

## Summary Table of Contents

### **Part I — Choosing E-Banking Products and Services**

- Chapter 1: E-Banking: Delivery Mechanism of Choice?
- Chapter 2: Migrating to Electronic Banking
- Chapter 3: Internet Banking: A Whole New World

### **Part II — Implementing Electronic Banking**

- Chapter 4: Developing an Electronic Banking Program
- Chapter 5: Security in E-Commerce

### **Part III — Management and Internal Control**

- Chapter 6: Managing Electronic Banking
- Chapter 7: Internal Controls
- Chapter 8: Internal Audit of Electronic Banking

### **Part IV — Electronic Banking Training**

- Chapter 9: Training: A Necessary Process
- Chapter 10: Sample Training Manual

### **Part V — Regulatory Guidance**

- Chapter 11: Regulatory Examinations
- Chapter 12: [Listing of Issuances and Regulatory Guidelines have been moved to Appendix A.]
- Chapter 13: Setting up an Internet Bank with a National Charter

### **Part VI — Glossary**

Glossary of Electronic Banking Terms

### **Part VII — Appendix A**

Listing of Issuances and Regulatory Guidelines



## Contents

Preface .....	iii
About the Authors .....	v
How to Use This Manual.....	vii
Summary Table of Contents.....	xv

### Part I — Choosing E-Banking Products and Services

#### Chapter 1 E-Banking: Delivery Mechanism of Choice?

General Overview of E-Banking .....	1 — 1
What Is E-Banking? .....	1 — 1
What Are the Components of E-Banking? .....	1 — 1
What Is Infrastructure? .....	1 — 1
What Are Portals? .....	1 — 1
How Does a Search Engine Work? .....	1 — 2
What Is a Call Center? .....	1 — 2
Is There an Organization That Works for Uniformity in E-Banking? .....	1 — 3
What Are the Regulatory Issues Affecting E-Banking? .....	1 — 3
What Are the Fair Information Practice Principles? .....	1 — 3
What Are the Risks to E-Banking? .....	1 — 4
What Are the Measures That Can Be Taken to Minimize the Risks of E-Commerce? .....	1 — 4
Internet Gambling .....	1 — 4
The Rush to Electronic Commerce and Banking .....	1 — 5
Competitive Forces .....	1 — 6
Regulatory-Based Strategic Forces .....	1 — 6
An Electronic Supply Chain: Will Payments Follow? .....	1 — 7
Looking Forward — Further Evolution.....	1 — 8
Business-to-Business E-Commerce .....	1 — 8
Customer Service Online .....	1 — 9
Lower Sales and Marketing Costs.....	1 — 9
Increased Sales Opportunities .....	1 — 9
Challenges to Electronic Commerce .....	1 — 10
Remittances for Immigrant Populations.....	1 — 10
Reasons to Pursue Remittances.....	1 — 11
Reasons Immigrant Populations Do Not Use Banks and Why Institutions Should Pursue This Market .....	1 — 12
Lending to Immigrants.....	1 — 13
Customer Identification.....	1 — 14

Security Breaches Over the Internet.....	1 — 15
Taxes and the Internet .....	1 — 15
Internal Controls and Audit.....	1 — 16
Reliability and Privacy .....	1 — 16
Retail Payment System: Payment Clearing and Electronic Settlement.....	1 — 19
FDIC and Federal Reserve Bank of Chicago Research Payment System Issues .....	1 — 19
Global Electronic Payments .....	1 — 20
Issues That Affect Cross-Border Payments.....	1 — 21
Policy Issues Facing Central Banks, Retail Payments .....	1 — 21
Federal Reserve Board Finalizes Policy on Payments System Risk (PSR), Fourth Quarter 2004.....	1 — 22
Primary Revisions to the Policy in Payment System Risk.....	1 — 23
Nonbanks in the Payments System: A Book Published by the Federal Reserve Bank of Kansas City .....	1 — 25
Conclusion.....	1 — 26
Exhibit 1.1: Automated Clearing House Activities (domestic) Industrialized Nations' Approaches ...	1 — 27

