

Summary Table of Contents

Part I — Legal Background for Use of Confidential Information

Chapter 1: Legal and Regulatory Requirements

Chapter 2: Marketing vs. Privacy: How Customer Data May Be Used

Chapter 3: Legal Restrictions on Data Sharing

Part II — Establishing an Information Privacy Policy

Chapter 4: Drafting a Corporate Policy and the Consumer Policy Statement

Chapter 5: Implementing the Policy

Chapter 6: Data Security Protection

Chapter 7: Training: A Necessary Process

Part III — Data Privacy Relating to Specific Operations

Chapter 8: Online and Internet Banking

Chapter 9: Insurance and Investment Services

Chapter 10: Mergers, Acquisitions, Joint Ventures, and Affiliations

Part IV — Review and Performance Measurement

Chapter 11: Monitoring Data Privacy and Controls for Data Sharing

Chapter 12: Examination by Independent Third Parties

Chapter 13: Data Privacy and MIS Performance

Chapter 14: Identity Theft

Appendixes

Appendix A: Glossary

Appendix B: Web Site Resources

Appendix C: FFIEC Training Resources (Available Only on CD)

Appendix D: Quick Reference Guide to Regulatory Issuances

Appendix E: Final Rulings on the Gramm-Leach-Bliley Act (GLB Act) (Available Only on CD)

Contents

About the Author	iii
Acknowledgments.....	v
About This Manual	vii
Summary Table of Contents	xv

Part I: Legal Background for Use of Confidential Information

Chapter 1 Legal and Regulatory Requirements

What Is Privacy?	1 — 1
Proposed Identity Theft Enforcement and Restitution Act of 2007 (ITERA)	1 — 1
Background.....	1 — 2
10 Exemptions to the Privacy Act	1 — 2
Freedom of Information Act (FOIA) vs. Privacy Act.....	1 — 2a
Significantly Engaged.....	1 — 3
Customer vs. Consumer.....	1 — 4
Special Rule for Servicing.....	1 — 5
NPPI.....	1 — 5
Restrictions on Reuse and Redisclosure if NPPI is Received Under the Section 14 or 15 Exceptions	1 — 6
Restrictions on Reuse and Redisclosure if NPPI is Received Outside Section 14 or 15 Exceptions	1 — 7
Disclosure of Account Numbers Is Prohibited	1 — 7
Security Breach.....	1 — 7
Practical Advice — Coexistence in a Digital World	1 — 9
Prevention is the Best Policy	1 — 12a
Privacy Compliance	1 — 12a
Privacy Counts	1 — 12b
Annual Report To Congress.....	1 — 14
Analysis of the Effectiveness of the National Registry	1 — 14
Number of Consumers Who Placed Their Telephone Numbers on the National Registry as of the End of FY 2007	1 — 14a
Number of Entities Paying Fees for Access to the National Registry During Fiscal Year 2007	1 — 14a

Analysis of Progress Coordinating the Operation and Enforcement of the National Registry with State Do Not Call Lists	1 — 14a
Analysis of the Progress of Coordinating the Operation and Enforcement of the National Registry with the FCC	1 — 14a
Conclusion	1 — 14b
Consumer Privacy, Regulations, and Communicating Effectively	1 — 14b
Trusted Financial Institutions.....	1 — 15
Five Practices to Increase Trust.....	1 — 16
90-Day Privacy Improvement Plan.....	1 — 16
Definitions of Privacy	1 — 17
Consumer Advantages from Information Sharing by Financial Services Companies.....	1 — 20
Myths About Information Sharing – Advantages and Disadvantages.....	1 — 20a
Sources of Consumer Advantages from Data Sharing	1 — 20a
More Advantages to Information Sharing	1 — 20b
Even More Advantages.....	1 — 20c
Objectives of Managing Data Access and Ensuring Data Privacy	1 — 20c
Fair Information Practices	1 — 20d
Privacy Notice	1 — 21
Data Security Program — Key Components.....	1 — 21
Laws and Regulations That Affect Privacy	1 — 22
Bank Secrecy Act	1 — 22
Children’s Online Privacy Protection Act (COPPA) 15 USC 6501-6505.....	1 — 24
Comprehensive Crime Control Act of 1984.....	1 — 28
Computer Fraud and Abuse Act of 1986.....	1 — 29
Electronic Communications Privacy Act of 1986	1 — 29
Electronic Fund Transfer Act	1 — 30
Fair Credit Billing Act.....	1 — 30
Fair Credit Reporting Act.....	1 — 31
Federal Trade Commission Insights into FCRA	1 — 32
Fair Debt Collection Practices Act	1 — 33
Right to Financial Privacy Act	1 — 33
Telemarketing and Consumer Fraud and Abuse Prevention Act of 1991	1 — 34
Telephone Consumer Protection Act of 1991.....	1 — 34
NAIC Model Insurance Information and Privacy Protection Act.....	1 — 34
Federal Securities Laws and Regulations	1 — 35
Privacy Provisions of the GLB Act	1 — 36
Study of Information Sharing Practices Among Financial Institutions and Their Affiliates	1 — 37
Unauthorized Access to Customer Information	1 — 37
Response Program.....	1 — 40
Customer Notice.....	1 — 41
Proposed Model Privacy Notice	1 — 44
FDIC’s Supervisory Policy on Identity Theft.....	1 — 46
FTC Brochure for Businesses on Safeguarding Personal Information.....	1 — 46
Strategic Plan of the President’s Identity Theft Task Force	1 — 47
GLB Act Compliance	1 — 48
Fair and Accurate Credit Transactions (FACT) Act of 2003	1 — 51

