8-27
[b]	Types of Firewalls	8-28
[c]	Need for Constant Evaluation	8-29
[d]	Data Transmission	8-29
[6]	Intrusion Detection	8-29
[a]	Intrusion Detection Terminology	8-30
[b]	Characteristics of a Good Intrusion Detection System	8-30
[c]	Publicly Available Intrusion Detection Systems	8-31
[d]	Commercial Intrusion Detection Systems	8-31
[7]	Web Linking	8-31
[a]	Implementing Web-Linking Relationships	8-31
[b]	Monitoring Web-Linking Relationships	8-32
[c]	Managing Service Providers	8-32
[8]	Wireless Technology	8-32
[9]	Software Patches	8-32
[a]	Identifying Patch Information	8-33
[b]	Evaluating the Impact of Patches	8-33
[c]	Testing and Installing Software Patches	8-33
[10]	Internet Security Controls for PC Users	8-34
[11]	Virus Protection	8-34
[12]	VoIP Protection	8-35
¶ 8.05	Online Privacy and Information Security—Regulatory Guidance and Developments	8-36
[1]	FDIC Guidance on Online Privacy and Security	8-36
[a]	Financial Institution Letter on Online Privacy	8-36
[b]	Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes	8-37
[c]	Guidance on Instant Messaging	8-39
[2]	OCC and Dept. of Treasury Guidance and Initiatives	8-40
[a]	Technology-Related Risk Management Guidance and Checklists	8-40
[b]	The Consumer Electronic Payments Task Force Recommendations (Dept. of Treasury)	8-42
[c]	Automated Clearinghouse Risks	8-43
[3]	FRB Sound Practices Guidance for Information Security for Networks	8-44
[4]	Securities Regulation of Confidentiality of Information	8-45
[a]	October 1995 Interpretive Release	8-45
[b]	May 1996 Interpretive Release	8-45
[c]	Internet Surveillance Program	8-46
[d]	Elimination of Social Security Filing Requirement	8-46
[5]	FDIC Study on Account Hijacking and Identity Theft	8-46
[a]	Ways of Perpetrating Account Hijacking	8-46
[b]	Industry Responses to Identity Theft	8-47

	[c] Interagency Final Rule and Guidelines on Identity Theft “Red Flags”	8-48
Exhibit 8.1:	Intrusion Detection Terms	8-49
Exhibit 8.2:	Glossary of Internet Terms*	8-50
Exhibit 8.3:	FFIEC Guidance on Authentication in an Internet Banking Environment	8-53
Exhibit 8.4:	FFIEC Supplement to Authentication in an Internet Banking Environment	8-67

Chapter 9

Security Training for Bank Employees

¶ 9.01	Importance of a Good Training Program	9-1
	[1] Required by the Bank Protection Act Regulations	9-1
	[a] Board of Directors Responsibility	9-1
	[b] Security Officer Responsibility	9-1
	[c] Employee Responsibility	9-1
	[2] Prevention of Crimes of Violence	9-2
	[3] Prevention and Detection of White-Collar Crime	9-2
	[4] Protection of Customer Information	9-2
¶ 9.02	Training for Banking Office Personnel	9-2
	[1] Opening Procedures	9-2
	[2] Closing Procedures	9-3
	[3] Security During Banking Hours	9-3
	[a] Cash Control	9-3
	[b] Keys and Locks	9-5
	[4] Bank Robbery	9-6
	[a] Prevention	9-6
	[b] Bait Money Procedures	9-7
	[c] Bank Robbery Response	9-7
	[d] Coping with a Robbery Attack	9-8
	[5] Burglary Response	9-8
	[6] Kidnapping, Extortion, and/or Hostage Situation	9-8
	[a] Preventive Techniques	9-9
	[b] Response Training	9-10
	[7] Safe Deposit Operations	9-10
	[a] Common Problems	9-11
	[b] Checklist of Safeguards	9-11
	[8] “Know Your Customer” Procedures	9-12
	[a] Objectives	9-12
	[b] Identifying the Customer	9-12
	[c] Suspicious Conduct and Transactions Checklist	9-12
	[9] Loan Fraud Prevention	9-13
	[a] Mortgage Fraud	9-15
	[b] The SAFE Act of 2008	9-15
	[10] Detecting Counterfeit Currency, Securities, and Checks	9-15
	[a] Counterfeit Currency	9-15
	[b] Securities	9-17
	[c] Checks	9-18
	[11] Preventing Wire Transfer Fraud	9-18
	[12] Security Equipment Testing	9-18.1
	[a] Robbery Alarms	9-18.1

