

Summary Table of Contents

Chapter 1	Growth and Detection of Identity Theft
Chapter 2	How Information Is Illegally Obtained and Used
Chapter 3	Assisting Victims of Identity Theft
Chapter 4	Basics of Prevention
Chapter 5	Interagency Identity Theft Red Flag Guidelines
Chapter 6	Information Security Requirements
Chapter 7	Customer Identification Program Requirements
Chapter 8	Fair Credit Reporting Act
Chapter 9	Related Policies and Procedures
Chapter 10	Corporate Originators of ACH Transactions
Chapter 11	Credit Card Fraud
Chapter 12	Fraud Involving ATM and Debit Cards

Appendixes

Appendix A	FTC's ID Theft Affidavit
Appendix B	FTC's ID Theft: What's It All About?
Appendix C	Red Flag Proposed Rule
Appendix D	FTC's Deter, Detect, Defend
Appendix E	FTC's Credit, ATM, and Debit Cards: What to Do If They're Lost or Stolen
Appendix F	Sample E-Sign Customer Agreement
Appendix G	Sample Online Access Agreement

Identity Theft Red Flag Toolkit

Contents

Chapter 1 Growth and Detection of Identity Theft

What Is Identity Theft?	1 — 1
Background: Growth and Detection	1 — 2
Identity Theft Data Clearinghouse.....	1 — 2
Efforts by Law Enforcement.....	1 — 2
President’s Identity Theft Task Force.....	1 — 2
Working Across Agencies to Disrupt Identity Theft.....	1 — 4
Federal Laws on Identity Theft.....	1 — 5
Identity Theft and Assumption Deterrence Act.....	1 — 5
Gramm-Leach-Bliley Act.....	1 — 5
Security Standards	1 — 6
The Fair and Accurate Credit Transaction Act (FACT Act).....	1 — 6

Chapter 2 How Information Is Illegally Obtained and Used

How Information Is Obtained	2 — 1
Personal Theft.....	2 — 1
Mail Theft.....	2 — 1
Third Parties.....	2 — 1
Dumpster Diving	2 — 2
Shoulder Surfing.....	2 — 2
Skimming.....	2 — 2
Unauthorized Credit Reports	2 — 3
Electronically Transmitted Information.....	2 — 3
Phishing	2 — 3
Pretext Calling	2 — 4
How Information Is Used.....	2 — 4
Overview	2 — 4
Illegal Uses of Information.....	2 — 5
Obtaining Identity Cards	2 — 5
Obtaining Employment	2 — 5
Tax Fraud	2 — 5

Account Hijacking.....	2 — 5
Credit Card Fraud.....	2 — 5
Loan Fraud.....	2 — 6
Mortgage Loan Fraud.....	2 — 6
Asset Rental Fraud.....	2 — 6
Debt Elimination Fraud.....	2 — 7
Checking Accounts.....	2 — 7
Filing Bankruptcy.....	2 — 7
Credit Card Loss Protection Offers.....	2 — 7
Providing the Identity Theft Victim’s Identity During an Arrest.....	2 — 7
Exhibit 2.1: Case Illustrations.....	2 — 8

Chapter 3

Assisting Victims of Identity Theft

Requirements of the Fair Credit Reporting Act.....	3 — 1
Fraud Alerts and Active Duty Alerts.....	3 — 1
Providing Records to Victims of Identity Theft.....	3 — 2
Information Available to Victims.....	3 — 2
Verification of Identity and Claim.....	3 — 3
Format of Request.....	3 — 3
Declining to Provide Information.....	3 — 4
Limitation on Civil Liability/Safe Harbor.....	3 — 4
Recordkeeping Obligations.....	3 — 4
What to Tell Victims of Identity Theft.....	3 — 4
Using the FTC’s Affidavit.....	3 — 5
President’s Identity Theft Task Force.....	3 — 6
Restitution.....	3 — 7
Universal Police Report.....	3 — 7
Exhibit 3.1: Sample Procedures for Responding to Identity Theft Victims.....	3 — 9
Exhibit 3.2: Sample Letter to Out-of-Area Identity Theft Victims.....	3 — 12