Anti-Money Laundering Focus: The USA PATRIOT Act.....	1 — 54
Regulatory Agency Issuances.....	1 — 55
Federal Reserve Board’s Proposed Statement of Customer Rights.....	1 — 55
Quick Reference Guide to Regulatory Issuances.....	1 — 56
State Financial Privacy Laws and Regulations.....	1 — 56
State Fair Credit and Consumer Protection Acts.....	1 — 57
California’s Financial Information Privacy Act.....	1 — 57
Contact Points.....	1 — 58
Responsibilities of Directors and Senior Management in Establishing Privacy Policies and Procedures.....	1 — 58
Chief Privacy Officer.....	1 — 60
Privacy Litigation.....	1 — 60
Monster.com.....	1 — 60
Pfizer.....	1 — 60a
The Cost of Credit Monitoring.....	1 — 60a
Current Regulatory Measures.....	1 — 60b
Identity Theft Prevention Program.....	1 — 60b
Privacy Lawsuit: Compliance Risk Rising.....	1 — 60c
Information Security and Protecting Consumer Information.....	1 — 61
Policies and Procedures.....	1 — 61
Privacy Notices.....	1 — 62
Limits on Disclosure.....	1 — 67
Identification of Technological Vulnerabilities.....	1 — 68
Intrusion Detection Systems.....	1 — 68
Virus Prevention.....	1 — 69
Exhibit 1.1: Components of the Privacy Plan Timeline.....	1 — 71
Exhibit 1.2: Provisions of Title III of the USA PATRIOT Act (Available Only on CD).....	1 — 72
Exhibit 1.3: National Information Infrastructure Sample Privacy Principles.....	1 — 73
Exhibit 1.4: Information Security Checklists (Available Only on CD).....	1 — 75
Exhibit 1.5: Disposal of Consumer Report Information and Records FACT Act of 2003 Final Rule Issued by the Federal Trade Commission.....	1 — 76
Exhibit 1.6: Using Information Security to Protect Privacy.....	1 — 77

Chapter 2

Marketing vs. Privacy: How Customer Data May Be Used

Collected Data.....	2 — 1
Understanding the Fundamental Concepts.....	2 — 2
Internal Data and Specific Privacy Definitions.....	2 — 2
Account Data Used for Marketing Purposes.....	2 — 3
Sharing Consumer Data.....	2 — 3
Collecting Consumer Data.....	2 — 5
Data Warehousing and Data Mining.....	2 — 7

Data Warehousing	2 — 7
Data Mining	2 — 8
Data-Mining Applications	2 — 8
Data-Mining Process	2 — 9
Steps to a Successful Data-Mining Project.....	2 — 10
Trends in Gathering Data.....	2 — 11
Customer Behavior Patterns	2 — 11
Market Saturation	2 — 12
New Niche Markets	2 — 12
Increased Commodization	2 — 13
Web Sites	2 — 13
Links	2 — 14
Marketing to Current Customers.....	2 — 14
In-House Marketing of Related Products and Services	2 — 14
Generally Acceptable Practices	2 — 15
Restricted Practices	2 — 16
The FACT Act and Its Impact on FCRA.....	2 — 16
Opt-Out Expiration Dates	2 — 16a
Model Forms and the Fair Credit Reporting Affiliate Marketing Regulations	2 — 16a
Practices That Attract Regulatory Attention	2 — 16b
In-House Marketing of Nonrelated Products or Services	2 — 16b
Generally Acceptable Practices	2 — 17
Restricted Practices	2 — 17
Marketing to Consumers.....	2 — 17
Nonaffiliate Use for Marketing of Services and Products.....	2 — 18
Generally Accepted Practices	2 — 18
Practices Requiring Care and Oversight	2 — 19
Practices That May Represent Higher Regulatory Risk	2 — 19
Credit Scoring.....	2 — 20
Brokerage and Insurance	2 — 20
Referral System	2 — 20
Sharing Numbers	2 — 20
Telemarketing Restrictions.....	2 — 21
Joint Marketing Efforts.....	2 — 22
Outside Service Providers.....	2 — 22
Denied Loan Applicants	2 — 23
Former Customers	2 — 23
Opt-Out Provisions	2 — 23
When Can Consumers/Customers Opt-Out?	2 — 23
Exceptions to Opt-Out Notice Requirements	2 — 24
Opt-Out Operational Issues — Documentation.....	2 — 24
Joint Accounts	2 — 24
Lifetime Tracking by Customer	2 — 24
Lifetime Tracking by Consumer.....	2 — 25
Partial Opt-Out Opportunities	2 — 25
Privacy Audits Experience Success	2 — 26
Privacy Sells	2 — 26