	[b] Burglar Alarms	9-19
	[c] Surveillance Cameras	9-19
	[d] Other Security Equipment	9-19
¶ 9.03	Training for All Employees	9-19
	[1] Customer Privacy Protection	9-19
	[2] Avoiding Pretext Phone Calling	9-20
	[3] Preventing Money Laundering	9-21
	[4] Bomb Threat	9-21
	[5] Fire	9-21
¶ 9.04	Special Training for Customers	9-22
	[1] Confidence Schemes	9-22
	[2] Robbery Prevention	9-22
Exhibit 9.1:	Daily Vault Control Log	9-23
Exhibit 9.2:	Bait Money Record	9-24
Exhibit 9.3:	Confidential Personal Profile	9-25
Exhibit 9.4:	Positions of Important Features on U.S. Currency	9-27
Exhibit 9.5:	The New Color Currency	9-29
Exhibit 9.6:	Redesigned \$5 Bill	9-30
Exhibit 9.7:	Redesigned \$100 Bill—New Security Features	9-32

Chapter 10

Investigation of White-Collar Crime

¶ 10.01	The Federal Criminal Justice System	10-1
	[1] Judicial Districts.....	10-1
	[2] Investigation	10-2
	[3] Prosecution	10-2
	[4] Incarceration	10-2
¶ 10.02	Federal Government Restraints On White-Collar Crime Investigations	10-3
¶ 10.03	The Internal Investigative Unit	10-3
	[1] Qualities to Look for When Hiring for These Positions.....	10-3
	[2] Threat Analysis Teams	10-4
	[3] Outsourcing the Investigative Function.....	10-5
¶ 10.04	Starting the Investigation	10-6
	[1] Reporting Criminal Activity.....	10-7
	[2] Planning the Investigation.....	10-8
	[a] Determining Objectives	10-9
	[b] Gathering Documentation	10-9
	[c] Identifying the Suspect.....	10-10
¶ 10.05	Interviewing	10-11
	[1] Objectives	10-11
	[2] Planning for Good Questions	10-11
	[a] Precise Questions	10-12
	[b] Extended Answer Questions.....	10-12
	[c] Leading Questions.....	10-13
	[d] Questions to Avoid.....	10-13

	[e]	Complex Questions.....	10-13
	[f]	The Five Interrogatives	10-13
	[g]	Question Sequence.....	10-14
	[h]	Controlled Answer Interviewing Techniques	10-14
	[i]	Free Narrative.....	10-14
	[j]	Direct Examination.....	10-14
[3]		Interview Environment	10-15
[4]		Investigator's Demeanor	10-15
[5]		Conducting the Interview	10-16
[6]		Recognizing Psychological Factors in Interviewing	10-16
	[a]	The Emotions.....	10-16
	[b]	The Physical Guilt Symptoms of Emotion.....	10-17
	[c]	Perception	10-17
	[d]	Memory	10-18
	[e]	Suggestion.....	10-19
	[f]	Bias	10-19
	[g]	Deception	10-19
§ 10.06		Interrogation	10-19
	[1]	Objectives	10-20
	[2]	Methodology.....	10-20
	[3]	Written Statements	10-21
§10.07		Polygraph and PSE Tests	10-22
	[1]	Polygraph.....	10-22
	[2]	Psychological Stress Evaluator.....	10-23
	[3]	Interpreting Test Results.....	10-23
	[4]	Legal Considerations.....	10-23
	[a]	Federal Polygraph Legislation	10-24
	[b]	State Polygraph Legislation.....	10-24
§ 10.08		Forensic Use of Hypnosis	10-25
	[1]	An Investigative Aid.....	10-25
	[2]	Guidelines for Use.....	10-26
§ 10.09		Implications of the <i>Miranda</i> Ruling	10-27
	[1]	Private Security Personnel Excluded	10-27
	[2]	Malicious Prosecution	10-27
	[3]	Employee's Rights	10-27
§ 10.10		Electronic Surveillance	10-28
	[1]	Wiretapping and Electronic Surveillance.....	10-28
	[2]	Telephone Conversations	10-28
§ 10.11		Investigating Computer Crime	10-29
	[1]	Areas of Vulnerability	10-29
	[2]	Definition of Computer Crime	10-30
	[3]	Computer Abuse Methods and Detection	10-30
	[4]	Clues to the Existence of Fraud	10-33
	[5]	Zeroing in on Suspects.....	10-33
	[6]	Special Training Needs of the Computer Crime Investigator	10-34
	[7]	Damage Control and Incident Response	10-34
	[8]	Evidence	10-38
§ 10.12		Bad Debt Investigation	10-39
	[1]	Commercial and Consumer Loans.....	10-40