## Chapter 2

### Migrating to Electronic Banking

Retail Payment Systems: Payment Instruments, Clearing, and Electronic Settlement .....	2 — 1
Check-Based Payments .....	2 — 2
Check Clearinghouses .....	2 — 3
Card-Based Electronic Payments .....	2 — 5
Credit and Charge Cards .....	2 — 5
General-Purpose Credit Cards .....	2 — 5
Co-Branded/Affinity Credit Cards .....	2 — 6
Private Label (Store) Credit Cards.....	2 — 6
Bankcard Associations.....	2 — 7
Debit and Automated Teller Machine (ATM) Cards .....	2 — 9
ATM Cards .....	2 — 10
EFT/POS Networks.....	2 — 10
Stored Value Cards .....	2 — 12
Other Electronic Payments.....	2 — 14
Online P2P Payments and Electronic Cash.....	2 — 14
Electronic Cash .....	2 — 15
Electronic Benefits Transfer (EBT) .....	2 — 15
The Automated Clearinghouse (ACH).....	2 — 16
The ACH Network .....	2 — 16
Payments System Risk (PSR) Policy .....	2 — 19
Which Format Is Best For Your Institution? .....	2 — 20
The Personal Computer as a Delivery System .....	2 — 21
Public Networks and the Internet .....	2 — 22
Infrastructure Requirements.....	2 — 24
Offering Services Through Public Networks.....	2 — 24
Strengths .....	2 — 25
Weaknesses .....	2 — 25
Personal Computers and Private Networks .....	2 — 26
Infrastructure Requirements for Private Networks Based on PCs .....	2 — 27

Offering Services Through Private Networks.....	2 — 28
Advantages.....	2 — 28
Disadvantages.....	2 — 28
Existing Online Services Vendors.....	2 — 29
The Intranet.....	2 — 29
The Telephone as a Delivery System.....	2 — 30
Screen Phones as a Delivery Mechanism.....	2 — 31
Fixed-Site Machines as a Delivery Mechanism.....	2 — 32
Card-Based Devices as a Delivery Mechanism.....	2 — 33
Consumer Credit Cards.....	2 — 34
Debit Cards.....	2 — 34
Business Cards.....	2 — 36
Purchasing Cards.....	2 — 37
Merchant Processing Cards.....	2 — 38
Smart Cards.....	2 — 38
Prepaid Cards.....	2 — 39
Federal Reserve Board Proposes Amendments to Regulation E Regarding Payroll Cards.....	2 — 41
Different Systems: Closed, Semi-Closed, Semi-Open, and Open.....	2 — 43
Interactive Television.....	2 — 46
Check 21 Act.....	2 — 47
Federal Reserve Board Finalizes Check 21, Effective October 28, 2004.....	2 — 47
The Impact of Check 21.....	2 — 48
Check 21 Specifics.....	2 — 48
Substitute Checks.....	2 — 49
Electronic Check Presentment.....	2 — 49
Bank Responsibilities.....	2 — 50
Expedited Recrediting for Consumers.....	2 — 50
Expedited Recrediting for Banks.....	2 — 51
Consumer Notices.....	2 — 52
Opportunities Created by Substitute Checks.....	2 — 52
Risk Analysis.....	2 — 54
Exhibit 2.1: Check 21 Internal Control Questionnaire.....	2 — 55
Exhibit 2.2: Retail Payments System Examination Checklist.....	2 — 61

## Chapter 3

### Internet Banking: A Whole New World

How Does Internet Banking Operate?.....	3 — 2
Cyberspace: The New Branch Bank of the Future?.....	3 — 5
Lower Operating Costs.....	3 — 6
A Different Customer and New Competitors.....	3 — 7
Customer Acceptance.....	3 — 7
Potential Benefits of Internet Banking.....	3 — 8
Offering Products through the Internet.....	3 — 9
Differentiating Internet Service and Incenting Usage.....	3 — 11
Internet Banking, Markets, and Examinations.....	3 — 12