Exhibit 2.1: Customer Information Data Elements	2 — 28
Exhibit 2.2: Management Members to Consult in Developing Marketing Campaigns.....	2 — 46
Exhibit 2.3: Sharing Consumer Data Flow Chart.....	2 — 47
Exhibit 2.4: Collecting Consumer Data Flow Chart.....	2 — 49
Exhibit 2.5: Regulatory Issues Checklist.....	2 — 51
Exhibit 2.6: Sample Opt-Out Notices.....	2 — 59

Chapter 3

Legal Restrictions on Data Sharing

Fair Credit Reporting Act	3 — 1
Consumer Reporting Agency, Section 603.....	3 — 2
The FACT Act’s Impact on FCRA, Section 624.....	3 — 2
Interagency Rules Implement Marketing Opt-Out Provisions	3 — 2a
Health Insurance Portability and Accountability Act	3 — 2b
Medical Information Privacy	3 — 2b
HIPAA and Financial Institutions.....	3 — 3
Gramm-Leach-Bliley Act	3 — 4
Privacy Provisions	3 — 4
Key Regulatory Components of the Regulation Definitions	3 — 4
Institution Privacy Policies and Practices.....	3 — 4
Privacy and Opt-Out Notices.....	3 — 5
Limits on Disclosures	3 — 6
Exceptions Noted in the Regulation	3 — 6
Relation to Other Law	3 — 7
Pretext Calling.....	3 — 7
Enforcement	3 — 8
Purpose and Scope.....	3 — 8
Definitions — Section 3	3 — 9
Privacy and Opt-Out Notices.....	3 — 20
Initial Required Privacy Notice to Consumers — Section 4	3 — 21
Annual Required Privacy Notice to Customers — Section 5.....	3 — 24
Information to Be Included in the Privacy Notices — Section 6	3 — 24
Short-Form Initial Notice	3 — 28
Future Disclosures	3 — 28
Form of Opt-Out Notice to Consumers and Opt-Out Methods — Section 7	3 — 30
Revised Privacy Notices — Section 8.....	3 — 33
Delivering Privacy and Opt Out Notices — Section 9.....	3 — 34
Alternatives for Privacy Notices.....	3 — 36
Limits on Nonpublic Personal Information Disclosure	3 — 37
Limits on Disclosure of Non-public Personal Information to Nonaffiliated	
Third Parties — Section 10	3 — 37
Limits on Redisclosure and Reuse of Information — Section 11	3 — 38

Limits on Sharing Account Number Information for Marketing Purposes — Section 12	3 — 40
Exception to Opt Out Requirements for Service Providers and Joint Marketing — Section 13	3 — 40
Exceptions to Notice and Opt Out Requirements for Processing and Servicing Transactions — Section 14	3 — 42
Other Exceptions to Notice and Opt Out Requirements — Section 15	3 — 43
Relation to Other Laws and the Effective Date	3 — 45
Fair Credit Reporting Act — Section 624 Fair Credit Reporting Affiliate Marketing Regulation	3 — 45
Protection of Fair Credit Reporting Act — Section 16	3 — 45
Relation to State Laws — Section 17	3 — 46
Sample Clauses	3 — 46
Checklists and Sample Notice	3 — 46a
Courts Interpret Privacy Rules	3 — 46a
Industry Sees Privacy Issues in Outsourcing	3 — 47
Exhibit 3.1: Legal Restrictions on Data Checklist	3 — 49
Exhibit 3.2: Reduced Regulatory Requirements	3 — 51
Exhibit 3.3: Evolution of a Prototype Financial Privacy Notice (Available Only on CD).....	3 — 57

Part II: Establishing an Information Privacy Policy

Chapter 4

Drafting a Corporate Policy and the Consumer Policy Statement

A Strong Foundation	4 — 1
What Not to Include in the Foundation	4 — 2
The Risks	4 — 2
Social Security Numbers and the Private Sector – Five FTC Recommendations	4 — 3
Recommendation 1: Improve Consumer Authentication	4 — 4
Recommendation 2: Restrict the Public Display and the Transmission of SSNs.....	4 — 4
Recommendation 3: Establish National Standards for Data Protection and Breach Notification.....	4 — 4
Recommendation 4: Conduct Outreach to Businesses and Consumers	4 — 4
Recommendation 5: Promote Coordination and Information Sharing on Use of SSNs.....	4 — 4
Conclusion	4 — 4a
Where to Begin in Drafting a Corporate Policy	4 — 4a
A Comprehensive Framework to Administer & Safeguard NPPI	4 — 4b
General Objectives Covered by a Privacy Policy and Consumer Policy Statement	4 — 5
Inventory	4 — 6
Specific Elements of the Corporate Privacy Policy and Consumer Privacy Policy Statement	4 — 9
Meeting Community Bank Needs	4 — 10
Sample Consumer Data Protection/Privacy Policy and Supporting Procedures	4 — 11