[2]	Real Estate Loans	10-40
[3]	Uncovering Hidden Assets	10-41
§ 10.13	Search	10-42
[1]	Power to Search.....	10-42
	[a] Searches by Private Security Personnel.....	10-42
	[b] Private Sector Workplace Searches.....	10-43
[2]	Evidence Obtained From Searches	10-44
§ 10.14	Arrest	10-44
[1]	Definition of an Arrest	10-44
[2]	Arrest With a Warrant.....	10-45
[3]	Arrest Without a Warrant.....	10-45
	[a] Common-Law Rule: Private Security Officer Is Treated as a Private Citizen.....	10-45
	[b] Statutory Provisions.....	10-46
	[c] Deputization Powers	10-46
§ 10.15	Report Writing: the Outcome of the Investigation	10-46
[1]	Report Elements	10-46
[2]	Sample Report	10-47
§ 10.16	Avoiding Pitfalls	10-49
§ 10.17	Files	10-49
§ 10.18	Presenting Cases to the U.S. Attorney	10-50
[1]	Fast Track Programs	10-50
[2]	Guidelines for Fast Track Prosecution.....	10-51
[3]	Participation in a Fast Track Program	10-52
§ 10.19	Interpol	10-52
[1]	Interpol's History	10-52
[2]	Interpol's Organization.....	10-53
	[a] General Secretariat	10-54
	[b] National Central Bureaus	10-54
[3]	Using Interpol's Resources.....	10-54

Chapter 11

Automated Teller Machine Security

§ 11.01	Expanded Use of Debit Cards	11-1
[1]	ATMs	11-1
	[a] On-Premises ATMs	11-1
	[b] Free-Standing ATMs	11-1
[2]	Shared Networks	11-1
[3]	Point-of-Sale Terminals	11-2
[4]	Smart Cards	11-2
	[a] Stored-Value Systems	11-3
	[b] FDIC Smart Card Overview	11-4
	[c] Smart Cards in ATM Operations	11-5
§ 11.02	Regulation E—Electronic Fund Transfers	11-5
[1]	Definitions	11-6
[2]	Issuance of Access Devices	11-7
[3]	Consumer Liability	11-7
	[a] Situations Illustrating Consumer Liability Limits	11-8

	[b] Lost or Stolen Access Devices	11-9
[4]	Documentation of Transfers	11-10
[5]	Procedures for Resolving Errors	11-10
[6]	Record Retention	11-11
¶ 11.03	Security Considerations For ATM Installations	11-11
[1]	Equipment Selection	11-13
	[a] Safes	11-13
	[b] Alarms	11-13
	[c] Surveillance Systems	11-13
	[d] Enclosures	11-14
[2]	Site Selection	11-14
	[a] Incidence of Neighborhood Crime	11-15
	[b] Lighting	11-15
	[c] Access Control	11-15
	[d] FDIC Approval to Establish a Remote ATM Facility	11-16
[3]	Card and PIN Management	11-16
	[a] Card Type	11-16
	[b] PIN Selection	11-17
	[c] Card and PIN Distribution	11-17
	[d] Lost and Stolen Cards	11-17
	[e] Fraud Investigations	11-18
[4]	Consumer Safety	11-18
	[a] ATM Users Feel Safe	11-19
	[b] Customer Safety Education	11-19
	[c] Welfare Money and Food Stamps via ATMs and POS Terminals	11-19
[5]	ATM Security Legislation	11-20
	[a] Federal Legislation	11-20
	[b] State Laws	11-20
	[c] Local Laws	11-24
¶ 11.04	ATM Servicing and Operations	11-26
[1]	Dual Control	11-26
[2]	Service Operations	11-26
	[a] Currency Replenishment and Customer Deposits	11-27
	[b] Supplies and Repair	11-27
	[c] Transport	11-27
¶ 11.05	ATM Security Checklists	11-27
[1]	Customer Security Checklist	11-27
[2]	ATM Personnel Security Checklist	11-28
[3]	ATM Facility Security Checklist	11-29
[4]	Checklist for Preventing Customer Fraud	11-29
[5]	Checklist for Personnel With Access to the ATM System	11-29
[6]	Internal Control Questionnaire Used by National Bank Examiners	11-29
Exhibit 11.1:	California ATM User Safety Bill.....	11-31