Complying with Federal Regulations.....	3 — 14
Scammers and Potential Fraudsters Pose as Government Operations .....	3 — 16
Identity Theft.....	3 — 18
Account Hijacking.....	3 — 19
Definition of Identity Theft.....	3 — 20
Survey of the Problem of Account Hijacking.....	3 — 21
Account Hijacking Methods .....	3 — 22
What Is the Cost of Identity Theft?.....	3 — 22
FDIC Explores Using Technological Solutions to a Technological Problem.....	3 — 23
Corporate Governance Tips for Preventing ID Theft.....	3 — 23
Transaction Cards.....	3 — 24
OCC Reminds Consumers and Banks About Gift Card Conditions .....	3 — 24
Fed to Study Debit Card Fees .....	3 — 24a
ACH TRansactions.....	3 — 25
National Automated Clearing House Association’s Operating Rules Amended .....	3 — 25
Managing Foreign Third-Party Relationships .....	3 — 26
Improperly Managed Electronic Disclosures May Lead to Increased Risks.....	3 — 27
Setting Up a Web Site .....	3 — 29
Infrastructure Technologies.....	3 — 29
Types of Hardware.....	3 — 29
Types of Software .....	3 — 29
Types of Services .....	3 — 30
Types of Web Sites .....	3 — 30
Information Choices.....	3 — 31
The Primary Privacy Issues.....	3 — 33
Virtual Paper Shredders .....	3 — 34
Site Development .....	3 — 34
E-Commerce for Credit Unions.....	3 — 35
Smaller Institutions Operating on the Internet.....	3 — 36
Oversight and Institution Strategy .....	3 — 37
Plan for Technology Use.....	3 — 37
Policies and Procedures .....	3 — 38
Risk Management Process.....	3 — 38
Risk Assessment as an Ongoing Process .....	3 — 39
Security Program Development Process.....	3 — 40
Physical Security vs. Information Security.....	3 — 40
Planning the Response to a Breach.....	3 — 41
Legal and Regulatory Compliance Considerations.....	3 — 41
Third-Party Assessments.....	3 — 42
Managing Third-Party Service Provider Relationships.....	3 — 43
Business Continuity.....	3 — 44
Research .....	3 — 45
FDIC Vendor Notification Requirement.....	3 — 46
Weblinking.....	3 — 46
Risks .....	3 — 47
Risk Management.....	3 — 48
Identifying Risk Areas .....	3 — 49
Reputation Risk.....	3 — 49
Compliance Risk.....	3 — 49

Risk Management Techniques .....	3 — 50
Account Aggregation Services .....	3 — 50
Privacy .....	3 — 52
Data Collection and Interactivity .....	3 — 53
Privacy Disclosures .....	3 — 54
Content of Disclosures .....	3 — 56
Results for the 50 Largest Institutions .....	3 — 58
Customer Identification Program (CIP) Requirements .....	3 — 60
Undertaking Implementation.....	3 — 61
Looking at Work Remaining.....	3 — 63
Future Points to Consider.....	3 — 63
PC/LAN Growth and Internet Access .....	3 — 65
Information Technology Security .....	3 — 67
Exhibit 3.1: Federal Privacy Laws and Regulations — A Summary.....	3 — 69
Exhibit 3.2: Online Privacy Practices .....	3 — 72
Exhibit 3.3: Sample Home Page Designs .....	3 — 75
Exhibit 3.4: Internet Banking Availability.....	3 — 78
Exhibit 3.5: Interagency Financial Institution Web Site Privacy Survey Report.....	3 — 80
Exhibit 3.6: Sample Customer CIP Notice for Electronic Banking.....	3 — 81

## **Part II — Implementing Electronic Banking**

### **Chapter 4 Developing an Electronic Banking Program**

Defining and Presenting the Proposal .....	4 — 1
Timing the Proposal Presentation.....	4 — 2
Sell It the First Time It’s Presented.....	4 — 2
Be Prepared to Explain the Benefits.....	4 — 3
Be Prepared with Specific Examples .....	4 — 4
Remember That Approval Also Creates Expectations.....	4 — 4
What About the Rejected Proposal?.....	4 — 5
Next Steps and Timelines.....	4 — 5
Internal and External System Failure .....	4 — 8
Research, Feasibility Study, and Development.....	4 — 9
The Importance of Market Research.....	4 — 10
Technology and Change.....	4 — 10
Beta Testing and Other Concerns.....	4 — 11
Privacy Issues in Electronic Banking.....	4 — 12
An Ongoing Commitment to Technology.....	4 — 12
Avoiding Mistakes .....	4 — 13
Don’t Forget Those Regulatory Concerns.....	4 — 13
Gramm-Leach-Bliley (GLB) Act .....	4 — 14
Children’s Online Privacy Protection Act (COPPA) .....	4 — 15
Customer Identification Program (CIP) .....	4 — 16