Chapter 4

Basics of Prevention

What Organizations Can Do to Prevent Identity Theft.....	4 — 1
Verification Procedures for New Accounts.....	4 — 1
Positive Verification.....	4 — 2
Logical Verification.....	4 — 2
Negative Verification.....	4 — 2

Third-Party Verification	4 — 2
Using Consumer Reports	4 — 2
Verifying Change of Address Requests	4 — 3
Security Standards	4 — 3
Risk Mitigation for E-Mail-Related Frauds	4 — 3
Prevention	4 — 4
Detection	4 — 5
Response	4 — 5
Risk Mitigation — Pretext Calling	4 — 5
Limiting Telephone Disclosures	4 — 6
Employee Training	4 — 6
Testing	4 — 7
Risk Mitigation — Automated Loan Processing	4 — 7
Third-Party Due Diligence	4 — 7
What Customers Can Do	4 — 7
Tools for Consumers	4 — 7
Teaching Prevention	4 — 7
Active Duty Alerts for Military Personnel	4 — 9
Protecting Social Security Numbers	4 — 10
Additional Information	4 — 10

Chapter 5

Interagency Identity Theft Red Flag Guidelines

Businesses Subject to the Identity Theft “Red Flag” Rules	5 — 1
Accounts Subject to the Identity Theft “Red Flag” Rules	5 — 2
Account	5 — 2
Development and Implementation of an Identity Theft Prevention Program	5 — 3
Red Flag Policies and Procedures	5 — 3
Identifying Red Flags	5 — 3
Detection of Red Flags	5 — 5
Responding to Detected Red Flags	5 — 6
Written Identity Theft Prevention Program	5 — 7
Incorporating Existing Policies and Procedures in Your Program	5 — 9
Using Existing Automated Fraud Programs	5 — 10
Identity Theft Prevention and Mitigation	5 — 10
Verify Identity of Persons Opening Accounts	5 — 10
Assess the Risk of Identity Theft	5 — 11
Risk Evaluation	5 — 11
Categories of Identity Theft	5 — 11
Which of Your Accounts or Groups of Accounts Are Subject to a Risk of Identity Theft? ...	5 — 12
Methods to Open These Accounts	5 — 12
Methods to Provide Your Customer’s Access to These Accounts	5 — 13

Size, Location, and Customer Base	5 — 13
Address the Risk of Identity Theft.....	5 — 14
Monitoring an Account for Evidence of Identity Theft.....	5 — 14
Contacting the Customer	5 — 15
Changing Any Passwords, Security Codes, or Other Security Devices That Permit	
Access to a Customer’s Account	5 — 15
Reopening an Account with a New Account Number or Closing an Existing Account	5 — 15
Not Opening a New Account	5 — 15
Implementing Any Requirements Regarding Limitations on Credit Extensions	5 — 15
Implementing Any Requirements for Furnishers of Information to Consumer Reporting	
Agencies to Correct or Update Inaccurate or Incomplete Information	5 — 16
Example of ID Theft “Red Flags” and Responses.....	5 — 16
Service Provider Arrangements.....	5 — 18
Board of Directors and Senior Management Involvement	5 — 18
Staff Training.....	5 — 19
Special Rules for Card Issuers	5 — 19
“Cardholders” Protected by the Rule.....	5 — 19
Address Validation Requirements	5 — 20
Alternative Timing of Address Validation	5 — 21
Form of Notice	5 — 21
Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal.....	5 — 22
Applicability of the Rules.....	5 — 22
Notice of Address Discrepancy	5 — 22
Response to Notice of Address Discrepancy.....	5 — 23
Requirement to Furnish Consumer’s Address to a Consumer Reporting Agency	5 — 23
Timing of Furnishing Consumer’s Address to CRA	5 — 24
Exhibit 5.1 Appendix A to Part 681 — Interagency Guidelines on Identity Theft	
Detection, Prevention, and Mitigation.....	5 — 26
Exhibit 5.2: Supplement A to Appendix A.....	5 — 29
Exhibit 5.3: Sample Identity Theft Policy	5 — 33
Exhibit 5.4: Procedures Relating to Identity Theft Prevention.....	5 — 36
Exhibit 5.5: Sample Training Outline.....	5 — 43
Exhibit 5.6: Identity Theft “Red Flags” and Responses.....	5 — 45