Exhibit 4.1: Sample Inventory of Existing Policies and Procedures	4 — 13
Exhibit 4.2: Sample Consumer Data Protection/Privacy Policy for Internal Use	4 — 14
Exhibit 4.3: Sample Consumer Data Protection/Privacy Information Sheet and Sample Initial Notice and Opt Out for XYZ BANK	4 — 49
Exhibit 4.4: Sample Consumer Data Protection/Privacy Policy for Internal Use at a Community Financial Institution	4 — 59
Exhibit 4.5: Sample Consumer Data Protection/Privacy Information Sheet and Sample Initial Notice for Community Bank	4 — 82
Exhibit 4.6: Sample Do-Not-Call Policy	4 — 84
Exhibit 4.7: Sample Letters	4 — 91
Exhibit 4.8: Sample Credit-Related Letters Checklist	4 — 93
Exhibit 4.9: Sample End User Profile Request Form	4 — 94

Chapter 5 Implementing the Policy

Developing and Implementing Procedures	5 — 1
Focusing on Primary Risk Areas	5 — 3
Security of Local Area Networks	5 — 4
Instituting Checks and Balances Within the Institution	5 — 7
Documenting Controls and Supervision of Data Privacy	5 — 8
Ensuring Management and Staff Awareness	5 — 8a
Exhibit 5.1: Sample Consumer Data Protection/Privacy Procedures for XYZ Bank	5 — 9
Exhibit 5.2: Sample Consumer Data Protection/Privacy Procedures for Community Bank (For a Financial Institution That Does Not Report Nonpublic Personal Information to Nonaffiliated Third Parties)	5 — 60
Exhibit 5.3: Tips and Hints for Privacy Implementation	5 — 116
Exhibit 5.4: Sample Consumer and Employee Personal Information Safeguards/Privacy Protection Procedures for Small Business	5 — 121

Chapter 6 Data Security Protection

Developing a Data Security Environment	6 — 1
Establishing Data Access Security Levels	6 — 2
Creating Various Walls to Protect Data from Outsiders	6 — 8
Physical Premises Internal Access Control Considerations	6 — 8
Passwords	6 — 9
Computer Terminal Safeguards	6 — 12
Dial-In Access	6 — 14

Using Software Safely	6 — 15
Remote Access	6 — 16
Electronic Information Channels and Required Security Controls.....	6 — 17
Cyber-Terrorism	6 — 19
Information-Rich and Getting Richer: Gathering Data and Protecting It Under the Bank Secrecy Act and the Privacy Act	6 — 22
CIP: The Devil Is in the Details.....	6 — 24
Major Policy Elements	6 — 24
Information Security Considerations.....	6 — 25
Privacy Rule Considerations	6 — 26
Internal Reviews for Data Privacy/Protection	6 — 27
Information Security Policy and Procedures	6 — 27
Developing or Enhancing Your Information Security Program	6 — 28
Personal Computers and Privacy	6 — 29
Exhibit 6.1: Checklist for Data Privacy Protection Security Systems Controls Review	6 — 30a
Exhibit 6.2: Checklist for Electronic Banking Internal Control.....	6 — 43
Exhibit 6.3: Checklist for Fedline EFT Internal Control.....	6 — 49
Exhibit 6.4: Checklist for Wholesale or Large-Dollar Fund Transfer Systems.....	6 — 52
Exhibit 6.5: Children’s Online Privacy Protection Act Worksheet for Notices	6 — 64
Exhibit 6.6: Information Security Policy.....	6 — 66
Exhibit 6.7: Information Security Procedures	6 — 82
Exhibit 6.8: ABC Bank Customer Identification Program Policy Supported by the ABC Information Security Policy and Privacy Policy	6 — 128
Exhibit 6.9: Data and Records Destruction Policy	6 — 163

Chapter 7

Training: A Necessary Process

Identifying Needs and Organizing Training	7 — 1
Training Group Identifiers.....	7 — 1
Training Dates and Priorities	7 — 3
Training Modules and Scope	7 — 3
Developing a Program	7 — 3
Identifying the Target Audience	7 — 3
Developing Training Resources and Support Materials	7 — 4
Conducting the Training Sessions	7 — 4
Overview of the Privacy of Consumer Financial Information Regulation	7 — 4
Data Privacy Terminology.....	7 — 5
Risks and Compliance Issues.....	7 — 5
Helpful Training Hints.....	7 — 5
Making Training Fit Your Organization	7 — 5
Business Areas Affected.....	7 — 6
Exhibit 7.1: Privacy of Consumer Financial Information Training Material (Available Only on CD)	7 — 13