Chapter 12

Safe-Deposit Security

¶ 12.01	Safe-Deposit Services	12-2
¶ 12.02	Liability Considerations	12-2

[1]	Bank's Legal Status	12-3
[a]	Bailment	12-4
[b]	Landlord and Tenant	12-4
[2]	Examples of Liability	12-4
§ 12.03	Design of the Safe-Deposit Department	12-5
[1]	Inside the Vault	12-6
[2]	Outside the Vault	12-6
[a]	Administrative Area	12-6
[b]	Privacy Booths	12-6
§ 12.04	Physical Security Considerations	12-7
[1]	Vault Construction	12-7
[2]	Vault Door	12-7
[3]	Day Gate	12-8
[4]	Safe-Deposit Boxes and Keys	12-8
[5]	Alarms	12-8
§ 12.05	Key and Lock Control	12-8
[1]	New Safe-Deposit Boxes	12-9
[2]	Unissued Key Control	12-9
[3]	Replacement Lock Control	12-9
[4]	Bank's Guard Key	12-10
§ 12.06	Safe-Deposit Contract	12-10
[1]	Suggested Contract Provisions	12-10
[2]	Types of Contracts	12-11
[3]	Customer Identification	12-11
§ 12.07	Operational Considerations	12-12
[1]	Opening and Closing Vault	12-12
[2]	Customer Access	12-13
[a]	Positive Identification	12-13
[b]	Records of Access	12-13
[c]	Entry Into Vault	12-14
[d]	Opening the Box	12-14
[e]	Use of Privacy Booth or Work Table	12-15
[f]	Return of Tin Container	12-15
[3]	Lost Customer Keys	12-15
[4]	Box Opening With a Court Order	12-16
[5]	Emergency Opening of a Box	12-16
[6]	Other Openings Without Renter's Presence	12-16
[7]	Surrendering the Box	12-17
§ 12.08	Dealing With a Burglary Attack	12-17
[1]	Notifications	12-18
[a]	Law Enforcement	12-18
[b]	Insurance Underwriters	12-18
[c]	Customers	12-18
[2]	Control of Customer and Bank Property	12-19
[a]	Dual Control	12-20
[b]	Evidence; Residue Examination	12-21
[c]	Serialization and Segregation of Property	12-21
[3]	Claims by Customers	12-21
[a]	Customer Interview	12-21

	[b] Customer Examination of Property	12-22
	[c] Resolution of Claims	12-22
¶ 12.09	Audits	12-22
¶ 12.10	Insurance	12-24
	[1] Combination Safe-Depository Policy	12-24
	[2] Lloyd's Safe-Deposit Box Insurance (Bankers Liability) Form NMA 903	12-25
	[3] Policies Available to Safe-Deposit Box Renters	12-25