Chapter 6

Information Security Requirements

Standards for Safeguarding Customer Information	6 — 4
Definitions	6 — 4
Information Security Program	6 — 4
Objectives	6 — 4
Elements	6 — 5
Disposal of Consumer Report Information.....	6 — 5

Implementing Security Programs	6 — 5
Securing Information.....	6 — 6

Chapter 7

Customer Identification Program Requirements

Background.....	7 — 1
CIP Requirements	7 — 1
Accounts Subject to CIP Requirements	7 — 2
Exemptions	7 — 2
Customers Subject to CIP Requirements	7 — 2
Additional or Substitute Account Holders.....	7 — 3
Accounts with Power of Attorney	7 — 3
Signatories	7 — 3
Accounts Held by Minors.....	7 — 4
Trust Accounts and Escrow Accounts	7 — 4
Pension Plan Administrators.....	7 — 4
Administrators of Non-ERISA Accounts	7 — 5
Exemptions	7 — 5
Banks	7 — 5
Persons Eligible for Automatic CTR Exemption	7 — 6
Existing Customers.....	7 — 6
Required Contents for Customer Identification Program	7 — 6
Reliance on Third Parties.....	7 — 7
Identity Information Collection and Verification	7 — 8
Required Customer Information to Be Collected	7 — 8
Exception for Persons Applying for a Taxpayer Identification Number.....	7 — 9
Trusts and Taxpayer Identification Number.....	7 — 9
Members of Religious Groups That Have No SSN.....	7 — 10
Special Rule for Credit Card Accounts	7 — 10
Customer Verification	7 — 10
Verification Through Documents.....	7 — 11
Consular ID Cards	7 — 11
Verification Through Nondocumentary Methods	7 — 12
Additional Procedures for Certain Signatories	7 — 12
Lack of Verification.....	7 — 13
Recordkeeping	7 — 13
Comparison with Government Lists	7 — 14
Customer Notice	7 — 15
Additional Exemptions	7 — 15

Chapter 8

Fair Credit Reporting Act

Persons Subject to the FCRA.....	8 — 1
Consumer Reporting Agencies.....	8 — 1
Joint Users of Consumer Reports.....	8 — 2
Information Subject to the FCRA.....	8 — 2
Information That Is Considered to Be a Consumer Report.....	8 — 2
Information That Is Not Considered to Be a Consumer Report.....	8 — 3
Transaction or Experience Information.....	8 — 3
Communications with Affiliates.....	8 — 4
Authorization or Approval of Credit Extensions.....	8 — 5
Notification of Credit Decisions to an Intermediary.....	8 — 5
Background Checks for Employment Purposes.....	8 — 5
Joint Users of Consumer Reports.....	8 — 5
Permissible Uses of Consumer Reports.....	8 — 5
Use of Consumer Reports for Business Loans.....	8 — 6
Certification by Users of Consumer Reports.....	8 — 7
Notices to Users and Furnishers.....	8 — 7
Adverse Action Notice Requirements.....	8 — 7
Adverse Actions Based on Information Obtained from a Consumer Reporting Agency.....	8 — 7
Adverse Actions Based on Information Obtained from Third Parties That Are Not Consumer Reporting Agencies or Affiliates.....	8 — 8
Notifying Multiple Applicants in Cases of Adverse Action.....	8 — 8
Obligations of Prescreened Lists Users.....	8 — 9
Prescreen Opt-Out Notice.....	8 — 10
Short Notice.....	8 — 10
Long Notice.....	8 — 11
“Simple and Easy to Understand”.....	8 — 11
Model Forms.....	8 — 12
Error Resolution and Information Reporting.....	8 — 12
Duties After Notice of Dispute from a Consumer.....	8 — 12
Duties After Notice of Dispute from a Consumer Reporting Agency.....	8 — 12
Duty to Provide Notice of Closed Accounts.....	8 — 13
Duty to Provide Notice of Delinquency of Accounts.....	8 — 13
FACT Act-Related Amendments to FCRA.....	8 — 13
Important FACT Act Definitions.....	8 — 13
Definition of “Identity Theft” (16 CFR 603.2).....	8 — 13
Definition of “Identity Theft Report” (16 CFR 603.3).....	8 — 13
Appropriate Proof of Identity (16 CFR 614.1).....	8 — 15
Fraud Alerts and Active Duty Alerts.....	8 — 15
Providing Identity Theft-Related Records to Victims.....	8 — 16
Content of Victim’s Request.....	8 — 17
Responding to the Customer’s Request.....	8 — 18
Limitations on Liability.....	8 — 19