Exhibit 7.2: Guidelines to Safeguarding Customer Information Training Materials (Available Only on CD)	7 — 14
Exhibit 7.3: USA PATRIOT Act Training Materials (Available Only on CD)	7 — 15
Exhibit 7.4: Customer Identification Program (CIP) (Available Only on CD)	7 — 16
Exhibit 7.5: Identity Theft Training Material (Available Only on CD)	7 — 17

Part III: Data Privacy Relating to Specific Operations

Chapter 8 Online and Internet Banking

Transactional Web Sites	8 — 1
Information Gathering on the Web Site	8 — 2
Media Channel Differences	8 — 2
Collection of Customer Information	8 — 2
Cookies	8 — 3
Interaction Between Customer and Financial Institution	8 — 4
Security Measures	8 — 5
Web Aggregation Services	8 — 5
Screen Scraping vs. Direct Feed	8 — 6
Screen Scraping	8 — 6
Direct Feed	8 — 6
Open Financial Exchange (OFX)	8 — 6
Background	8 — 6
Unique Advantages of Web Aggregation to Consumers	8 — 7
Advantages of Web Aggregation Services to Financial Institutions	8 — 7
The Challenges	8 — 7
Authentication Risks	8 — 8
Safeguards	8 — 8
Disadvantages – Screen Scraping	8 — 8
Disadvantages – Direct Feed	8 — 9
Standards to Consider	8 — 9
Dual Passwords – Another Solution	8 — 10
The Ability to Deny Access	8 — 10
Security Issues – A Basic Level of Agreement	8 — 11
Future Possibilities	8 — 11
Additional Protection – The Regulatory System and Congress	8 — 11
Two Divisions of Web Aggregators	8 — 11
Gramm-Leach-Bliley Act Privacy Requirements	8 — 12
BITS Financial Service Roundtable Guidelines	8 — 13
Security Guidelines	8 — 13
Guidelines for Aggregation Authentication and Data Feeds	8 — 13

Final Thoughts on Security.....	8 — 17
Disclosure Statements.....	8 — 17
Need for Privacy Policy.....	8 — 18
Clear and Prominent Display of the Privacy Policy.....	8 — 18
Basic Tenets of the Privacy Policy.....	8 — 18
Fair Information Practices.....	8 — 19
Adoption and Implementation.....	8 — 19
Notice and Disclosure.....	8 — 19
Choice and Consent: Opting Out.....	8 — 20
Information Access and Quality.....	8 — 20
Security and Integrity.....	8 — 21
Enforcement and Redress.....	8 — 21
Point of Contact.....	8 — 21
Use of Customer Information.....	8 — 21
Data Profiling.....	8 — 22
Data Matching.....	8 — 22
Third-Party Affiliates.....	8 — 22
Nonaffiliated Third Parties.....	8 — 22
Internet Banking and Marketing.....	8 — 23
Exhibit 8.1: Checklist for Adequacy of Privacy Policy.....	8 — 24
Exhibit 8.2: Sample Web Site Including Privacy Statement and Disclosures.....	8 — 25
Exhibit 8.3: BITS Privacy Principles.....	8 — 34
Exhibit 8.4: Checklist for Customer Information Security.....	8 — 36
Exhibit 8.5: Questions and Answers RE: Online and Internet Banking.....	8 — 37

Chapter 9

Insurance and Investment Services

Privacy Concerns.....	9 — 1
Affiliation Authority.....	9 — 2
Operating Subsidiaries.....	9 — 2
Sales Authority.....	9 — 2
Underwriting Authority.....	9 — 2
Other Restrictions/Limitations.....	9 — 2
Securities.....	9 — 3
Privacy Provisions.....	9 — 3
“Financial in Nature”.....	9 — 4
Provisions Protecting Privacy.....	9 — 5
Customer Financial Information Privacy.....	9 — 5
Protection of the Privacy of Nonpublic Personal Information.....	9 — 6
Duty to Establish Regulatory Standards.....	9 — 6
Required Disclosures.....	9 — 7
Required Timing of Disclosures.....	9 — 8

Disclosures Regarding Affiliated Third Parties.....	9 — 9
Requirement of Consumer Notification.....	9 — 10
Insights	9 — 10
Exceptions to the Consumer Opt-Out Right.....	9 — 10
Service Agreements with a Financial Institution.....	9 — 12
Marketing Agreements Between Financial Institutions for Joint Products or Services	9 — 12
Insights	9 — 12
Disclosure to Consumer of Use of Exception and Requirement of Third-Party Confidentiality Agreement	9 — 13
Prohibition on Sharing Account Number Information for Marketing Purposes.....	9 — 13
Insurance Industry and Privacy Issues	9 — 13
Medical Information Privacy Protections	9 — 14
Medical Privacy.....	9 — 15
Penalties for Noncompliance.....	9 — 16
Summary and Purpose of the Rule	9 — 17
Applicability	9 — 18
Entities Covered	9 — 18
Protected Health Information	9 — 18
General Rules.....	9 — 18
Uses and Disclosures with Individual Authorization.....	9 — 19
Uses and Disclosures for Treatment, Payment, and Health Care Operations.....	9 — 20
Permissible Uses and Disclosures for Purposes Other Than Treatment, Payment, and Health Care Operations.....	9 — 20
Enforcement.....	9 — 21
Investments/Securities and Privacy Issues.....	9 — 21
Common Law Agency Duties	9 — 21
Federal and State Securities Laws and Regulations	9 — 22
Self-Regulatory Organization Rules.....	9 — 22
Investment Company Institute	9 — 22
A Word About Nondisclosure Obligations.....	9 — 22
Exhibit 9.1: Insurance and Investment Privacy Checklist.....	9 — 24

