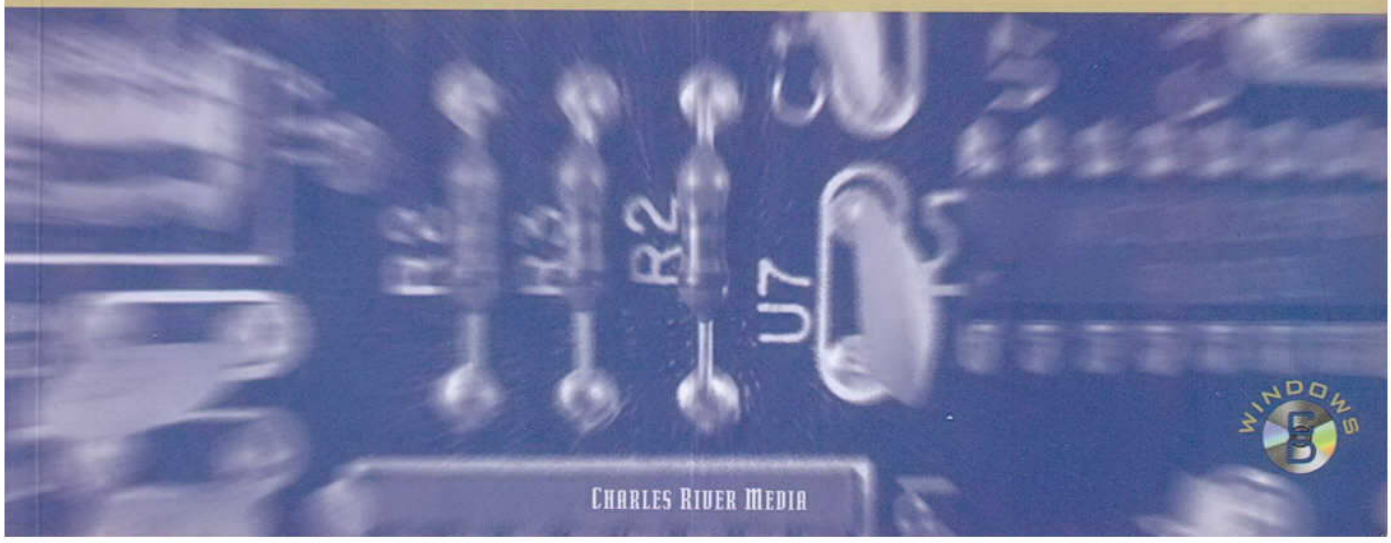
THE INTERNET MERCHANT MASTER SERIES

SELLING ONLINE WITH...

FIRST VIRTUAL

PETE LOSHIN

FOREWORD BY NATHANIEL BORENSTEIN



CHARLES RIVER MEDIA

Shopify Exhibit 1013

FIRST VIRTUAL

LOSHIN

SELLING ONLINE WITH . . .
FIRST VIRTUAL HOLDINGS, INC.

THE INTERNET MERCHANT MASTER SERIES

LIMITED WARRANTY AND DISCLAIMER OF LIABILITY

CHARLES RIVER MEDIA, INC. ("CRM") AND/OR ANYONE WHO HAS BEEN INVOLVED IN THE WRITING, CREATION OR PRODUCTION OF THE ACCOMPANYING CODE ("THE SOFTWARE") OR THE THIRD PARTY PRODUCTS CONTAINED ON THE CD, CANNOT AND DO NOT WARRANT THE PERFORMANCE OR RESULTS THAT MAY BE OBTAINED BY USING THE SOFTWARE. THE AUTHOR AND PUBLISHER HAVE USED THEIR BEST EFFORTS TO ENSURE THE ACCURACY AND FUNCTIONALITY OF THE TEXTUAL MATERIAL AND PROGRAMS CONTAINED HEREIN; WE HOWEVER, MAKE NO WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, REGARDING THE PERFORMANCE OF THESE PROGRAMS. THE SOFTWARE IS SOLD "AS IS " WITHOUT WARRANTY (EXCEPT FOR DEFECTIVE MATERIALS USED IN MANUFACTURING THE DISK OR DUE TO FAULTY WORKMANSHIP); THE SOLE REMEDY IN THE EVENT OF A DEFECT IS EXPRESSLY LIMITED TO REPLACEMENT OF THE CD, AND ONLY AT THE DISCRETION OF CRM.

THE AUTHOR, THE PUBLISHER, DEVELOPERS OF THIRD PARTY SOFTWARE, AND ANYONE INVOLVED IN THE PRODUCTION AND MANUFACTURING OF THIS WORK SHALL NOT BE LIABLE FOR DAMAGES OF ANY KIND ARISING OUT OF THE USE OF(OR THE INABILITY TO USE) THE PROGRAMS, SOURCE CODE, OR TEXTUAL MATERIAL CONTAINED IN THIS PUBLICATION. THIS INCLUDES , BUT IS NOT LIMITED TO, LOSS OF REVENUE OR PROFIT, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THE PRODUCT.

THE CD WHICH ACCOMPANIES THE BOOK MAY BE USED ON A SINGLE PC ONLY. THE LICENSE DOES NOT PERMIT THE USE ON A NETWORK (OF ANY KIND). YOU FURTHER AGREE THAT THIS LICENSE GRANTS PERMISSION TO USE THE PRODUCTS CONTAINED HEREIN, BUT DOES NOT GIVE YOU RIGHT OF OWNERSHIP TO ANY OF THE CONTENT OR PRODUCT CONTAINED ON THIS CD. USE OF THIRD PARTY SOFTWARE CONTAINED ON THIS CD IS LIMITED TO AND SUBJECT TO LICENSING TERMS FOR THE RESPECTIVE PRODUCTS.

THE USE OF "IMPLIED WARRANTY" AND CERTAIN "EXCLUSIONS" VARY FROM STATE TO STATE, AND MAY NOT APPLY TO THE PURCHASER OF THIS PRODUCT.

Requests for replacement of a defective CD must be accompanied by the original disk, your mailing address, telephone number, date of purchase and purchase price. Please state the nature of the problem, and send the information to CHARLES RIVER MEDIA, INC., P.O. Box 417, 403 VFW Drive, Rockland, Massachusetts 02370. CRM's sole obligation to the purchaser is to replace the disk, based on defective materials or faulty workmanship, but not on the operation or functionality of the product.

SELLING ONLINE WITH . . .
FIRST VIRTUAL HOLDINGS, INC.

THE INTERNET MERCHANT MASTER SERIES

CHARLES RIVER MEDIA, INC.
ROCKLAND, MASSACHUSETTS

Copyright © 1996 by CHARLES RIVER MEDIA, INC.
All rights reserved.

No part of this publication may be reproduced in any way, stored in a retrieval system of any type, or transmitted by any means or media, electronic or mechanical, including, but not limited to, photocopy, recording, or scanning, without *prior permission in writing* from the publisher.

Publisher: David F. Pallai
Interior Design/Comp: Reuben Kantor
Cover: Gary Ragaglia
Printer: InterCity Press, Rockland, MA.

CHARLES RIVER MEDIA, INC.
P.O. Box 417
403 VFW Drive
Rockland, Massachusetts 02370
617-871-4184
617-871-4376 (FAX)
chrivmedia@aol.com

This book is printed on acid-free paper.

Pete Loshin. *Selling Online With . . . First Virtual Holdings, Inc.*
ISBN: 1-886801-41-X

All brand names and product names mentioned in this book are trademarks or service marks of their respective companies. Any omission or misuse (of any kind) of service marks or trademarks should not be regarded as intent to infringe on the property of others. The publisher recognizes and respects all marks used by companies, manufacturers, and developers as a means to distinguish their products.

Printed in the United States of America
96 97 98 99 00 6 5 4 3 2 First Edition

CHARLES RIVER MEDIA titles are available for site license or bulk purchase by institutions, user groups, corporations, etc. For additional information, please contact the Special Sales Department at 617-871-4184.