Recordkeeping	8 — 19
Affirmative Defense in Civil Actions	8 — 19
Blocking Information Resulting from Identity Theft	8 — 19
Prevention of Repollution of Consumer Reports	8 — 20
Prohibition of Sale or Transfer of Debt Caused by Identity Theft	8 — 20
Disposal of Consumer Report Information	8 — 20
Improved Disclosure Disputed Information Results	8 — 21
Truncation of Credit Card and Debit Card Account Numbers	8 — 21
Summary of Rights of Identity Theft Victims	8 — 22
Businesses Subject to the Identity Theft “Red Flag” Rules	8 — 23
Accounts Subject to the Identity Theft “Red Flag” Rules	8 — 23
Account	8 — 23
Development and Implementation of an Identity Theft Prevention Program	8 — 24
Red Flag Policies and Procedures	8 — 25
Identifying Red Flags	8 — 25
Detection of Red Flags	8 — 27
Responding to Detected Red Flags	8 — 28
Updating the Program	8 — 29
Administration of the Program	8 — 29
Approval of the Board of Directors	8 — 30
Ongoing Involvement of the Board and Senior Management	8 — 30
Staff Training	8 — 31
Oversight of Service Provider Arrangements	8 — 32
Appendix A — Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation	8 — 32
Supplement A to Appendix A: Examples of Red Flags	8 — 32
Inactive Accounts	8 — 33
Duties of Card Issuers Regarding Changes of Address	8 — 33
“Cardholders” Protected by the Rule	8 — 33
Address Validation Requirements	8 — 34
Alternative Timing of Address Validation	8 — 35
Form of Notice	8 — 35
Duties of Users of Consumer Reports Regarding Address Discrepancies and Records	
Disposal	8 — 36
Applicability of the Rules	8 — 37
Notice of Address Discrepancy	8 — 37
Response to Notice of Address Discrepancy	8 — 37
Requirement to Furnish Consumer’s Address to a Consumer Reporting Agency	8 — 38
Timing of Furnishing Consumer’s Address to CRA	8 — 39
Affiliate Marketing Opt-Out	8 — 39
Affiliate Marketing Opt-Out and Exceptions	8 — 41
Eligibility Information	8 — 41
Solicitations Subject to the Rule	8 — 42
Examples of the Application of the Rule	8 — 44
Exceptions	8 — 46
Affiliates Who May Provide the Notice	8 — 51
Scope and Duration of Opt-Out	8 — 51