Chapter 10

Mergers, Acquisitions, Joint Ventures, and Affiliations

Similar, Yet Dissimilar, Events.....	10 — 1
Looking at Each Event.....	10 — 1
Merger, Acquisition, and Affiliations.....	10 — 2
Information Systems.....	10 — 2
Economies of Scale	10 — 3
Staffing	10 — 3
Cost Considerations.....	10 — 3
Data Security and Customer Privacy During Change	10 — 3

Enlightened Self-Interest	10 — 4
“Chinese Wall” Policies and Nonaffiliated Parties in Joint Ventures	10 — 4
Insight	10 — 4
Joint Ventures in the Future	10 — 5
Gramm-Leach-Bliley Act Creates New Opportunities	10 — 5
Affiliation Authority	10 — 6
Operating Subsidiaries	10 — 6
Sales Authority	10 — 6
Underwriting Authority	10 — 6
Other Conditions	10 — 6
Securities	10 — 7
Financial in Nature	10 — 7
Protection of the Privacy of Nonpublic Personal Information During Mergers, Acquisitions, Joint Ventures, and Affiliations	10 — 8
Duty to Establish Regulatory Standards	10 — 8
Required Disclosures	10 — 8
Information to Be Included	10 — 9
Disclosures to Affiliated Third Parties	10 — 9
Requirement of Consumer Notification	10 — 10
Exceptions to the Consumer Opt-Out Right	10 — 10
Service Agreements with a Financial Institution	10 — 11
Marketing Agreements Between Financial Institutions for Joint Products or Services	10 — 11
Disclosure to Consumer of Use of Exception and Requirement of Third-Party Confidentiality Agreement	10 — 12
Prohibition on Sharing Account Number Information for Marketing Purposes	10 — 12
Regulation	10 — 12
Information to Be Included in Initial and Annual Notices of Privacy Policies and Practices	10 — 13
Information About Former Customers	10 — 14
Information Disclosed to Service Providers	10 — 15
Right to Opt Out	10 — 15
Disclosures Made Under the FCRA	10 — 15
Confidentiality, Security, and Integrity	10 — 16
Limitation on Disclosure of Nonpublic Personal Information About Consumers to Nonaffiliated Third Parties	10 — 16
Form and Method of Providing Opt-Out Notice to Consumers	10 — 18
Insight	10 — 18
Exception to Opt-Out Requirements for Service Providers and Joint Marketing Agreements	10 — 19
Insight	10 — 19
Exceptions to Notice and Opt-Out Requirements for Processing and Servicing Transactions	10 — 20
Other Exceptions to Notice and Opt-Out Requirements	10 — 20
Insight	10 — 20
Limits on Redisclosure and Reuse of Information	10 — 21
Limits on Sharing of Account Number Information for Marketing Purposes	10 — 21
Insight	10 — 22
Pretexting	10 — 22

Insights	10 — 23
Protection of FCRA	10 — 24
Fair Credit Reporting Act	10 — 24
Section 214 of the FACT Act	10 — 25
Scope and Definitions	10 — 26
Affiliate Marketing Opt-out and Exceptions	10 — 28
Scope and Duration of Opt-out.....	10 — 36
Contents of Opt-out Notice; Consolidated and Equivalent Notices	10 — 38
Reasonable Opportunity to Opt Out	10 — 40
Examples of a Reasonable Opportunity to Opt Out	10 — 40
By Mail.....	10 — 40
By Electronic Means	10 — 40
At the Time of an Electronic Transaction	10 — 40
At the Time of an In-person Transaction.....	10 — 41
By Including in a Privacy Notice	10 — 41
Reasonable and Simple Methods of Opting Out.....	10 — 41
Reasonable and Simple Opt-out Method.....	10 — 41
Opt-out Methods That Are Not Reasonable and Simple	10 — 42
Specific Opt-out Means	10 — 42
Delivery of Opt-out Notices	10 — 42
Renewal of Opt-out.....	10 — 43
Effective Date, Compliance Date, and Prospective Application	10 — 44
Identity Theft Prevention Program and Red Flags.....	10 — 45
Overview	10 — 45
Four Basic Elements of the Program.....	10 — 45
Steps to Administer the Program.....	10 — 46
Establishment of an Identity Theft Prevention Program.....	10 — 46
Elements of the Identity Theft Prevention Program	10 — 47
Identifying Relevant Red Flags	10 — 47
Detecting Red Flags	10 — 48
Preventing and Mitigating Identity Theft	10 — 48
Updating the Program.....	10 — 49
Administration of the Program.....	10 — 49
Supplement A	10 — 50
Duties of Card Issuers Regarding Changes of Address	10 — 53
Overview	10 — 53
Address Validation Requirements	10 — 53
Alternative Timing of Address Validation	10 — 54
Form of Notice	10 — 54
Medical Information Privacy Protections	10 — 54
Uses and Disclosures with Individual Authorization.....	10 — 55
Uses and Disclosures for Treatment, Payment, and Health Care Operations.....	10 — 55
Permissible Uses and Disclosures for Purposes Other Than Treatment, Payment, and Health Care Operations.....	10 — 55
Offshore Outsourcing Data Services and Consumer Privacy Risks	10 — 56
Critical Steps to Consider	10 — 58
Identity Theft	10 — 59