CONTENTS

FOREWORD xv
PREFACE xix

Part I Introducing First Virtual and Internet Commerce 1

1 INTRODUCTION TO INTERNET COMMERCE 3

BUYING AND SELLING ON THE INTERNET 6
What's Different? 7
What's the Same? 7

THE INTERNET ENVIRONMENT 9
The Internet Advantage 9
World Wide Web, Killer App of the Internet 11

THE WORLD WIDE WEB 13
World Wide Web Standards 14
Web Browsers and Web Servers 16
Selling on the World Wide Web 18
Other Internet Sales Venues 19

INTERNET COMMERCE ISSUES 22
Informal Procedures Aren't Enough 22
Securing Financial Information 23
Authenticating Transaction Data 25
Paying for the Privilege 26

THE FIRST VIRTUAL WAY 27
A Holistic Approach to Security 28
Paying for the Service 30

FIRST VIRTUAL OVERVIEW 30
Can't People Steal My Information Products? 33
Can't VirtualPINs Be Compromised? 34
It Seems Awfully Complicated 35

2 SECURITY ISSUES, SECURITY TOOLS 37

WHY THE INTERNET IS UNSECURE 38
It's the Protocols 40
Where the Risks Are 42
What the Risks Are 42
Internet Security Holes 43
A Bigger Risk 45
What It All Means 46

NEW TOOLS FOR CRYPTOGRAPHY 46
Cryptography 47
Cryptographic Objectives 48
Codes and Ciphers 50
Breaking Encryption Schemes 51
Securing Algorithms 53
Distributing Keys and Keeping Them Secret 54
The Public Key Solution 55
Public Key Implications 56
Key Distribution and Certification 58
Trusted Key Distribution and Verification 59

CRYPTOGRAPHIC APPLICATIONS 60
Encryption 60

Digital Signature 61
Nonrepudiation and Message Integrity 62

3 SECURING INTERNET COMMERCE 65

THE INTERNET COMMERCE STORY, SO FAR 66
Five Internet Commerce Techniques 66
Security through Obscurity 66
Consumer/Merchant Channel Encryption 67
Digital Envelope Encryption 68
Digital Currencies 69
Offline Handling of Transaction Data 69
Representative Internet Commerce Players 70
Other Internet Commerce Actors 72

TRANSACTION SECURITY THROUGH OBSCURITY 73
The "No Security" Choice 73
Choosing No Security 74
Incomplete Security Solutions 75
Marks of Unsecure Solutions 76

THE ENCRYPTED CHANNEL APPROACH 77
How an Encrypted Channel Works 78
Advantages for Merchants 81
Advantages for Consumers 82
Weaknesses and Disadvantages 82

THE DIGITAL ENVELOPE APPROACH 83
How Digital Envelopes Work 85
Advantages for Merchants 85
Advantages for Consumers 86
Weaknesses and Disadvantages 86

DIGITAL CURRENCIES 87
How Digital Cash Works 88
Advantages for Merchants 89
Advantages for Consumers 89
Weaknesses and Disadvantages 89

EXTERNAL CHANNEL APPROACH 90
How the External Channel Approach Works 91
Advantages for Merchants 92
Advantages for Consumers 93
Weaknesses and Disadvantages 94

Part II First Virtual: The Company, Its Products and Services 97

4 THE FIRST VIRTUAL APPROACH TO INTERNET COMMERCE 99

THE BIRTH OF FIRST VIRTUAL 100

HOW FIRST VIRTUAL WORKS 101
Creating an Account 102
Account Requirements 103
Submitting the Application 103
Terms and Conditions 103
Making a Purchase 104
Making a Sale 105

FIRST VIRTUAL PROTOCOLS 105
The Green Commerce Model 107
Cardholders and Cardholder Accounts 109
Green Commerce Transactions 110
Funds Transfer 111
Cardnumber Inquiries 114
Transfer Inquiries 114
Chargebacks 115
Green Commerce Server Capabilities 115
Cardholder Account Application 115
Account Maintenance 116
Account History Requests 116
Application/Green-Commerce MIME Content-Type 117
Simple MIME Exchange Protocol (SMXP) 118
Simple Green Commerce Protocol (SGCP) 118

SELLING HARD GOODS WITH FIRST VIRTUAL 119
Added Security Measures 119
Selling Hard Goods vs. Information Products 119
Digital Signature Key Management 120
Validating Digital Signatures 121

5 FIRST VIRTUAL PRODUCTS AND SERVICES 123

THE FIRST VIRTUAL ORGANIZATION 124
A Virtual Corporation 124
Using Automation 125
First Virtual Products and Services 126

TERMS AND CONDITIONS 127
Getting the Terms and Conditions Documents 128
Buyer's Terms and Conditions 129
Seller's Terms and Conditions 129
InfoHaus Seller's Terms and Conditions 130

BUYERS' SERVICES 130
Account Requirements 130
Account Creation 131
Buying Privileges 132
Customer Support Services 132

SELLERS' SERVICES 133
Account Creation and Requirements 134
Selling Privileges 135
Customer Support Services 135

WHY THE 91-DAY HOLDBACK PERIOD? 136

THE INFOHAUS SERVICE 137
Storefront Creation and Requirements 138
Storefront Management 138
Rights and Responsibilities 139
Customer Support Services 139

REACHING FIRST VIRTUAL 139
Contacting First Virtual via the World Wide Web 140

E-mail Addresses 141
Automatic E-mail Responder 141
Special Addresses for Sellers 141
Special InfoHaus Addresses 142
Other Internet Resource Addresses 142
ftp 143
Telnet 143
First Virtual Users Mailing List 144
How To Subscribe To the FV-Users List 144
Unsubscribing From the FV-Users List 145
Participating In the FV-Users List 145
Reaching a Human 146

Part III Buying and Selling with First Virtual 149

6 OPENING YOUR FIRST VIRTUAL ACCOUNT 151

THE FIRST VIRTUAL ACCOUNT PROCESS 152
Methods for Initial Contact 152
Providing Some Information Online 153
Different Applications, Identical Followup 156
Providing Some Information Offline 157
Buying and/or Selling 158
Waiving the Holding Period for Merchants 158

SIGNING UP BY WORLD WIDE WEB 159
Connecting to the First Virtual Web Site 159
Filling in the Application Form 160
What Follows 164

SIGNING UP BY TELNET 164
Connecting to the First Virtual Telnet Server 164
Answering Application Questions 167
Reviewing and Submitting the Application 170
What Follows 173

SIGNING UP BY E-MAIL 174
Getting the E-mail Application 174
Filling in the Application Form 174
Submitting the Application Form 180
What Follows 181

ACCOUNT VERIFICATION AND FOLLOWUP 181
E-mail Confirmation of Application 182
Responding by Telephone for Buyers 186
Responding by Mail for Sellers 187
Finishing the Process 188

GETTING EXPRESS MERCHANT STATUS 188

ACCOUNT MAINTENANCE 190
Tracking Your Account Status 190
Making Changes 191

7 BUYING WITH FIRST VIRTUAL 193

THE TRANSACTION PROCESS 194

A SAMPLE PURCHASE 195

TRANSACTION COMPLETION 199

PRODUCT DELIVERY 206

BUYING HARD GOODS 207

BUYING BY E-MAIL AND FTP 208
Buying by ftp 208
Buying by E-mail 209

8 SELLING ON THE INFOHAUS 213

INTRODUCTION TO THE INFOHAUS 214
Why the InfoHaus? 214
How It Works 216
It's Not Just for the World Wide Web 216
What It Costs 217

SETTING UP YOUR STOREFRONT 218
Opening Your InfoHaus Storefront 218
Setting up a Storefront Using Telnet 219
Setting up a Storefront Using E-mail 225
Stocking Your Store 227
Preparing Your Information Products 228
Uploading Products by ftp 232
Uploading Products by E-mail 233
Checking in Products by Telnet 233
Installing Products by E-mail 235