Providing Menu of Alternatives for Opt-Out	8 — 52
Special Rule for a Notice Following Termination of All Continuing Relationships.....	8 — 53
Duration of Opt-Out	8 — 53
Time of Opt-Out.....	8 — 53
Contents of Opt-Out Notice, Consolidated and Equivalent Notices.....	8 — 53
Contents of Opt-Out Notice.....	8 — 53
Opt-Outs Involving Joint Relationships	8 — 54
Alternative Contents in Cases of Broader Opt-Out Rights.....	8 — 54
Model Notices	8 — 55
Coordinated and Consolidated Notices	8 — 55
Equivalent Notices.....	8 — 55
Methods of Providing the Opt-Out Notice	8 — 55
Methods of Opting Out.....	8 — 56
Delivery of Opt-Out Notices.....	8 — 57
Expiration and Renewal of Opt-Out.....	8 — 57
Contents of Renewal Notice.....	8 — 58
Timing of the Renewal Notice.....	8 — 59
Obtaining or Using Medical Information To Determine Eligibility for Credit.....	8 — 59
Medical Information Subject to the Rule.....	8 — 60
Obtaining or Using Medical Information in Connection with a Determination of Eligibility for Credit	8 — 60
General Exceptions for Obtaining and Using Medical Information.....	8 — 61
Specific Exceptions for Obtaining and Using Medical Information	8 — 63
Limits on Redisclosure of Information.....	8 — 66
Sharing Medical Information with Affiliates.....	8 — 67
FACT Act Provisions Awaiting Final Rules Before They Become Effective.....	8 — 68
Coordination of Identity Theft Complaint Investigations (Section 153; FCRA Section 621(f)).....	8 — 68
Risk-Based Pricing Notice (Section 311; FCRA Section 615(h)).....	8 — 68
Procedures to Enhance the Accuracy and Integrity of Information Furnished (Section 312; FCRA Section 623(e)).....	8 — 68
Exhibit 8.1: Fair Credit Reporting Act Checklist.....	8 — 70
Exhibit 8.2: Federal Trade Commission Interpretation of Section 615(a).....	8 — 74
Exhibit 8.3: Appendix A to Part 681 — Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation	8 — 77
Exhibit 8.4: Supplement A to Appendix A.....	8 — 80
Exhibit 8.5: Appendix C Model Notices	8 — 84

Chapter 9 Related Policies and Procedures

Customer Identification Policy and Procedures.....	9 — 1
Sample Policy	9 — 1

Specific Procedures	9 — 2
Business Entities (Corporation, Partnership, LLC, or LLP).....	9 — 3
Business Entities (U.S. Persons).....	9 — 3
Business Entities (Non-U.S. Persons)	9 — 4
Verifying Account Opening Documentation.....	9 — 4
Authorized Signers on Accounts	9 — 4
Opening Accounts When the Customer Is Not Present.....	9 — 4
Information Security Policy and Procedures	9 — 5
Sample Policy	9 — 5
Assessment of Risk.....	9 — 6
Elements of Information Security Plan.....	9 — 7
Risk Assessment.....	9 — 7
Internal Routines and Controls	9 — 7
Management Supervision and Internal Controls	9 — 7
Service Providers.....	9 — 7
Expertise and Training	9 — 8
Testing	9 — 8
Contingency Planning and Business Continuity	9 — 8
Approval	9 — 8
Incident Response Policy and Procedures	9 — 8
Policy Statement.....	9 — 9
Management Reporting	9 — 9
Notify Regulatory and Law Enforcement Agencies.....	9 — 9
Contain and Control the Situation	9 — 10
Customer Notice and Assistance	9 — 10
Delay of Notice for Law Enforcement Investigation	9 — 10
Affected Customers	9 — 10
Content of Customer Notice.....	9 — 10
Information from Credit Reporting Agencies	9 — 11
Roles and Responsibilities.....	9 — 11
Chief Information Officer (CIO).....	9 — 11
Senior Information Systems Security Manager.....	9 — 11
Department Managers	9 — 11
Employees	9 — 12
Incident Response Teams	9 — 12
Online Services and Web Site Access Policy and Procedures.....	9 — 13
Introduction.....	9 — 13
Training	9 — 13
Legal and Regulatory Risk	9 — 13
Legal Framework.....	9 — 13
Regulatory Compliance	9 — 13
Children’s Online Privacy Protection Act	9 — 14
Operational Risk	9 — 15
Authorization.....	9 — 15
Access Controls.....	9 — 15
Authentication	9 — 15
Secure Data Storage	9 — 16