Chapter 13

Controlling Money Laundering

¶ 13.01	Federal Legislation to Control Money Laundering	13-1
	[1] The Bank Secrecy Act	13-1
	[2] Money Laundering Control Act of 1986	13-1
	[3] Anti-Drug Abuse Act of 1988	13-2
	[4] Housing and Community Development Act of 1992	13-2
	[5] Money Laundering Suppression Act of 1994	13-2
	[6] International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001	13-2
¶ 13.02	Money Laundering in the Financial Community	13-3
	[1] Law Enforcement Efforts to Investigate Money Laundering Activities	13-3
	[a] United Nations	13-4
	[b] Financial Action Task Force	13-4
	[c] European Community	13-4
	[2] Money Laundering Examples	13-4
	[a] Pan American International Bank	13-4
	[b] Bank of Credit and Commerce International	13-5
	[c] Essex Imports Inc.	13-5
	[d] Check Express Inc.	13-5
	[e] Dollar Savings and Trust Company	13-5
	[f] Ratzlaf v. United States	13-6
	[g] Colombian Black Market Peso Exchange	13-6
	[h] Reconstruction of 9/11 Hijackers' Financial Activities	13-7
	[i] Riggs National Bank.....	13-7
¶ 13.03	Financial Recordkeeping and Reporting of Currency and Foreign Transactions Regulation	13-7
	[1] Recordkeeping Requirements	13-8
	[2] Customer Identification Programs for Banks, Savings Associations, and Credit Unions	13-9
	[3] Checking New Customers Against Government Terrorist Lists	13-10
	[4] Voluntary Information Sharing Among Financial Institutions	13-10
	[5] Reporting Requirements	13-10
	[a] Currency Transaction Report	13-10
	[b] Transactions of Exempt Persons	13-11
	[c] Businesses Not Excluded From CTR Reporting	13-13
	[d] Recordkeeping for Exempted Customers	13-13
	[e] Monitoring Exemptions	13-13
	[f] Discovery of Improper Exemptions	13-13
	[g] Multiple Transactions	13-14
	[h] Safe Harbor Law	13-14
	[i] Report of International Transportation of Currency or Monetary Instruments	13-16
	[j] Report of Foreign Bank Financial Accounts	13-16

	[k] Due Diligence Program for Foreign Accounts	13-17
[6]	Compliance Requirements	13-17
[7]	Internal Controls and Employee Training for Compliance	13-17
	[a] Financial Action Task Force	13-17
	[b] The President’s Commission on Organized Crime	13-18
	[c] FDIC Guidelines for Compliance	13-20
	[d] Treasury Department Training Guidelines for Employee Compliance	13-21
	[e] Other Training Guidelines for Employee Compliance	13-22
	[f] “Payable-Through” Accounts	13-23
[8]	Independent Audit Testing	13-23
[9]	Violations	13-24
	[a] Role of Federal Regulatory Agencies	13-24
	[b] Examination Guidelines	13-25
	[c] Internal Compliance Officer	13-25
[10]	Penalties for Violations	13-26
[11]	Questions and Answers	13-26
	[a] Bank Secrecy Act	13-26
Exhibit 13.1:	Currency Transaction Report	13-27
Exhibit 13.2:	FinCEN Form 110	13-31
Exhibit 13.3:	FinCEN Form 105. Report of International Transportation of Currency of Monetary Instruments	13-33
Exhibit 13.4:	Report on Foreign Bank and Financial Accounts	13-35
Exhibit 13.5:	FinCEN Guidance on CIP Regulations	13-43
Exhibit 13.6:	Guidance on Interpreting “Frequently” Found in the Criteria for Exempting a “Non-Listed Business” Under 31 CFR § 103.22(d)(2)(vi)(B)	13-53

Chapter 14

Check Fraud Prevention

§ 14.01	Check Fraud	14-1
	[1] Check Fraud Losses Increasing	14-1
	[2] ABA Check Fraud Survey	14-1
	[a] 2002 Survey	14-1
	[b] 2007 Survey	14-2
	[c] 2009 Survey	14-3
§ 14.02	Opening New Accounts	14-3
	[1] Customer Identification Program	14-4
	[2] Establishing Proper Identification	14-4
	[a] Forms of Identification	14-4
	[b] Required Identification	14-5
	[3] Personal Accounts	14-5
	[a] Required Federal Procedures for Personal Accounts	14-5
	[b] Suggested Procedures for Personal Accounts	14-6
	[4] Business Accounts	14-6
	[a] Required Federal Procedures for Business Accounts	14-6
	[b] Suggested Procedures for Business Accounts	14-6
	[5] International Correspondent Accounts	14-7
	[6] Government Terrorist Lists	14-7