ADDING HTML TO YOUR INFOHAUS STOREFRONT 238

INFOHAUS PERIODICALS 240
Subscribing to a Periodical 241
Creating Periodicals 241
Adding Issues to a Periodical 242

9 SELLING FROM YOUR WEB SERVER 243

WHAT YOU NEED TO GO ONLINE 245
Hardware, Software, Services 246
Hardware 246
Software 247
Services 247
If You Outsource Your Web Site... 248

FIRST VIRTUAL RESOURCES 249
Using First Virtual Programs and Templates 250
Using the First Virtual Web Site 251
Scripts, Templates, and More 253

THE SELLING PROCESS 254
Initiating a Transaction 254
Using E-mail 255
Using Telnet 256
Using the Simple Green Commerce Protocol 257
Making Sales off the Internet 257

Verifying a Buyer's VirtualPIN 258
Finger 258
Telnet 259
E-mail 260
Using the FV-API 260

INFOHAUS HTML FORMS 261
Emailform 261
Emailpayform 263

CGI SELLING TOOLS 265
Member 265
Installing and Running Member 266
Websale 268
Using Tcl 269
Installing Websale 269

THE FIRST VIRTUAL API 269
Getting and Installing the First Virtual API 271
FV-API Operations 271
Autosell URLs 271
Manusell URLs 272
Formsell URLs 272

10 TIPS, TRICKS, AND POINTERS 273

TIPS FOR EVERYONE 274

TIPS FOR INFOHAUS MERCHANTS 275

GETTING YOUR STORE LISTED 279

COMMERCIAL OPTIONS FOR MERCHANTS 280

MAKING TEST SALES THROUGH FIRST VIRTUAL 281
InfoHaus "QuickBuy" Numbers 282

LEARNING MORE ABOUT HTML AND CGI 284
Getting Help from the World Wide Web 284
Books about HTML and CGI 285

APPENDIX A INTERNET COMMERCE GLOSSARY 287

APPENDIX B ELECTRONIC COMMERCE ONLINE RESOURCES 305

WORLD WIDE WEB RESOURCES 306
Electronic Commerce Companies 306
Financial Institutions 311
International Internet Commerce Sites 314
General Catalog and News Services 316
Online Commerce Organizations 318
Online Marketing, Buying, and Selling 320

MAILING LISTS 322

COMMERCENET 326
CommerceNet Charter 326
CommerceNet Participation 327
What CommerceNet Offers 327

APPENDIX C FIRST VIRTUAL TERMS AND CONDITIONS DOCUMENTS 329

BUYER'S TERMS AND CONDITIONS 330

SELLER'S TERMS AND CONDITIONS 341

INFOHAUS TERMS AND CONDITIONS 360

APPENDIX D GUIDE TO THE CD-ROM 371

INSTALLING THE CD-ROM 371
Accessing the CD-ROM Index 372

SUPPORT FOR SOFTWARE ON THE CD-ROM 371

CD-ROM CONTENTS 371
Structure of the CD-ROM 371
First Virtual Specification Documents 371
InfoHaus Templates 371
HTML Templates and CGI Scripts 371
The First Virtual API 371
First Virtual Enabling Your ftp Server 371

ELECTRONIC COMMERCE LINKS 371

INDEX 377

FOREWORD

We're living in very strange and interesting times. Nearly twenty-five years ago, as a high school student, I met my first computer. It was an IBM 360, to which I typed via a teletype connected cross-town at 110 baud. I thought it was the second-coolest thing I had ever seen. Like many others of my generation, I quickly realized that this was an encounter that would change my life, but I didn't have a clue what was coming. If anyone had tried to convince me, as a 15-year-old would-be hippie in Columbus, Ohio, that by 1996 I would be something like an international banker, I would have laughed out loud. Ten years later, as a computer science graduate student working on ARPAnet email technology, I would have been equally amused.

In hindsight, it's clear that computers, communication, and banking have been on a collision course for a long time. Now, the collision has happened. People who know how to use the Internet safely and effectively are suddenly considered vital to the future of human commerce. Established players in the game of international finance are on the edge of panic, so uncertain are they as to how the new technologies will

restructure their world. Their reactions vary in every conceivable way, sharing only one common theme: a desperate hunger to understand this strange new thing called the Internet.

First Virtual came from another planet, more or less. The FV founders came from inside the Internet, understood it deeply, and were totally comfortable with it. Of course, our ignorance and naivete on the financial side of things were pretty impressive, too. If the established players had understood the Internet, they would have eaten us for lunch. As it was, we all found ourselves in a frantic race to learn more. Our biggest advantage was probably that it was easier to find people who could explain the financial world to us than it was for banks to find people who could explain the Internet to them.

It will be a long time before the dust settles on Internet commerce mechanisms. It may yet happen that all the players currently on the scene will be swept away by forces that are, at this writing, just lurking in the wings. But so far, a few of First Virtual's key features seem to have struck a receptive chord with the Internet community. They seem likely to be around for a long time in one form or another.

One such idea is open, universal access to commerce. First Virtual has without a doubt opened up more entrepreneurial horizons than any other payment system in history. With ten dollars and a bank account, you can start selling things to people all over the planet. There's no credit-scoring or approval process that restricts merchant status to large, established corporations. Anyone can be a seller. This aspect of the FV system has met with nearly universal approval, and seems to be in tune with one of the most important aspects of the Internet — its role in opening, leveling, and universalizing human communication.

Another aspect of First Virtual's system design that seems to have been validated by experience is our reluctance to rely on special consumer-level mechanisms to facilitate commerce. All that you really need in order to be a buyer with First Virtual is access to Internet e-mail. This means that neither First Virtual nor the merchants who use our system have to be in the business of persuading customers to acquire, learn, and use any new tools. In essence, the entire Internet is our installed software base, and FV customers don't have to sacrifice any freedom of choice regarding the software that they use for Internet access.

Perhaps the most important aspect of FV's system design, however, is that we have demonstrated that it is possible to build a secure commerce mechanism based entirely on protocols that are truly open. Programmers who want to write applications that use First Virtual's payment system can download complete specifications, sample code, and even some fully functioning software, all for free from our site. There are no woolly-headed claims for security through obscurity, no requirements for programmers to license patented algorithms, and no dependencies on proprietary computing platforms. Contrary to many people's expectations, FV demonstrates that it is possible to make Internet commerce as open as the Internet itself. Unfortunately, not everyone wants to keep it that way.

We all know that there's a gold rush going on right now on the Internet, with people and companies vying for position in the much-discussed but little-understood infrastructure for the future of human communication and commerce. What's less recognized is that implicit in this gold rush is a struggle over the very organization of society in the years to come. Computing technology serves fundamentally to amplify human abilities. Thus, it inherently tends to push organizations towards one of two extremes, centralization or democratization, depending on how it is applied and in what

organizational structures. Nowhere is this more important than in the area of payment systems.

Internet payment systems can be designed to enable the masses to be entrepreneurs, or they can be designed to further concentrate power in the hands of the largest companies and wealthiest individuals. If you look carefully at the technical design of a payment system, you will always find assumptions about the social structure of commerce, and you will often find a political agenda as well.

First Virtual makes no bones about its political agenda: We want to make sure that the little guy has a chance, along with the big guy, to set up businesses on the Internet. Ultimately, we want a musician in rural Uganda to be able to sell his music directly to consumers in the United States, Tonga, or anywhere else. We don't believe our payment system is the only way to enable such commerce, but we do believe that this goal is conspicuously absent from many other proposed payment systems.

Unlike this preface, the book you're holding in your hands is not a political or ideological statement. It's a very practical "how-to" book, and by the time you're done reading it, you should be able to set up a whole new business in cyberspace starting with nothing but $10, an Internet connection, a good idea, and a willingness to work. I hope that's why you're reading these words. I don't really mind if you don't share my political agenda. If you're an industrious would-be entrepreneur with a dream of your own, you *are* my political agenda. I hope you do very well.