Operations.....	9 — 16
Policies and Procedures	9 — 17
Audit Procedures	9 — 17
Internet Products Offered by the Organization.....	9 — 17
Audits and Testing.....	9 — 17
Record Retention	9 — 17
Online Privacy and Security Policy and Disclosure	9 — 18
Vendor Management Policy and Procedures.....	9 — 18
Policy Statement.....	9 — 18
Risk Assessment.....	9 — 18
Operational Risk.....	9 — 18
Reputation Risk.....	9 — 19
Strategic Risk.....	9 — 19
Compliance (Legal) Risk.....	9 — 19
Interest Rate, Liquidity, and Price (Market) Risk.....	9 — 19
Quantity of Risk	9 — 19
Vendor Management	9 — 20
Foreign-Based Vendors	9 — 20
Selection of Vendors	9 — 20
Due Diligence on Vendors/Potential Vendors.....	9 — 21
Vendor Contracts.....	9 — 22
Specific Contract Provisions	9 — 22
Complaint Policy and Procedures.....	9 — 24
Policy Statement.....	9 — 24
Electronic Fund Transfer Act (12 CFR 205, 15 USC 1693).....	9 — 25
Types of EFTA Errors	9 — 25
Timely Notice.....	9 — 25
Time Limits and Extent of Investigation.....	9 — 26
Notifying the Customer	9 — 27
Complaint File.....	9 — 27
Regulation CC — Substitute Check Inquiries/Complaints.....	9 — 27
Circumstances Giving Rise to a Claim.....	9 — 28
Timing of Claim	9 — 28
Content of Claim	9 — 28
Action on Claims.....	9 — 29
Recredit Pending Investigation.....	9 — 29
Availability of Recredit	9 — 29
Reversal of Recredit	9 — 30
Notices Relating to Customer Expedited Recredit Claims.....	9 — 30
Mortgage Servicing Errors under the Real Estate Settlement Procedures Act (24 CFR 3500, 12 USC 2601)	9 — 31
Qualified Written Request.....	9 — 31
Responses to Inquiries.....	9 — 31
Action Regarding Inquiries	9 — 31
Periodic Billing Errors (Regulation Z) (12 CFR 226, 15 USC 1601)	9 — 32
Types of Errors.....	9 — 32
Acknowledging Notice of the Error	9 — 33

Timing of Investigation and Resolution of Errors	9 — 33
Corrective Action	9 — 33
Resolution of Error Notices — Credit Cards	9 — 34
Relation to Electronic Fund Transfer Act and Regulation E	9 — 34
Fair Credit Reporting Act (FCRA)	9 — 34
Consumer Privacy	9 — 34
Exhibit 9.1: FTC Model Letter for the Compromise of Social Security Numbers	9 — 36
Exhibit 9.2: Customer Identification Worksheet	9 — 37