Procedures to Guard Against Predatory Identity Thieves	10 — 60
Cost and Incidence of ID Theft	10 — 62
Conclusion	10 — 64
Exhibit 10.1: Mergers and Acquisitions Review Checklist.....	10 — 65
Exhibit 10.2: Joint Venture Data Privacy Checklist.....	10 — 70
Exhibit 10.3: FDIC Study Data Services Outsourcing	10 — 72

Part IV: Review and Performance Measurement

Chapter 11 Monitoring Data Privacy and Controls for Data Sharing

Why Share Data if Privacy Is a Concern?.....	11 — 1
A Common Practice.....	11 — 1
Safeguard Customer Accounts.....	11 — 1
Target Marketing	11 — 1
One-Stop Shopping.....	11 — 2
Establishing a Monitoring Process and Its Role in Daily Operations Quality	11 — 2
Basic Points to Consider	11 — 3
Verifying Data Obtained.....	11 — 4
The Written Monitoring Process.....	11 — 5
Training	11 — 5
Scheduling Periodic Reviews	11 — 6
Risk Exposure Assessment	11 — 6
Formal Tracking Process	11 — 6
Role of the Internal Audit	11 — 7
Exhibits	11 — 9
Exhibit 11.1: Sample Internal Audit Program Re: Customer Data Privacy/ Data Security	11 — 10a
Exhibit 11.2: Sample Internal Audit Procedures Re: Customer Data Privacy/ Data Security	11 — 18
Exhibit 11.3: Sample Internal Audit and Monitoring Review Issues/Concerns Memorandum and Stated Corrective Action	11 — 33
Exhibit 11.4: Sample Audit Review Corrective Action Follow-Up Grid.....	11 — 36
Exhibit 11.5: Sample Scheduling Internal Control Monitoring.....	11 — 37
Exhibit 11.6: Sample Monitoring Internal Control Procedures Worksheets	11 — 41
Exhibit 11.7: Sample Monitoring Review Issues/Concerns Memorandum and Stated Corrective Action	11 — 64
Exhibit 11.8: Sample Monitoring Review Corrective Action Follow-Up Grid	11 — 67
Exhibit 11.9: Sample Independent Third-Party Onsite Vendor Review Internal Controls Checklist	11 — 68

Exhibit 11.10: Sample Controlling the Assault of Non-Solicited Pornography & Marketing Checklist	11 — 91
Exhibit 11.11: Sample Telephone Protection Act and Junk Fax Protection Act Checklist	11 — 101
Exhibit 11.12: Cross-Border Privacy Checklist	11 — 111
Exhibit 11.13: Sample E-Banking Information Authentication Checklist	11 — 113
Exhibit 11.14: Outsourcing Information Security Protection Review Checklist.....	11 — 127
Exhibit 11.15: Identity Theft Risk Policy.....	11 — 169

Chapter 12

Examination by Independent Third Parties

Importance of Documentation Process and Monitoring	12 — 1
Scope of Independent Reviews	12 — 2
Findings from Independent Reviews	12 — 2
Regulatory Examinations.....	12 — 2
Exhibit 12.1: FFIEC Examination Objectives for Protecting Consumer Data and Other Privacy Matters (Available Only on CD).....	12 — 6
Exhibit 12.2: Interagency Workprogram RE: Safeguarding of Customer Information (Available Only on CD)	12 — 7
Exhibit 12.3: Sharing Information Table Customer/Noncustomer (Available Only on CD)..	12 — 8

Chapter 13

Data Privacy and MIS Performance

Determining Appropriate Benchmarks for Data Security and Data Privacy	13 — 1
Monitoring Data Performance	13 — 2
Accountability for Reviewing Periodic Reports Tracking Data Security and Data Privacy	13 — 4
Testing, Then Stress Testing, Data Security Controls	13 — 4a
Exhibit 13.1: Customer Data Protection/Privacy Coordinator Action Plan Initial/Next Steps	13 — 5
Exhibit 13.2: Customer Data Protection/Privacy Coordinator Action Plan (Ongoing) Planner.....	13 — 15
Exhibit 13.3: Corporate Governance Organizational Chart	13 — 16
Exhibit 13.4: Data Security and Privacy Risk Ratings Risk Assessment of Data Privacy and Security Concerns by Critical Systems and Support Products	13 — 17
Exhibit 13.5: Customer Data Complaint Tracking System	13 — 22
Exhibit 13.6: Monthly Efficiency Reports	13 — 23
Exhibit 13.7: Information Systems Intrusion Detection Report	13 — 24
Exhibit 13.8: Information Request Report	13 — 25