Undertaking Implementation.....	4 — 16
Looking at Work Remaining.....	4 — 17
Future Points to Consider.....	4 — 18
Board of Directors' Final Sign-Off.....	4 — 19
Time to Market and Sell.....	4 — 19
Subsequent Assessment of System.....	4 — 20
Accessibility Through Call Centers.....	4 — 20
Benefits of Call Centers.....	4 — 21
Development of a Call Center — Commitment by Management Is Essential.....	4 — 21
Exhibit 4.1: Electronic Banking Outline.....	4 — 22
Exhibit 4.2: Presentation to Board of Directors and Senior Management Sample	
Discussion Outline.....	4 — 32
Exhibit 4.3: Initial/Next Steps Action Plan.....	4 — 35
Exhibit 4.4: Customer Service Delivery Preferences Survey.....	4 — 42

## Chapter 5

### Security in E-Commerce

The Five Components of Security Control.....	5 — 3
Control Environment.....	5 — 3
Risk Assessment.....	5 — 5
Data Review.....	5 — 6
Evaluating Analysis Tools.....	5 — 6
Control Activities.....	5 — 7
Ergonomic Considerations in E-Banking and E-Commerce.....	5 — 7
Accounting, Information, and Communication Systems.....	5 — 8
Simplification of Procurement Processes.....	5 — 8
Automation of Routine or Repetitive Tasks.....	5 — 9
Consolidation of Redundant Resources.....	5 — 10
Standardization of Data and Processes.....	5 — 10
Strategic Alignment of Procurement Activities with Overall Corporate Goals	
and Suppliers.....	5 — 11
Self-Assessment and Monitoring.....	5 — 11
Internal Security Control System Design.....	5 — 12
Risk Assessment.....	5 — 14
Control Activities.....	5 — 18
Accounting, Information, and Communication Systems.....	5 — 23
Self-Assessment or Monitoring.....	5 — 24
Other Security Control Considerations.....	5 — 26
Managing the Risks.....	5 — 26
Information Technology Security.....	5 — 27
Information Security Risk Management Practices.....	5 — 28
Information Security Practices Specifically Addressing Electronic Banking.....	5 — 30
Risk Measurement, Monitoring, and Management Information Systems.....	5 — 30
Electronic Banking Information Security Focus Points.....	5 — 31
Accountability.....	5 — 31
Authorization.....	5 — 31

Access .....	5 — 32
Authentication .....	5 — 33
Data Transmission and Storage .....	5 — 33
Encryption and Digital Signatures .....	5 — 34
Firewalls .....	5 — 34
Acknowledgment .....	5 — 35
Confidentiality .....	5 — 35
E-Mail Do's .....	5 — 35
Treat E-Mail as a Business Record .....	5 — 36
Security and the Internet .....	5 — 36
Grade of Service Use in Evaluating Service Levels .....	5 — 37
Confidentiality of Information Transmitted over Public Networks .....	5 — 37
Examination Insights on Web Sites .....	5 — 38
Security Concerns for Private Networks .....	5 — 38
Security Program Key Components .....	5 — 40
Prevention .....	5 — 40
Detection .....	5 — 41
Response .....	5 — 42
Conclusion .....	5 — 42
Exhibit 5.1: Risk Analysis Tables .....	5 — 43
Exhibit 5.2: Risk Management for Electronic Banking .....	5 — 44
Exhibit 5.3: Security and Confidentiality Agreement .....	5 — 50
Exhibit 5.4: Information Security Questionnaire .....	5 — 55
Exhibit 5.5: Data Review Modeling Worksheet .....	5 — 61
Exhibit 5.6: Risk Management Checklist .....	5 — 62
Exhibit 5.7: Internet Fraud Preventive Measures .....	5 — 63