— Nathaniel Borenstein
Chief Scientist, First Virtual Holdings

PREFACE

Business people who heard about the Internet in 1994 tended to ask, "What is it good for?" It was a valid question back then — most people had never even heard of the Internet. In 1996, there are still many people in all walks of life who aren't sure how they can make the Internet pay off. This book will show you how to use the First Virtual Internet payment system to sell (and buy) goods and services over the Internet — safely, easily, and inexpensively. What's more, this book will provide you with a solid foundation for understanding all types of Internet commerce, as well as how the First Virtual approach fits into the global Internet.

You'll find here everything you need to know to confidently get started selling on the Internet using the First Virtual system. Part One will give you a basic understanding of the issues and tools now in general use by Internet merchants of all stripes. Chapter 1, "Introduction to Internet Commerce," explains what it means to buy and sell using the Internet to carry your transaction information, as well as what problems you can expect to encounter in doing business on the Internet. Chapter 2, "Security Issues, Security Tools," explains how

advances in cryptography have been providing the tools needed to solve Internet commerce security issues. Chapter 3, "Securing Internet Commerce," explains how companies have been putting together the various cryptographic tools to create Internet commerce solutions. Here is an overview of how Internet commerce is developing, your choices as an Internet merchant, and the advantages and disadvantages of using these different solutions.

Part Two provides an overview of the First Virtual organization and their products and services. Chapter 4, "The First Virtual Approach to Internet Commerce," explains how the company came to be, the logical and technological underpinnings of the First Virtual system, and how that system works. Chapter 5, "First Virtual Products and Services," provides a summary of First Virtual contact, product, and information resources.

In Part Three, the nuts and bolts of buying and selling with First Virtual are laid out in full. Chapter 6, "Opening Your First Virtual Account," explains in detail how to open your account for buying and selling, including applying for Express Merchant status. Chapter 7, "Buying With First Virtual," examines the process of making a purchase with First Virtual. Chapter 8, "Selling on the InfoHaus," explains how you can set up your own Internet storefront using First Virtual's InfoHaus hosting service; Chapter 9, "Selling from Your Web Server," explains how to use scripts and other tools for selling your own information products or hard goods on your own Internet or World Wide Web server. Finally, Chapter 10, "Tips, Tricks and Pointers," brings you tips and pointers from First Virtual staff and merchants to help make your selling experience more profitable.

Appendices include "Internet Commerce Glossary" (Appendix A), "Electronic Commerce Online Resources (Appendix B), "First Virtual Terms and Conditions Documents" (Appendix C) and "Guide to the CD-ROM" (Appendix D). Included on the CD-ROM are First Virtual protocol specifications as well as scripts and other code for implementing your own First Virtual Internet storefront.

This book was possible only with the cooperation, support, and help of many people. In particular, thanks are due the people at First Virtual, who are making Internet commerce a reality for anyone connected to the Internet, not just big companies. Special thanks also go to Nathaniel Borenstein of First Virtual for his help in getting this book finished on time, as well as to publisher David Pallai and production specialist Reuben Kantor.

Finally, very special thanks to Lisa Wolfe, Ph.D., for her very special support, and to our genetic repository for his help in focusing my attention.

PART ONE

INTRODUCING FIRST VIRTUAL AND INTERNET COMMERCE

CHAPTER ONE

INTRODUCTION TO INTERNET COMMERCE

Summary This chapter explains what is happening in terms of doing business on the Internet. It describes the basic ideas, issues, and problems of buying and selling on the Internet, and it introduces (briefly) the First Virtual approach and services.

Contents

BUYING AND SELLING ON THE INTERNET 6
What's Different? 7
What's the Same? 7

THE INTERNET ENVIRONMENT 9
The Internet Advantage 9
World Wide Web, Killer App of the Internet 11

THE WORLD WIDE WEB 13
World Wide Web Standards 14
Web Browsers and Web Servers 16
Selling on the World Wide Web 18
Other Internet Sales Venues 19

INTERNET COMMERCE ISSUES 22
Informal Procedures Aren't Enough 22
Securing Financial Information 23
Authenticating Transaction Data 25
Paying for the Privilege 26

THE FIRST VIRTUAL WAY 27
A Holistic Approach to Security 28
Paying for the Service 30

FIRST VIRTUAL OVERVIEW 30
Can't People Steal My Information Products? 33
Can't VirtualPINs Be Compromised? 34
It Seems Awfully Complicated 35

There can be no question: as we approach the end of the century, commercial life as we know it is changing rapidly. One of the most prominent vehicles of that change is the expansion of the global Internet. In 1990, after twenty years of research and development, only a tiny fraction even of well-informed technologists knew what the Internet was. Five years later, Internet e-mail addresses are almost as common on business cards as fax numbers, major print and media companies have begun publishing and broadcasting online through the World Wide Web, and consumer products companies advertise their home pages in broadcast television commercials. More important, the business world is looking to the Internet to provide a new sales and delivery channel capable of reducing costs and improving the bottom line. The Internet flattens the playing field for those providing "soft goods" (products capable of being delivered electronically), and can lower the costs of entry to national and global markets for sellers of "hard goods" (products with a physical presence) as well.

There are a lot of companies that want to be your Internet commerce provider, each with its own philosophy and approach to enabling the buying and selling of goods and services over open networks. The different offerings reflect those different approaches, and each has its advantages and disadvantages. No single approach to digital commerce has yet been chosen by the market to the exclusion of any others, nor is any likely to be. After all, there are easily half a dozen different payment methods available to consumers in the real world, so expect room for coexistence in the digital world as well.

In October of 1994, before most other companies providing Internet commerce services even had a product to show, First Virtual Holdings, Incorporated, unveiled a unique Internet

payment system and began processing commercial transactions. This chapter very briefly introduces First Virtual, but more details on its organization, products, and services are provided later in the book. This chapter also introduces the Internet, the World Wide Web, and the concepts of digital commerce.

First Virtual is but one of many companies offering services variously referred to as supporting "electronic commerce," "digital commerce," or "Internet commerce." To understand what First Virtual brings to the table, it is important to understand what its competitors bring, and how those offerings relate to the issues and challenges of doing business on the Internet.

During its first year of operation, some critics dismissed First Virtual as simply a system providing secured aliases for credit cards to be used safely on the Internet. By itself, this is hardly a small feat — but the First Virtual protocols were designed to support much more than this type of commercial transaction. The protocols were enhanced at the start of 1996, making possible the secure purchase and sale of physical goods, along with the addition of special services aimed at larger merchants. This makes First Virtual's service far more adaptable and useful than was at first imagined.

The first iteration of the First Virtual payment system allowed consumers only one way to pay for goods or services — by credit card. It allowed merchants only one way to receive the proceeds of those sales — by direct deposit to a checking account. Each First Virtual participant uses what amounts to a pseudonym for Internet commerce, so some critics dismissed the service as nothing more than a credit card alias service. However, First Virtual's protocol specifications are written sufficiently broadly to allow a much wider variety of pay-in and

pay-out methods, and as they expand, you should expect to see more options implemented.

This chapter explores the issues and ideas behind Internet commerce, and then returns to First Virtual's system briefly to examine how it fits into the general scheme of things.

BUYING AND SELLING ON THE INTERNET

To understand Internet transactions, you should understand a little about the Internet, as well as a little about transactions. Later in this chapter the Internet, and commerce-related Internet issues, will be discussed in greater detail. Here, though, we will clarify the basics of Internet commerce through the judicious use of comparisons with other types of commerce.

It is assumed that the reader will have some real-world experience with various types of commerce, including the following:

- Direct purchases of goods or services in person (in retail stores or between individuals).
- Purchase of goods or services through catalog, mail order, or periodical advertisements.
- Purchase of goods or services through telemarketing programs (inbound or outbound telemarketing).
- Purchase of goods or services through direct mail solicitation.