Chapter 10

Corporate Originators of ACH Transactions

The Corporate Originator	10 — 1
Originating Depository Financial Institution	10 — 1
ACH Operator	10 — 2
Receiving Depository Financial Institution	10 — 2
Receiver	10 — 2
Third-Party Service Provider	10 — 2
Third-Party Service Provider as Third-Party Sender	10 — 2
ACH Origination Flow Charts	10 — 3
ACH Credit Origination	10 — 3
ACH Debit Origination	10 — 4
ACH Origination Using a Third-Party Service Provider	10 — 5
Data Security	10 — 5
Use of ACH Transactions by the Originator	10 — 6
Prearranged Payment and Deposit Entry (PPD)	10 — 6
Cash Concentration and Disbursement (CCD)	10 — 6
Corporate Trade Exchange (CTX)	10 — 7
Represented Check Entry (RCK)	10 — 7
Accounts Receivable Entry (ARC)	10 — 7
Point-of-Purchase Entry (POP)	10 — 7
Back-Office Conversion Entry (BOC)	10 — 7
Internet-Initiated Entry (WEB)	10 — 8
Telephone-Initiated Entry (TEL)	10 — 8
Use of Pre-Notification Transactions	10 — 8
Applying Transaction Codes	10 — 9
Obligations of Originators	10 — 9
Authorizations and Agreements	10 — 10
Consumer Debit Entries	10 — 11
Returned Check Entries (RCK)	10 — 11
Accounts Receivable Entries (ARC)	10 — 12
Point-of-Purchase Entries (POP)	10 — 14
Back-Office Conversion Entries (BOC)	10 — 16

Internet-Initiated Entries (WEB)	10 — 18
Telephone-Initiated Entries (TEL).....	10 — 18
PIN Requirements.....	10 — 19
Origination of Files by Originators.....	10 — 19
Exposure Limits.....	10 — 19
Creating ACH Data.....	10 — 19
Dating of Originated Entries.....	10 — 20
Settlement of Originated Entries.....	10 — 20
Submission of Originated Files by the Originator to the ODFI.....	10 — 20
Creating and Submitting Reversing Files	10 — 21
Creating and Submitting Reversing Entries.....	10 — 21
The Originator’s Role in OFAC Compliance	10 — 22
What to Do When ACH Transactions Are Returned.....	10 — 22
What to Do When a Notification of Change Is Received	10 — 23
Originator Audit Obligations	10 — 24
Compliance Tips for Originators	10 — 25

Chapter 11

Credit Card Fraud

Introduction.....	11 — 1
The Basic Credit Card Transaction.....	11 — 2
Merchant Credit and Charge Backs	11 — 3
Types of Credit Card Fraud	11 — 3
The Law Concerning Credit Card Fraud.....	11 — 5
Notice.....	11 — 8
Resolution Procedures and Burden of Proof.....	11 — 8
Liability for Cards Used in Business	11 — 9
Unauthorized Use	11 — 10
Relevant Court Cases	11 — 12
Apparent Authority and Cardholder Responsibility	11 — 13
Relevant Court Cases	11 — 13
Benefit to the Cardholder.....	11 — 15
Termination of Authority.....	11 — 16
Relevant Court Cases	11 — 16
Rights Against Third Parties.....	11 — 17
Relevant Court Cases	11 — 18
Option to Forgo Cardholder Liability.....	11 — 19
Fraudulent Use by Merchants and Merchants’ Employees	11 — 20
Relevant Court Cases	11 — 20
Statute of Limitations	11 — 23
Actions Against Merchants for Failure to Protect Cardholder Information.....	11 — 24
Relevant Court Cases.....	11 — 25

Detection and Deterrence of Credit Card Fraud	11 — 28a
Care in Issuance of Cards	11 — 28a
Monitoring for Suspicious Transactions.....	11 — 28b
Merchant Involvement.....	11 — 30
Guidance for Cardholders.....	11 — 31
Guidance for Merchants	11 — 32
Long-Distance Transactions.....	11 — 33
Technological Deterrents.....	11 — 34
Holograms and Photographs.....	11 — 34
Smart Cards	11 — 34
Detention of Customers	11 — 34
Credit Cards and Money Laundering.....	11 — 35
Screening	11 — 36
Merchant Involvement.....	11 — 37
Exhibit 11.1: Checklists to Protect Against Credit Card Fraud.....	11 — 39