## **Part III — Management and Internal Control**

### **Chapter 6 Managing Electronic Banking**

Establishing a Management Approach .....	6 — 1
Management Responsibility .....	6 — 1
E-Banking Management Manual: Corporate Governance Policies .....	6 — 3
Electronic Banking Policy .....	6 — 4
Electronic Funds Transfer Policy .....	6 — 16
Online Privacy Policy .....	6 — 21
Customer Data Protection/Privacy Policy .....	6 — 28
Debit Card Products Policy .....	6 — 45
Electronic Mail (E-Mail) Systems Policy .....	6 — 52
Internet Access Policy .....	6 — 59
E-Banking Training and Education Policy .....	6 — 67
E-Banking Security Policy .....	6 — 74
Information Security Policy .....	6 — 98

Outsourcing Policy .....	6 — 110
Customer Identification Program Policy .....	6 — 122
Server Security Policy .....	6 — 136
Data and Records Destruction Policy .....	6 — 149
Electronic Banking Information Authentication Policy .....	6 — 162
Prepaid Cards Policy .....	6 — 171
Automated Clearing House Policy .....	6 — 187
Remote Deposit Capture Policy .....	6 — 197
Identity Theft Risk Policy .....	6 — 211
Incident Response Policy .....	6 — 225

## Chapter 7 Internal Controls

Building Internal Control Systems .....	7 — 1
Information Security .....	7 — 3
Establishing Accountability .....	7 — 4
Authorization, Access, and Authentication .....	7 — 4
Data Security and Confidentiality .....	7 — 5
Cyber-Terrorism .....	7 — 6
Input and Output Controls .....	7 — 8
Data Integrity .....	7 — 9
Separation of Duties .....	7 — 10
Change Controls .....	7 — 10
Other Control Issues .....	7 — 11
Internet Activities .....	7 — 11
Electronic Mail (E-Mail) .....	7 — 13

## Chapter 8 Internal Audit of Electronic Banking

Audits of Planning and Implementation .....	8 — 1
Audit of Operating Policies and Procedures .....	8 — 2
Audit of Monitoring Activities .....	8 — 2
Legal and Regulatory Issues .....	8 — 3
Audit of Vendors and Outsourcing Relationships .....	8 — 4
Suggested Audit Approaches .....	8 — 4
Basel Committee Insights on Possible Risks .....	8 — 5
Internal Audit Procedures — Electronic Banking Policy .....	8 — 7
Electronic Banking Policy Checklist .....	8 — 14
Internal Audit Procedures Electronic Funds Transfer Systems Policy .....	8 — 28
Internal Audit Procedures Electronic Funds Transfer Systems Policy Checklist .....	8 — 30
Electronic Fund Transfer Systems Policy Checklist .....	8 — 35
LAN Security Checklist .....	8 — 40

Data Processing Checklist .....	8 — 48
Fed-Line Checklist .....	8 — 52
Server Security Policy Checklist .....	8 — 55
Server Security Policy Checklist .....	8 — 70

**Part IV — Electronic Banking Training**

**Chapter 9  
Training: A Necessary Process**

Identifying Needs and Organizing Training .....	9 — 1
Training Group Identifiers .....	9 — 2
Training Dates and Priorities.....	9 — 3
Training Modules and Scope.....	9 — 3
Developing a Program.....	9 — 4
Training Preparation.....	9 — 4
Identifying the Target Audience .....	9 — 4
Developing Training Resources and Support Materials .....	9 — 5
Conducting the Training Sessions.....	9 — 5
Overview of Electronic Banking.....	9 — 6
Electronic Banking Terminology.....	9 — 6
Risks and Compliance Issues.....	9 — 6
Helpful Training Hints .....	9 — 7
Making Training Fit Your Organization .....	9 — 7
Exhibit 9.1: Sample Preclass Reading Material.....	9 — 9
Exhibit 9.2: Sample Preclass Reading Material.....	9 — 16
Exhibit 9.3: Sample Preclass Reading Material.....	9 — 22