Even without a clear understanding of what the Internet is, you can better understand Internet commerce by drawing comparisons between these types of transactions and transactions that are initiated, paid, and delivered by transmitting data across the Internet.

What's Different?

Buying and selling over the Internet differs from more familiar commerce media. For example, over the Internet there is no way for the consumer to check the seam stitching on a sport jacket or look underneath a vase for factory markings. However, this same restriction applies to any remote ordering method, including mail order catalogs, television shopping shows, and direct mail marketing.

The biggest difference between shopping on the Internet and shopping anywhere else is that all information traveling across the Internet may be subject to interception by a person or persons unknown — and there is no way to tell if the order you submit to an Internet merchant is being intercepted. Even more disturbing is the fact that it can be difficult to discover a transmission's actual origin, making the issue of trust in the merchant's online presence another source of uncertainty.

On the positive side, using the Internet to trade makes possible trading with no physical interaction of any kind. Delivery of information products from any part of the world to any other part of the world is trivial, as long as buyer and seller are both connected to the Internet. However, this presupposes that there is a way of billing the customer digitally as well.

What's the Same?

In a nutshell, the most basic similarity between real world and Internet transactions is *caveat emptor* — except that *caveat vendor* applies as well. Internet transactions take place over public channels (the Internet) between two entities that may have no prior contact and little or no way to confirm identities and build trust. The result is that both parties

to such transactions must have relatively high levels of trust in each other ("Why would someone steal from me?"), or else must use systems that obviate the need for such trust ("We don't trust anyone, but that's OK because we've got that covered").

A flashy Web storefront, use of well-known brand names, or references from reliable sources may help inspire greater confidence on the part of Internet consumers, just as a plush storefront under a nationally known chain store name can inspire confidence on the part of real-world consumers. However, other parts of the real-world shopping experience are less easily reproduced on the Internet.

Printed receipts are not possible for Internet transactions, but digital receipts are possible. Just as a cash trade with a street corner vendor is less likely to be reversible than a credit card purchase from a department store, Internet transactions that leave an audit trail can also usually be reversed. For example, using a credit card to pay for something in person leaves an audit trail in addition to your paper receipt, so you have recourse through the credit card issuer when there is a problem. If you pay with cash and do not have a copy of a sales receipt, you may have more trouble returning unsatisfactory merchandise.

In short, the buyer and seller need to maintain a comfort zone of trust, within which they both feel comfortable that the other cannot get away with too much. If the system used to complete the transaction is properly designed, the merchant can feel comfortable that buyers have relatively little opportunity to get products without paying, and the consumer can feel comfortable that merchants have relatively little opportunity to get paid without delivering products.

THE INTERNET ENVIRONMENT

Electronic commerce is hardly an entirely new idea. Nor is the online transaction. Dial-up computer services, like those provided by CompuServe since 1980, usually include services and products that can be ordered online. Electronic funds transfer (EFT) is another relatively mature field that is only now reaching a mass market as ATMs, gas stations, and supermarkets increasingly accept credit, debit, and charge cards.

In 1993, when the World Wide Web protocols were first being proposed as Internet standards, few people outside the research and academic world had even heard of the Internet, let alone used it. But by 1995, the Internet and the World Wide Web were sufficiently well-known that major mainstream publications no longer defined Internet-related terms such as Web site, home page, or Usenet news posting.

The Internet Advantage

The Internet had a long existence as a noncommercial research network. Its commercialization owes its apparent success to several factors:

- The Internet is an open network.
- The Internet itself belongs to everyone.
- The World Wide Web is the Internet's "killer app."

All the Internet protocols are open and public, and anyone can use them to write software implementations that can interoperate with other computers and networks running those Internet protocols. Most of the competition among vendors of Internet and TCP/IP software is based on performance, ease of

use, and compatibility. Few vendors are foolhardy enough to announce new versions of their software offering even the most attractive of new features at the cost of compatibility with other TCP/IP implementations.

LAN (local area network) operating system vendors such as Novell and Microsoft have traditionally kept their product specifications private and incompatible, but by doing so they lost the benefits of having an entire community of researchers and developers working on interoperable implementations, as has happened with the Internet protocols.

Because of this openness, a wide range of implementations are available, from freeware and shareware versions of Internet application and networking software through high-performance, high-function versions of Internet software sold by companies such as FTP Software and SunSoft. This lowers the monetary barrier to small companies and individuals who wish to connect, but cannot afford to spend $500 or more per system to equip a personal computer to connect to the Internet.

Part of the openness of the Internet is derived from the fact that you do not have to belong to any special group, pay any special fees, or become anyone's customer to access any Internet content. True, there are fees to be paid to the Internet Service Provider (ISP) for initiating service, charges for connect time, and perhaps other value-added services such as e-mail accounts, but on the whole, the ISP functions like a telephone company, providing access and connectivity only.

In contrast, the more traditional online services (such as America Online, CompuServe, and Prodigy) charge users fees for connect time as well as to access certain value-added content and activities. More important is the limitation on the par-

ticipation in CompuServe or Prodigy forums or mailing lists: only CompuServe members can read or submit to CompuServe forums, and only Prodigy members can read or submit to Prodigy forums. No single online service overpoweringly dominates this market by force of an overwhelmingly large installed base of users, nor does any service offer sufficiently compelling content to capture that installed base of users.

Connectivity through the Internet allows any connected individual to browse any freely available content, without regard to memberships. At least as important is that anyone with a dedicated Internet connection and a computer can be not just an information consumer, but also an information provider. And instead of communicating with an online service population, the largest of which might include no more than four or five million members, people with Internet connectivity have the potential to communicate with anyone else connected to the Internet: 30, or 60, or 100 million people, or more, depending on when you read this.

The online services have recognized that, given the choice, users would prefer full Internet access to more limited online service access. They have moved quickly to provide Internet services to their users. Their online service content remains as a value-added product, but demand for the much vaster content available on the Internet is much greater.

World Wide Web, Killer App of the Internet

Most Internet applications were developed by computer scientists who were often more concerned with performance and extensibility than with usability. Applications such as telnet (for running terminal sessions on remote computers), and ftp (the File Transfer Protocol application, for transferring files

between two computers) once required that users have a high level of awareness and expertise about the operating systems of both the local and the remote computers. Modern implementations of these applications with graphical user interfaces are quite easy to use even for less technically sophisticated users, but before these front-ends were written telnet and ftp had a sufficiently high cost of entry — long learning curves — to turn off many potential users.

Even before 1993, there were enough different information providers on the Internet to make it a complicated matter to find a desired resource. Various applications were developed to make searching the Internet simpler, but none was sufficiently compelling to users. One application, Gopher, held promise. Gopher servers simply made various Internet resources available through a common interface, using menus instead of requiring entry of explicit commands. The resources could be file repositories or remote computers allowing guest logins, or they could use any other allowable Internet application; Gopher simply provided a simple character-based, menued front end to those resources.

No serious contender for a killer Internet application appeared until the World Wide Web began with the deployment of Web servers, and until graphical Web browsers became widely available. It had always been a hassle to track down sources of information on the Internet, connect to the server, and attempt to locate the desired data. The World Wide Web lets the end user simply point and click to navigate the Web and locate interesting or necessary information. It lets the information providers offer access to their own data, as well as other related information to a much wider audience. Even more attractive is the ease with which regular users can create and publish documents for Internet consumption.

The Web was an application that appealed to a huge potential user base: those wanting access to free or cheap information and entertainment, but without the hassles of figuring out how to work all the different computers and programs.

THE WORLD WIDE WEB

In 1989, the World Wide Web began to take shape as the ultimate networked hypertext document. The idea was to use a markup language to create documents, relying on *tags* (function-oriented labels that define how a part of a document behaves) rather than using traditional word-processing formatting options to control the way the document is displayed. The result is that parts of each marked-up document behave the way they are supposed to, no matter how they are being displayed. For example, if a line is tagged as a title, it can be printed out in a specified font and size appropriate for hard copy, but when it is displayed on a monitor it may appear in a different specified font, size, and color appropriate for that particular video display monitor.