- [7] False Identification 14-7
 - [a] False Identification Crime Control Act of 1982 14-7
 - [b] Personal Identity Theft 14-8
 - [c] Federal Requirements for Driver’s Licenses 14-9
- [8] New Account Documentation and Verification 14-9
 - [a] Documenting the Account 14-9
 - [b] Credit for New Accounts 14-10
 - [c] Social Security Verification 14-10
 - [d] Electronic Screening of New Customers 14-10
- ¶ 14.03 Check Fraud Types 14-10**
 - [1] Statistical Data 14-10
 - [2] On-Us Checks 14-11
 - [3] Forged Endorsement 14-11
 - [4] Affidavits of Forgery 14-12
 - [5] Counterfeit Checks 14-12
 - [6] Check Kiting 14-12
 - [7] Phishing 14-13
- ¶ 14.04 Check Processing 14-13**
 - [1] Federal Reserve System 14-13
 - [2] Check Signature Verification 14-13
 - [3] Compliance With Regulation CC 14-14
 - [a] Compliance With Availability Schedules 14-15
 - [b] Compliance With Disclosure Requirements 14-15
 - [c] Compliance With Changes in Check Processing 14-15
 - [d] Compliance With Other Requirements of the Law 14-16
 - [e] Check Clearing for the 21st Century Act 14-16
 - [4] Uniform Commercial Code Applicability 14-17
 - [a] Return Items 14-17
 - [b] Dishonor 14-17
 - [c] Payment on Uncollected Items 14-18
 - [5] Rules for Cashing U.S. Treasury Checks 14-18
 - [6] Counterfeit Checks 14-19
 - [7] Remote Deposit Capture 14-20
 - [a] Fraud Risks 14-20
 - [b] Risk Assessment 14-20
 - [c] Legal and Compliance Considerations 14-21
 - [d] Operational Considerations 14-21
 - [e] Customer Contracts and Agreements 14-21
- ¶ 14.05 Check Fraud Investigation 14-22**
 - [1] Check Fraud Criminal Laws 14-22
 - [a] Forgery 14-22
 - [b] Check Kiting 14-22
 - [c] Identity Fraud 14-22
 - [2] Selecting and Training the Investigator 14-22
 - [3] Conducting the Investigation 14-23
 - [a] Initial Steps 14-23
 - [b] Handwriting Analysis 14-23
 - [c] Photographs 14-24
 - [4] Recovery of Lost Funds 14-24
 - [5] Check Print Program 14-24

§ 14.06	Training to Prevent Check Fraud	14-25
[1]	Teller Training	14-25
[2]	Customer Service Representative Training	14-26
[3]	Fraud Prevention Programs	14-28
[4]	Warning Notices	14-28
[5]	Advice From a Forger	14-28
[6]	Check Fraud Prevention Checklists	14-29
[a]	Check Forgery	14-29
[b]	Check Kiting	14-30
[c]	Counterfeit Checks	14-30
[7]	Three Points to Remember	14-31
§ 14.07	Using Technology to Prevent Check Fraud	14-31
[1]	Check Kiting	14-31
[2]	ABA's Touch Signature Fingerprint Program	14-31
[3]	Enhanced Check Paper	14-32
[4]	Establishing a Fraud Management System	14-32
[5]	Positive Pay	14-33
[6]	Reverse Positive Pay	14-33
§ 14.08	Other Check Fraud Prevention Measures	14-33
[1]	General Policy Considerations	14-33
[2]	Internal Controls to Prevent Check Fraud by Insiders	14-33
Exhibit 14.1:	BSA Exam Procedures for Customer Identification Programs.....	14-35
Exhibit 14.2:	Guidance on Accepting Accounts from Foreign Governments, Embassies, and Political Figures	14-42
Exhibit 14.3:	Affidavit of Forgery—Maker	14-44
Exhibit 14.4:	Affidavit of Forgery—Endorsement.....	14-45
Exhibit 14.5:	Federal Reserve Routing Numbers	14-46
Exhibit 14.6:	Disclosure Forms	14-47
Exhibit 14.7:	Endorsement Standard	14-51