**Chapter 10  
Sample Training Manual**

Electronic Banking Training Overheads .....	10 — 5
Training Objectives .....	10 — 5
Electronic Banking Defined .....	10 — 5
Types of Mechanisms Used to Deliver Electronic Banking Products and Services .....	10 — 6
Advantages of Offering PC-Based Services Through a Public Network .....	10 — 6
Disadvantages of Offering PC-Based Services Through a Public Network.....	10 — 7
What Are the Challenges to Electronic Commerce? .....	10 — 7
Internet Banking Defined .....	10 — 8
Why Is Internet Banking a Preferred Service Delivery Mechanism?.....	10 — 8
Sample Home Page Design .....	10 — 9
Types of Internet Sites.....	10 — 10

Internet Access Policy .....	10 — 10
Potential Benefits of Internet or Online Banking .....	10 — 11
Potential Disadvantages of Internet or Online Banking .....	10 — 11
With Approved Internet Access, Remember.....	10 — 12
Information Security.....	10 — 13
Information Security and Our Bank .....	10 — 13
Information Security — Violations .....	10 — 14
Information Security — “Social Engineering” .....	10 — 14
Cyber-Terrorism Is a Concern; Internet Use Requires Caution.....	10 — 15
Phases of Development and Implementation .....	10 — 16
Beta Testing Defined.....	10 — 16
Potential Pitfalls .....	10 — 17
Factors to Consider in Your Follow-up Performance Assessment.....	10 — 17
Recommendations for Protecting Customer Information.....	10 — 18
The Board’s Role in Managing Risks Associated with Information Security.....	10 — 18
Elements of an Effective Information Security Policy .....	10 — 19
Internal Control .....	10 — 19
Establishing Internal Control Systems .....	10 — 20
How Are Networks Vulnerable to Information Security Attacks?.....	10 — 20
Types of Internal Control .....	10 — 21
New Technology for Identity Authentication.....	10 — 21
Privacy Issues .....	10 — 22
Laws and Regulations that Affect Privacy Issues .....	10 — 22
Elements of an Effective Privacy Policy .....	10 — 23
Planning and Deployment Risks .....	10 — 23
Operating Policies and Procedures Risks .....	10 — 24
Legal and Regulatory Risks.....	10 — 24
Administration and System Operations Risks .....	10 — 25
Vendor and Outsourcing Risks.....	10 — 25
Potential Management Reports.....	10 — 26
Safeguarding Customer Information .....	10 — 27

## **Part V — Regulatory Guidance**

### **Chapter 11 Regulatory Examinations**

Potential Regulatory Problem Areas .....	11 — 1
Home Pages and Web Sites.....	11 — 1
Internet Applications .....	11 — 4
E-Mail Correspondence.....	11 — 7
Competition and Compliance.....	11 — 8
Frequently Cited Violations of Regulation E.....	11 — 9
Privacy Issues.....	11 — 9
Privacy Seals.....	11 — 10

Use of Vendors.....	11 — 11
Other Considerations.....	11 — 12
Fair and Accurate Credit Transactions Act.....	11 — 13
Proper Disposal of Consumer Information.....	11 — 13
Board Oversight.....	11 — 15
Specific Goals.....	11 — 16
Policy Elements.....	11 — 16
Destruction Authorization.....	11 — 17
Informal Destruction.....	11 — 17
Formal Officer Authorization.....	11 — 18
Formal Information Destruction as Directed by the Records Retention Policy and Schedule.....	11 — 18
Destruction of Confidential Data.....	11 — 19
Document Destruction Log(s).....	11 — 19
Methods of Destruction.....	11 — 20
Outside Vendor Support.....	11 — 21
Special Handling of Sensitive Information.....	11 — 22
Monitoring.....	11 — 23
External Reviews.....	11 — 24
External Training.....	11 — 24
Audit.....	11 — 25
Personal Computers and Privacy.....	11 — 25
Pre-Examination Preparation.....	11 — 26
Internet Banking Risks.....	11 — 28
Credit Risk.....	11 — 28
Interest Rate Risk.....	11 — 29
Liquidity Risk.....	11 — 29
Price Risk.....	11 — 30
Foreign Exchange Risk.....	11 — 30
Transaction Risk.....	11 — 31
Compliance Risk.....	11 — 32
Strategic Risk.....	11 — 33
Reputation Risk.....	11 — 34
Risk Assessment.....	11 — 35
Risk Management.....	11 — 36
Exhibit 11.1: Sample Review/Examination Procedures.....	11 — 41
Exhibit 11.2: Examples of Possible Risks and Risk Management Measures in Retail Electronic Banking and Electronic Money.....	11 — 59
Exhibit 11.3: Disposal of Consumer Report Information and Records.....	11 — 68
Exhibit 11.4: Data and Records Destruction Policy Checklist.....	11 — 70
Exhibit 11.5: Personal Computer End-User Security Checklist.....	11 — 75