This is a very dry and technical way of saying that Web documents can be created in such a way that a person using virtually any kind of computer (with a character-based or graphical user interface) can access virtually any information, resource, or device connected to a World Wide Web server. The user starts up client software and connects to a home page, and can surf on to other Web documents by traversing links on the home page and other connected pages. The result is a worldwide web of connections between information services on the Internet.

Connected services are often provided directly through Web documents, but the protocols allow any type of Internet

application to be accessed, including more traditional file transfer servers and terminal sessions on larger host systems.

Although backward compatibility with existing services and systems is vital, the Web owes its success to an extraordinarily simple user interface. Rather than requiring an explicit search for Internet resources using arcane tools, the Web makes all the services available in a graphical format, and the user simply points and clicks to access them. As it becomes trivially easy for increasing numbers to access a Web site, it also becomes an especially attractive avenue for companies looking for new ways to market their products.

World Wide Web document development, server maintenance, specifications, and standards are all important topics, but are also entirely beyond the scope of this book. Even though most Internet commerce activity is oriented to buying and selling through Web sites, it should be noted that First Virtual's services are entirely application independent — this means you can sell through Web sites as well as through ftp servers, telnet sessions or even e-mail exchanges just as easily. However, Web programming to enable servers to accept First Virtual payment will be discussed in Chapter 9.

World Wide Web Standards

The World Wide Web is defined by a handful of protocol specifications. Software developers use those specifications to implement the Web browser and Web server programs. The interaction between browser and server is defined by the Hypertext Transfer Protocol (HTTP). Web browsers send messages conforming to this protocol to Web servers; these, in turn, return the requested information.

Traditional Internet addressing conventions are for locating computers attached to specific network interfaces. Special Internet host names and addresses are used, but these are sufficient only to locate a computer — locating a specific resource on a computer can be equally complicated, requiring the user to search through (sometimes unfamiliar) operating system directories, folders, and files. The Uniform Resource Locator (URL) protocol specifies how individual resources (files, documents, or even a specific section of a document) are to be identified within the World Wide Web. Web browsers use these URLs in HTTP requests to remote servers. They identify to the server exactly what resource is being requested.

Information transmitted from servers to browsers comes from Web documents stored on the server that have been specially tagged using Hypertext Markup Language (HTML) tags that define the different functional pieces of each document. As mentioned earlier, tags allow different parts of a document to behave differently; most important are the abilities of text and graphics to behave as pointers to other parts of a document, other documents and resources, and especially resources on other Web servers. HTML documents consist of plain text (ASCII) files and may point to graphics files, other types of multimedia files (for example, sound or full-motion video files) stored in standard formats, or other network resources (URLs).

It isn't possible to put all the information that a person browsing the Web would like from your site into HTML formatted files. Large databases, in particular, work better when they stay in their original formats. The Common Gateway Interface (CGI) specifies mechanisms for passing information from the person browsing your Web server to other resources available through that server, in particular by collecting information

from the remote user in Web forms and then passing that information along to the other resource.

This type of interchange is vital to allow the remote user to access resources such as databases, but it is equally critical to collecting information (and then using it correctly and automatically) for the purposes of transacting business through the World Wide Web. Designing forms to collect orders through a Web site is not enough; there must be some mechanism outside the server to handle that information. The user's order needs to be processed: if a physical product has been ordered, inventory and shipping information must be handled; billing information must always be processed. CGI provides the link between the Web server and the rest of the commercial process.

Java, a network application programming language developed by Sun Microsystems, adds a further level of interaction between browser and server. By offering a set of programming tools that allow the browser system to actually download small programs from the server, Java permits much more sophisticated interaction between client and server.

Finally, the security protocols relevant to the World Wide Web include Secure Sockets Layer (SSL) and Secure Hypertext Transfer Protocol (S-HTTP). These will be discussed in passing later in the book, particularly in Chapter 3, but very simply these protocols add security to by providing methods for encrypting the information that passes between the browsers and server programs that support them.

Web Browsers and Web Servers

Web browsers (or clients) must be able to send HTTP requests and receive HTTP replies from servers. The most popular

browsers are fully graphical, although nongraphical browsers are a necessity for character-based operating systems. Browsers range from Spartan text-only implementations, such as Lynx for UNIX and other operating systems, to full-featured commercial products such as Spyglass Mosaic and Netscape Navigator. Browser functions can also be integrated into more complete network or communications packages (such as Netcom's Netcruiser or Wollongong's Emissary), or even into operating systems (such as IBM's OS/2 Warp).

There is no shortage of Web browsers for any taste or budget. All should provide access to any Web-connected resource, although some will offer extra functions or features such as integration with other Internet tools (e-mail, network news), options for saving or copying retrieved data to files, and display customization options. Performance enhancements, such as the ability to "cache" or save documents already retrieved, can also differentiate browsers.

Just as Web browsers are available for virtually every computer and operating system, Web server software is also widely available. To offer Web services, a computer must be connected to the Internet, be running a Web server program, and have Web documents available. Web servers can contain highly graphical content without being able to display that content locally: The server system need only be able to run the server software and store the hypertext documents and files.

Although a basic PC with a full-time dial-up telephone link to the Internet is sufficient to act as a Web server, it would not be sufficient to serve very many simultaneous users. More often, Web servers are set up on higher-performance systems with higher-performance connections to the Internet. Individuals and organizations wishing to provide Web services have the option of setting up (and managing and maintaining) their

own system, or paying an Internet presence provider to run their Web sites for them.

Again, despite industry focus on the World Wide Web, First Virtual commerce can be conducted across other applications with a variety of software.

Selling on the World Wide Web

With its easy-to-use and graphical interface, the World Wide Web is an ideal medium for commerce. The biggest obstacle to commercialization of the Internet, its funding by government agencies for research purposes only, disappeared rapidly in the early 1990s as those subsidies expired and were not renewed. The current obstacles, lack of market penetration and lack of mechanisms for secure transactions, are rapidly disappearing as consumers and businesses are flocking to the Internet and developers are turning their attentions to the problem of securing the Internet for commerce.

Keeping in mind the previous discussion of commercial transactions, selling on the World Wide Web parallels selling in the real world. Very simply, the customer enters the merchant's Web site and views the product and company information made available there. If the merchant successfully sells a product and fosters sufficient trust in the customer, the customer will place an order. How and whether that order is placed will depend to some extent on what payment options are available.

For example, the purchase of a digital product, such as the text of an article, can be carried on entirely through the Web page: The buyer selects the desired article, provides payment information (for instance, providing a First Virtual Internet payment system account identifier), and the Web server trans-

mits the article. Purchases of physical goods require that the customer provide complete shipping information, and the merchant may desire a higher level of assurance that the customer's payment will be made good. First Virtual provides this level of assurance through digitally signed payment authorization notifications to merchants, which consumers need never concern themselves with.

Many merchants don't accept any type of secure (or unsecure) online payments. Instead, they require customers to make purchases through "traditional" means: a telephone call, a fax order, an e-mailed request for ordering information, or perhaps they must even come into a physical store or office to make a purchase.

First Virtual's approach to Internet commerce is to provide a basic, intermediary service to buyers and sellers. Unlike some other companies offering Internet commerce services, First Virtual does not tie participants to any particular Internet application — like the World Wide Web — or to any particular software program, operating system, or hardware platform. First Virtual does this by creating open protocols for Internet commerce and earning its profit from the transactions themselves. While First Virtual merchants are free to sell on the World Wide Web, they also have the option of selling through other Internet applications, including e-mail.

Other Internet Sales Venues

For many years before anyone even imagined the World Wide Web, electronic mail and network news existed. And for many years before Internet access providers started selling dial-up access, people were doing business with each other by e-mail and network news.