Exhibit 13.9: Customer Central Information File Administration Schedule 13 — 26
 Exhibit 13.10: Special Customer Data Coordinator Assistants’ “Security ID” Listing 13 — 27
 Exhibit 13.11: Listing of Outside Information Service Providers 13 — 28
 Exhibit 13.12: Listing of Approved Outside Vendor/Service Providers 13 — 29
 Exhibit 13.13: Audit and Examination Issues/Concerns and Stated Corrective Action
 (Plus Internal Reviews) 13 — 30
 Exhibit 13.14: Examination and Audit Corrective Action Followup Grid 13 — 33

Chapter 14 Identity Theft

What Is Identify Theft? 14 — 1
 Identity Theft Techniques 14 — 2
 FDIC Releases Study on Account-Hijacking Identity Theft 14 — 3
 FTC Issues Study About Consumer Fraud 14 — 4
 Privacy: What Each Individual Should Know 14 — 5
 Credit Bureaus 14 — 5
 Department of Motor Vehicles (DMV) 14 — 6
 Direct Marketers 14 — 6
 Telemarketing 14 — 6
 Mail 14 — 6
 E-Mail 14 — 7
 For More Information 14 — 7
 Consumer Insights on What Might Provide Further Assistance 14 — 7
 Identity Theft Facts and Insights 14 — 8
 Anti-Spam Laws Equal New Marketing Challenges for Banks 14 — 9
 Emerging Identity Fraud Tactics 14 — 9
 Tips for Consumers to Protect Against Identity Theft 14 — 10
 General Consumer Tips to Protect Information and Privacy 14 — 10
 Consider the Personal Computer 14 — 11
 Credit Accounts 14 — 12
 Checks 14 — 12
 Social Security Numbers 14 — 13
 If an Individual’s Identity Has Been Stolen 14 — 14
 Tips from the Federal Trade Commission 14 — 14
 Legislative Proposals 14 — 15
 Identify Theft Risk Management 14 — 16
 Exhibit 14.1: Identity Theft Risk Program Questionnaire 14 — 17
 Exhibit 14.2: Identity Theft Risk Policy 14 — 24
 Monitoring to Detect Red Flags 14 — 34
 Appendix A.1: Identity Theft Prevention Program Action Plan 14 — 44
 Appendix A.2: ITPP Implementation Action Plan Checklist 14 — 46
 Appendix A.3: XYZ Bank Anywhere, USA Timeline for Development of Identity
 Theft Prevention Program 14 — 49

Appendix B.1: Sample Covered Accounts or Services — Initial Account Opening/Service (Identity Theft Detection)	14 — 51
Appendix B.2: Sample Covered Accounts or Services — Initial Account Opening/Service (Identity Theft Detection) (Detailed Analysis) — Electronically	14 — 55
Appendix B.3: Sample Covered Accounts or Services — Initial Account Opening/Service Identity Theft Detection (Detailed Analysis) — By Mail.....	14 — 59
Appendix B.4: Sample Covered Accounts or Services — Initial Account Opening/Service Identity Theft Detection (Detailed Analysis) — By Telephone.....	14 — 62
Exhibit 14.3: Identity Theft Risk Procedures	14 — 65
Exhibit 14.4: FDIC Identity Theft Study (Available Only on CD)	14 — 77
Exhibit 14.5: Sample Identity Theft Red Flags Procedures	14 — 78
Exhibit 14.6: You Have the Power to Stop Identity Theft	14 — 84

Appendixes

Appendix A: Glossary

Appendix B: Web Site Resources

Appendix C: FFIEC Training Resources (Available Only on CD)

Appendix D: Quick Reference Guide to Regulatory Issuances

Quick Reference Guide to Regulatory Issuances RE: Data Protection and Data Privacy	D — 1
State Law Considerations	D — 15

Appendix E: Final Rulings on the Gramm-Leach-Bliley Act (GLB Act) (Available Only on CD)

May 10, 2000: Joint Release from Board of Governors of the Federal Reserve System,
Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency,

and Office of Thrift Supervision: Final Regulations for Privacy of Consumer
Financial Information E — 1
February 15, 2001: Interagency Guidelines Establishing Standards for Safeguarding
Customer Information and Rescission of Year 2000 Standards for Safety and Soundness;
Final Rule..... E — 97
December 30, 2003: Interagency Proposal to Consider Alternative Forms of Privacy Notices
Under the Gramm-Leach-Bliley Act, Proposed Rule E — 127