## Chapter 12

### Issuances and Regulatory Guidance

(Listing of Issuances and Regulatory Guidelines has been moved to Appendix A.)

## Chapter 13

### Setting Up an Internet Bank with a National Charter

General Information .....	13 — 1
Chartering a New Internet Bank.....	13 — 2
Acquiring the Stock of an Existing National Bank .....	13 — 2
Converting to a National Bank.....	13 — 4
Types of Electronic Banking.....	13 — 4
Informational Web .....	13 — 5
Transactional Web.....	13 — 5
Wireless.....	13 — 5
Personal Computer Banking.....	13 — 6
Application Process .....	13 — 6
Exploratory Inquiry .....	13 — 7
Prefiling Discussions and Meetings .....	13 — 7
Preparation of Filing.....	13 — 8
Application Issues .....	13 — 8
Branching.....	13 — 9
Capital .....	13 — 11
Liquidity.....	13 — 12
Contingency Funding Plan.....	13 — 13
Alternative Business Strategy .....	13 — 14
Management Selection.....	13 — 14
Narrowly Focused Operations .....	13 — 15
Use of Vendors.....	13 — 16
Verification and Authentication.....	13 — 18
Internal Controls .....	13 — 19
Business Resumption Contingency Planning.....	13 — 19
Cross-Border Operations.....	13 — 20
Organization Costs.....	13 — 20
Community Reinvestment Act (CRA).....	13 — 21
Field Investigation.....	13 — 22
Decisions .....	13 — 23
Preliminary Conditional Approval.....	13 — 23
Final Conditional Approval .....	13 — 24
Pre-opening Examination.....	13 — 25
Opening .....	13 — 25
Supervision and Oversight .....	13 — 26
Board of Directors' Oversight.....	13 — 26
Supervision by Risk.....	13 — 28
Risk Considerations.....	13 — 29
Outsourcing.....	13 — 29
Information System Security.....	13 — 29
Firewalls.....	13 — 31
Intrusion Detections and Management.....	13 — 32
Encryption.....	13 — 32
Backup and Recovery.....	13 — 33
Customer Confusion.....	13 — 33

Hypertext Links to Third Parties.....	13 — 33
Weblinking.....	13 — 34
Risks.....	13 — 34
Risk Management.....	13 — 36
Identifying Risk Areas .....	13 — 36
Reputation Risk.....	13 — 36
Compliance Risk.....	13 — 37
Risk Management Techniques .....	13 — 37
Trade Names .....	13 — 38
Liability Insurance .....	13 — 39
Examination Frequency and Scope .....	13 — 40
The Evaluation Process .....	13 — 40
Compliance Supervision .....	13 — 42
Privacy .....	13 — 42
Advertising.....	13 — 43
Fair Lending Statutes .....	13 — 44
Exhibit 13.1: OCC Contacts.....	13 — 45
Exhibit 13.2: Wireless Networks Risk Management Checklist .....	13 — 50
Exhibit 13.3: Data Processing Procedures Checklist.....	13 — 55
Exhibit 13.4: Debit Card Product Procedures Checklist.....	13 — 63

**Part VI — Glossary of Electronic Banking Terms**

**Part VII — Appendix A: Listing of Issuances and Regulatory Guidelines**