Acceptable Use Policies (AUPs) forbade commercial use of those parts of the Internet supported with government funds until the government moved out of the Internet business, but in practice this was interpreted to mean activities engaged in purely for profit. Personal possessions were routinely advertised in the appropriate news forums, although trying to sell magazine subscriptions or aluminum siding in lists devoted to computer operating systems was highly inadvisable. Used cars, computers, memory, and telephone answering machines were routinely sold online, generally through postings on lists devoted to personal items for sale.

Setting aside some of the "religious" discussions that "for sale" posts often incited (Is it appropriate to advertise a used network hub for sale on a network discussion group? Is puppy-farming a hobby or a business?), the problems of transacting business across an unsecure, unreliable, and public medium became glaringly obvious.

First was the problem of fraud. Negotiating prices and delivery options by e-mail is quite easy; making sure that payment and delivery both occur is hard. Unless the parties were able to meet physically, there was no satisfactory solution to this problem. With no control over online identities, it is difficult or impossible to determine exactly who has sent an e-mail message, and unscrupulous individuals have taken advantage of this fact. Buyers often found that they had sent a check or money order off to a post office box, but never received the disk drive or monitor they thought they bought. Sellers often shipped their used equipment off to a remote address and then never got the check that was forever in the mail.

Obviously, there were enough honest individuals buying and selling to make it worthwhile, and there were ways to check up on uncertain quantities. One was to get phone numbers,

addresses, and references for faraway buyers and sellers — but this added significant costs in time and money. Another option was to limit all sales to cash, in-person transactions, which also limited to the number of potential buyers, but eliminated the problems of nonpayment and nondelivery.

Credit card sales, though far from common, did happen. Some individuals had set up as corporations for the sale of specialized books, software, music CDs, and other products; when buying from these people, it was possible to send a credit card account number by e-mail. Despite it being transmitted in clear text between any number of different hosts through the Internet, I am not aware of any instance of a credit card number being intercepted on the Internet and misused. Either no one is willing to admit having sent credit card numbers by e-mail (it is widely considered to be pure folly to do so), or thieves looking for credit card numbers have easier ways to steal them than by putting a packet sniffer on an Internet backbone and digging them out of the gigabytes of e-mail, news posts, and World Wide Web graphics image downloads.

First Virtual makes commerce by e-mail a much more viable option for those without World Wide Web access, particularly as further security and authentication features are added. Adding the ability to sell simply and easily via e-mail (or any other Internet application) is a further advantage that First Virtual offers to aspiring entrepreneurs and large marketing organizations alike.

While the Web is popular in the United States and other developed nations where multimedia, high-performance, personal computers and workstations are routinely installed in home and office, the rest of the world still makes do with character-based interfaces and must rely on e-mail for their Internet

access. Being able to sell to those further millions whose only Internet link is through e-mail is a big plus for vendors.

INTERNET COMMERCE ISSUES

Doing Internet commerce is not necessarily a simple matter. If it were, there wouldn't be so many different approaches. Some of the approaches are quite similar to each other, some quite different from each other. To be considered seriously, though, every approach needs to address certain basic issues raised by doing business over an open network.

Informal Procedures Aren't Enough

There was a time when informal procedures were sufficient to do business on the Internet. It is not unusual, for example, to post a digital classified advertisement on a Usenet newsgroup devoted to sales of personal items. Terms and conditions of the sale are determined by the seller and the buyer. The participants in the transaction may determine the following by e-mail or by telephone prior to making the deal:

- How the buyer can view or try out the goods for sale (meet at the seller's home or office, the buyer's home or office, or some intermediate public place).
- How the product is to be delivered (personal pickup, UPS, postal service, private delivery, etc.).
- How the product is to be paid for (personal check, cash, barter, etc.).
- What recourse the parties to the transaction have in the event of a dispute.

Some individuals even sold products via e-mail, with purchasers sending their credit card numbers in the clear. Before the Internet expanded significantly beyond the borders of the academic/research universe, where most people know (or know of) each other, this approach worked reasonably well. However, it is inadequate for dealing with the much larger Internet population of today.

More to the point, doing business as a business, rather than selling your used car or old sofa, requires a much more formal approach that protects both customer and merchant from fraud and theft. Finally, negotiating the terms of each sale individually between customer and merchant is a waste of time for both the buyer and seller, but establishing the terms of doing business requires that the interests of both parties — as well as other interested parties, such as credit card issuers — all must be protected.

Securing Financial Information

So far, the explicit focus of Internet commerce mechanisms has been security: the transaction, which occurs in an open forum (the Internet), has to be done in such a way as to protect the customer and the merchant. The customer needs to feel comfortable that credit card numbers (for example) cannot be stolen and used without the customer's knowledge. The merchant needs to have some way of making sure that thieves cannot pass invalid credit cards, cannot steal other people's valid credit cards from the merchant, and cannot steal the merchant's products. The participant in the process with the most to lose, perhaps, is the credit card industry.

The issue is that credit card numbers are easily recognizable: they use account numbers of uniform length, different types of

credit cards all begin with certain number sequences, and when used for payments, they end with expiration dates that also conform to an easily recognized pattern.

Until digital currency and digital check cashing achieve a higher level of acceptance, the credit card is the vehicle of choice for digital commerce — everyone (at least, almost everyone deemed desirable as a customer, and with Internet access) has a credit card. Those using digital currency or digital checking are still in the minority.

Protecting customers' credit cards from theft on the Internet, therefore, can be accomplished in two ways:

- Send the sensitive data over the Internet, but make it readable only by the merchant and/or the credit card authorizing organization by encrypting it.
- Don't send the sensitive data over the Internet, but send something else that references the credit card or other payment method.

How these approaches are implemented in real-world Internet commerce mechanisms will be discussed in Chapter 3, while encryption techniques will be discussed in Chapter 2. The payment data must be protected, since it is a relatively simple matter to tap into Internet transmissions and monitor them for credit card numbers.

> **NOTE:** The ease with which this type of Internet sniffing can occur depends on the level of physical security in place on the networks being monitored. Internet service providers and companies providing Internet backbone service are expected to exercise great vigilance to prevent this from occurring. While network thieves would prefer to monitor backbones, they may find it much easier to monitor organizational internetworks connected to the Internet.

Authenticating Transaction Data

The process of making purchases in the real world has been defined and refined over the years, to the point that most take it for granted. However, there are certain aspects of the process that are not easily or intuitively transferred to the virtual world of Internet buying and selling.

For one thing, the process of authenticating an offer from a seller or buyer is trivial in real life. A merchant of physical goods usually puts a price tag on or near the product being sold; additional discounts or other promotions can be documented through posters in the store or copies of ads placed in magazines or newspapers. Even broadcast media promotions can be verified by referring to a magic word or phrase, so the merchant knows the customer heard or saw a specific commercial.

In the store, you can decide precisely which product you want, at what price and in what color; if there is any question, you can ask a sales clerk or store manager. Once the product is purchased, both merchant and customer keep a copy of a receipt for the purchase.

Translating these functions to the Internet takes some doing. One approach is to use digital signatures (explained in Chapter 2): the merchant can sign an offer of a product, and the customer can sign a purchase request, to provide a higher level of assurance that all parties are willing to stand behind the deal. First Virtual uses digital signatures on messages they send to merchants who request them, to verify that a payment has been authorized for a particular transaction. This mechanism makes it possible for merchants to sell hard goods over the Internet, because the digitally signed notification indicates that the credit card transaction has actually been authorized, not just that the buyer has approved the transaction.

First Virtual also uses another method of authenticating transactions: the consumer must respond by e-mail to confirm (or deny) all transactions. By keeping the transaction initiation separate from the confirmation process, and by relying on authoritative Internet address services, First Virtual is able to maintain a high level of confidence that transactions are properly authorized. For example, there is no way to deduce a buyer's account identifier from the buyer's e-mail address, nor is there any way to deduce the buyer's e-mail address from the buyer's account identifier. Therefore, breaking the First Virtual system requires malefactors to get both those pieces of information before they can complete a fraudulent transaction.