Chapter 15

Protecting Consumer and Proprietary Information

§ 15.01	Information Security Program	15-1
[1]	Information Security Officer	15-1
[2]	Written Information Security Program	15-1
[a]	Information Security Definitions	15-1
[b]	Information Classification	15-2
[c]	Need to Protect Certain Information	15-2
[d]	Risk Identification and Assessment	15-3
[e]	Information Protection	15-3
[f]	Guidance from the National Institute of Standards and Technology (NIST)	15-3
§ 15.02	Federal Privacy Laws	15-3
[1]	Title V of the Gramm-Leach-Bliley Act	15-4
[a]	Guidelines for Customer Information Security	15-4
[b]	Regulations Implementing GLBA	15-5
[c]	Overview of Privacy Rule Requirements	15-6

	[d] Protected Information	15-7
	[e] Privacy Policy Notices	15-7
	[f] Maintaining Compliance With the GLBA	15-8
	[g] Training Employees	15-8
	[h] Audit for Compliance	15-8
[2]	Right to Financial Privacy Act of 1978	15-8
	[a] Confidentiality of Records	15-8
	[b] Subpoenas	15-8
	[c] Civil Penalties	15-9
	[d] Cost Reimbursement	15-9
	[e] Department of Justice Advisory	15-9
	[f] Amendments to the Act	15-10
[3]	Fair Credit Reporting Act of 1970	15-11
[4]	Electronic Fund Transfer Act of 1978	15-11
[5]	Fair Debt Collection Practices Act	15-11
[6]	Fair Credit Billing Act	15-11
[7]	Telephone Consumer Protection Act of 1991	15-11
[8]	Telemarketing and Consumer Fraud and Abuse Prevention Act of 1991	15-11
[9]	Federal Trade Commission Act	15-11
[10]	Electronic Communications Privacy Act of 1986	15-11
[11]	Cable Communications Policy Act of 1984 and Cable Television Consumer Protection and Competition Act of 1992	15-12
[12]	Comprehensive Crime Control Act of 1984	15-12
¶ 15.03	Other Privacy Laws and Self-Regulation	15-12
	[1] State Privacy Laws	15-12
	[2] Insurance Industry	15-12
	[3] State Insurance Regulation	15-12
	[4] The United States Constitution	15-12
	[5] Common Law Invasion of Privacy	15-12
	[6] The Fair Credit Reporting Act	15-12
	[7] Medical Information Privacy Protections	15-13
	[8] NAIC Model Insurance Information and Privacy Protection Act	15-13
	[9] Securities Industry	15-13
	[a] Common Law Agency Duties	15-14
	[b] Federal and State Securities Laws and Regulations	15-14
	[c] Fair Credit Reporting Act	15-14
	[d] Self-Regulatory Organization Rules	15-14
	[10] Investment Companies	15-15
¶ 15.04	Online Privacy and Security	15-15
	[1] Consumer Privacy Concerns and the Online Environment	15-15
	[2] Online Privacy—Federal Government and Banking Industry Concerns	15-16
	[a] Federal Trade Commission	15-16
	[b] FDIC	15-16
	[c] OCC	15-16
	[d] Banking Industry	15-17
¶ 15.05	Privacy Training for Employees	15-17
	[1] Building Employee Awareness	15-17
	[2] Protecting Information	15-17
	[3] Guidance on Pretext Phone Calling: Recommendations to Avoid Pretext Phone Calling	15-18

[a]	Account Information Brokers	15-18
[b]	Violations of Law	15-18
[c]	Background	15-18
[d]	Actions to Avoid Pretext Phone Calling	15-19
[e]	Reporting Suspicious Activity	15-20
[4]	Privacy of Communication Channels	15-20

VOLUME 2—APPENDIXES

Appendix 1

Bank Protection Act of 1968: Implementing Regulations

1.1	The Bank Protection Act of 1968	A1-1
1.2	Federal Reserve—Regulation H, Subpart F	A1-2
1.3	FDIC—12 CFR Part 326	A1-9
1.4	Comptroller of the Currency, Part 21—Minimum Security Devices and Procedures and Reports of Crimes and Suspected Crimes for National and District Banks (12 CFR 21)	A1-13
1.5	Office of Thrift Supervision—Part 568—Security Procedures	A1-21
1.6	National Credit Union Administration, Part 748—Security Program	A1-23