Chapter 12

Fraud Involving ATM and Debit Cards

The Basic Transaction.....	12 — 1
Debit Card Transactions	12 — 2
Offline Transactions	12 — 3
Visa/MasterCard Antitrust Litigation	12 — 4
ATM Card Transactions	12 — 5
Check Conversion.....	12 — 5
Payroll Card Transactions.....	12 — 6
Types of Consumer Electronic Fund Transfer Fraud.....	12 — 6
Other Fraudulent Schemes.....	12 — 9
The Law Governing Consumer Electronic Fund Fraud.....	12 — 9
Basic Liabilities for Unauthorized Transfers.....	12 — 9
Force or Fraud.....	12 — 10
The Irrelevance of Consumer Negligence	12 — 11
Actual Authority	12 — 12
Ratification of Use of Access Device	12 — 13
Obtaining Cards Without Authorization.....	12 — 13
Transfers That Constitute Errors by the Financial Institution	12 — 15
Liability for Unauthorized Electronic Fund Transfers.....	12 — 15
Related Unauthorized Transfers	12 — 16
Consumer Responsibilities and Additional Tiers of Liability	12 — 17
\$50 Liability	12 — 17
\$500 Liability	12 — 17
Unlimited Liability	12 — 18
Receipt of Statement as “Learning”	12 — 19

Burden of Proof and Financial Institution Procedures for Unauthorized Transfers	12 — 20
Notice.....	12 — 21
Regulations with Respect to Payroll Cards.....	12 — 22
Detection and Deterrence of Electronic Transfer Fraud	12 — 23
Care in Issuance of Access Devices	12 — 23
Care in Monitoring Use of ATMs.....	12 — 24
Guidance for Customers	12 — 26
Guidance for Merchants	12 — 28
Exhibit 12.1: Consumer Liability to Financial Institution for Fraudulent Use of Consumer’s Account.....	12 — 30
Exhibit 12.2: Checklists to Protect Against ATM and Debit Card Fraud	12 — 31

Appendixes

Appendix A FTC’s ID Theft Affidavit

Appendix B FTC’s ID Theft: What’s It All About?

Appendix C Red Flag Proposed Rule

Appendix D FTC’s Deter, Detect, Defend

Appendix E FTC’s Credit, ATM, and Debit Cards: What to Do If They’re Lost or Stolen

Appendix F Sample E-Sign Customer Agreement

Appendix G Sample Online Access Agreement

Identity Theft Red Flag Toolkit

Step-By-Step Guide to Developing Your Identity Theft Prevention Program	Toolkit — 1
What Accounts Fall Under the ID Theft “Red Flag” Rules?.....	Toolkit — 1
Step 1 — Determine the Red Flags That Affect Each Department in the Organization	Toolkit — 2
Step 2 — Assess the Level of Risk to Your Organization for Each Red Flag.....	Toolkit — 3
Step 3 — Examine Existing Policies and Procedures to Ensure They Address Red Flags Risks	Toolkit — 4
Step 4 — Determine Your Response to Each of the Red Flags When They Are Encountered by Your Employees	Toolkit — 5
Step 5 — Implement and Monitor Your ID Theft Red Flag Program.....	Toolkit — 6
Completing the Red Flag Risk Assessment and Mitigation Worksheet	Toolkit — 7
Sample Red Flag Risk Assessment and Mitigation Worksheet.....	Toolkit — 8
Red Flag Risk Assessment and Mitigation Worksheet.....	Toolkit — 11
Sample Identity Theft Prevention Policy and Procedures.....	Toolkit — 20
Sample Identity Theft Prevention Policy.....	Toolkit — 20
Procedures Relating to Identity Theft Prevention.....	Toolkit — 23
FTC Model Letter for the Compromise of Social Security Numbers.....	Toolkit — 29
Sample Identity Theft Training Outline.....	Toolkit — 30
Related Policies and Procedures	Toolkit — 32
Customer Identification Policy and Procedures.....	Toolkit — 33
Customer Identification Worksheet.....	Toolkit — 38
Information Security Policy and Procedures	Toolkit — 39
Incident Response Policy and Procedures	Toolkit — 43
Online Services and Web Site Access Policy and Procedures	Toolkit — 48
Online Privacy and Security Policy and Disclosure	Toolkit — 54
Vendor Management Policy and Procedures.....	Toolkit — 55