Appendix 2

Reporting Requirements and Regulations

2.1	Title 31 — Money and Finance	A2-1
2.2	Part 103—Financial Recordkeeping and Reporting of Currency and Foreign Transactions	A2-34
2.2.1	Final CIP Rule	A2-42
2.2.2	FinCEN Guidance on CTR Exemption Procedures	A2-50
2.3	Money Laundering Control Act of 1986	A2-105
2.4	Title XI—Right to Financial Privacy	A2-123
2.5	The Housing and Community Development Act of 1992	A2-139
2.6	Privacy of Consumer Financial Information	A2-141
2.7	Interagency Guidelines Establishing Standards for Safeguarding Customer Information	A2-217
2.8	Gramm-Leach-Bliley Act	A2-221
2.9	FDIC Bank Secrecy Act Examination Procedures	A2-253
2.10	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice	A2-275

Appendix 3

Securities and Exchange Commission Rules

3.1	Rule 17F-1 and Rule X-17F-1A	A3-1
3.2	Rule 17F-2	A3-5

Appendix 4 (Reserved)

Appendix 5

Sources of Information for Background Check

5.1	State Banking Authorities.....	A5-1
5.2	U.S. Postal Inspection Offices	A5-3
5.3	FBI Local Offices	A5-5
5.4	Guide to Investigative Sources for White-Collar Crimes.....	A5-7
5.5	U.S. Secret Service Field Offices	A5-11
5.6	Listing of U.S. Attorneys' Offices	A5-23
5.7	List and Boundaries of Federal Reserve System Locations.....	A5-41

Appendix 6

Regulations Concerning Employment of Criminal Offenders

6.1	Section 19—Penalty for Unauthorized Participation by Convicted Criminal	A6-1
6.2	FDIC Statements of Policy.....	A6-3
6.3	FDIC Advisory Opinions.....	A6-7

Appendix 7

Consumer Protection

7.1	The Fair Credit Reporting Act.....	A7-1
7.3	Electronic Fund Transfers Act.....	A7-20
7.4	Part 205—Electronic Fund Transfers (Regulation E) (Available Only on CD)	A7-33

Appendix 8

Foreign Corrupt Practices Act of 1977

Appendix 9

Federal Criminal Laws and Prosecution Policies

9.1	Selected Sections From Title 18 of the U.S. Code: Crimes and Criminal Procedure	A9-1
9.2	Justice Department Policy on Bank Bribery Prosecution	A9-33
9.3	Section 1014, Title 18 of the U.S. Code: False Statements	A9-39
9.4	Suspicious Activity Report	A9-43
9.5	Identity Theft and Assumption Deterrence Act of 1998	A9-49
9.6	18 U.S.C. 1030. Fraud and Related Activity in Connection With Computers	A9-55

Appendix 10

Regulation CC: Implementing The Expedited Funds Availability Act

Appendix 11

Employee Polygraph Protection Act of 1988

Appendix 12

Selected FDIC Statements of Policy

12.1	[Reserved]	A12-1
12.2	Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations	A12-12
12.3	Interagency Policy on Contingency Planning for Financial Institutions	A12-16.11
12.4	Risks and Controls in End-User Computing	A12-19
12.5	Statement of Policy Providing Guidance on External Auditing Procedures for State Nonmember Banks	A12-22
12.6	Interagency Statement on EDP Service Contracts	A12-31
12.7	Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners	A12-32
12.8	Statement Concerning the Responsibilities of Bank Directors and Officers	A12-36
12.9	Warning Guidelines on Use of “Payable Through” Accounts	A12-39
12.10	Environmental Risk Program	A12-43
12.11	Information Technology Examination Officer’s Questionnaire	A12-45
12.12	Interagency Guidelines Establishing Information Security Standards	A12-53
12.13	Interagency Statement of Subprime Mortgage Lending	A12-70

Appendix 13

Foreign Assets Control Regulations

Appendix 14

Electronic Signatures in Global and National Commerce Act

Appendix 15

Private Security Officer Employment Authorization Act

Index