Paying for the Privilege

The costs of doing business on the Internet parallel many of the costs of doing business in real life. Companies with interests in Internet commerce can make their money through a number of different mechanisms:

- Sales commissions
- Transaction fees
- Software sales
- Financial services

Since most consumer-oriented Internet commerce uses credit cards, the costs of most transactions are already split between the consumer and the merchant. The consumer may pay an annual credit card membership fee, as well as interest on balances. The merchant pays a percentage of credit sales, as well as certain transaction and other charges.

Internet commerce companies therefore have the option of staying entirely out of the transaction between merchant and

consumer. They can make their money through selling the software the merchant and consumer use to do business — or they can make money off the interaction between the merchant's bank and the financial institutions that authorize credit card charges.

As a result, consumers who use secured browsers or digital wallets to make purchases do not pay any extra for the privilege, though they may have to purchase special software. For example, the Netscape Navigator browser is sold for about $40; the CyberCash digital wallet, on the other hand, is distributed freely to all consumers.

Merchants, too, may have to install special software to support acceptance of payments from secured browsers or digital wallets. This software may be free, like the merchant software from CyberCash that is installed on merchants' existing Web servers. Secure Web servers, however, are generally not free. While vendors are now starting to offer secure Web servers for well under $1,000 (some as low as $100), merchants can easily pay much more for secure Web servers from companies such as Netscape or Open Market.

First Virtual charges merchants a percentage of their sales proceeds (2%) as well as small transaction fees. Customers, too, have to pay a small fee for opening their account. But there are no other customer fees, and there is no software to buy. The merchant pays no additional banking fees, and does not need to open a merchant banking account.

THE FIRST VIRTUAL WAY

Many of the companies offering Internet commerce services have done so by examining the way business is currently being

conducted and then translating those procedures (as much as possible) into procedures that can be completed over the Internet. To a large extent, security is built through reliance on encryption technologies. For the most part, Internet commerce systems implemented to date make buying on the Internet very much like buying from a mail order catalog.

First Virtual has attempted to engineer a way to do business on the Internet that is

- Safe for consumers and sellers
- Profitable for sellers
- In harmony with the open nature of the Internet

They've done this by taking a holistic approach to securing the entire transaction process, by using automation and the Internet itself to keep entry and ongoing costs low, and by devising commerce protocols and procedures that make it possible to browse and to buy without special software or expensive services.

A Holistic Approach to Security

The First Virtual approach to transaction security is based on the assumption that anything transmitted on the Internet can be intercepted by criminals. Rather than putting all their security eggs in the encryption basket, First Virtual has done everything possible to keep transactions from being susceptible to fraud, while at the same time keeping exposure from such crimes to a minimum.

Systems that depend entirely on an encryption scheme for their security may suffer catastrophic losses in the event that their

encryption scheme is defeated by a criminal. For example, a version of Netscape's Navigator program released in 1995 improperly implemented a very secure algorithm — in an unsecure manner. The result was discovered, made public, and corrected in a matter of days. However, if someday someone discovers and exploits a more subtle flaw in a key piece of software or a trusted encryption algorithm, the result could be literally catastrophic.

In one scenario, the criminal could choose to simply skim a few credit card numbers at a time off the Internet and use each of them, once, to steal something of value. In another scenario, the criminal could accumulate a huge number of credit card numbers over some period of time and then flood the system with fraudulent transactions to disrupt the entire system.

First Virtual avoids this type of problem by disconnecting the credit card (or other payment information) from the transaction data transmitted on the Internet. If a thief were able to steal a First Virtual account identifier, that identifier by itself would not be very useful. The process has been engineered so as to make it difficult in the extreme for a criminal to fraudulently complete even a single transaction, let alone create an automated procedure for stealing.

If a First Virtual account identifier is stolen, it can be used to initiate a transaction — but consummating a transaction requires that the malefactor be able to discover the e-mail address of the owner of the account, capture all e-mail messages sent to that account, and forge e-mail from that account. The First Virtual process and how it provides security to the transaction are discussed in greater detail in Chapter 3. Very briefly, however, First Virtual provides security by making it costly, in time and effort, to defeat the system — and by keeping the losses due to such defeats relatively small.

Paying for the Service

The First Virtual payment system depends on volume: if you don't make money by selling your product, neither does First Virtual. More to the point, however, is that First Virtual is an ideal tool for small businesses, entrepreneurs, and aspiring entrepreneurs to test the market for their wares. With the charge for a seller's account only $10, practically anyone can start selling on the Internet on a shoestring (accounts activated for buying only can be opened for just $2.00).

The transaction costs are paid directly by the merchant to First Virtual (more properly, they are deducted from customer payments by First Virtual before the balance of sales proceeds are paid to the merchant). The actual costs are probably shared by the consumer and merchant, as most merchants very likely build those costs into product prices — just as real-world merchants build transaction costs into their prices.

FIRST VIRTUAL OVERVIEW

The rest of this chapter outlines the way First Virtual's payment system works. The principles of its implementation are to do the following:

- Separate the payment mechanism (credit card, checking account) from the transaction and delivery mechanism (transmission of information across the Internet).
- Define a set of protocols and procedures for transactions that allow the widest possible use by making them independent of software and applications, and by making allowance for different payment options.

- Use the lowest common denominator, Internet e-mail, for transport of transaction information, as well as to use secure, reliable, and robust tools for securing the sale of physical goods as well as information.

Very briefly, First Virtual's Internet payment system consists of a set of rules for transacting purchases and sales. One of the first rules is that vulnerable payment information (a credit card account number, for example) is never transmitted over any open network. Instead, although consumers and merchants initiate their applications for First Virtual accounts over the Internet, actual financial data is collected through direct telephone transactions or by postal mail, and transactions are settled by First Virtual through secured private networks connecting them to credit card authorizers.

Another rule is to provide commerce services independent of any particular Internet application or protocol. This means that whether you have complete and direct Internet connectivity or only indirect, e-mail access to the Internet, you can buy or sell through the First Virtual system. This also means there are generally several different ways to accomplish any First Virtual function (buying, selling, or administering accounts) to accommodate different levels of connectivity and Internet applications of choice.

One more general rule is that a purchase of soft goods (information in the form of data, such as a text file, a graphics file, or a program file) should not be a matter of blind acceptance by the buyer that the product is worth the price. First Virtual strongly encourages that merchants allow consumers to download the soft-good product prior to making a purchase commitment.

Once the account is associated with payment information (a credit card to charge the buyer's purchases and/or a checking

account to credit the seller's sales), that data is kept entirely offline from any public network. A separate, nonsecured account ID (called a VirtualPIN) is associated with the account for the purposes of buying and selling.

The First Virtual rules define the way purchases and sales are transacted, and they require the exchange of certain information. Very briefly, the process typically goes something like this for the sale of a product that can be transmitted across the Internet (a text, graphic, or program file):

- Purchaser decides to buy a product.
- Purchaser sends VirtualPIN to the seller.
- Seller sends a copy of the product to the buyer.
- Buyer reviews the product and decides whether or not to pay for the product.
- First Virtual sends e-mail to the purchaser asking for purchase decision.
- Buyer can choose to pay for the purchase, or decline, based on whether the product meets needs and expectations.
- First Virtual credits seller for approved sales (a three-month holding period, to allow purchasers the ability to refuse improper charges on credit card statements, is waived for sellers who submit an application and qualify for the waiver).

The process is slightly different for selling hard goods, where merchants can request a higher level of assurance of payment for the sale before they deliver a product.

First Virtual charges $2.00 to create a new buyer's account, and $10 to create a seller's account. The buyer pays no other fees, while the seller pays a 2% commission on all sales through First Virtual plus some small transaction fees.

There are a number of questions that often come up on first hearing about the First Virtual payment process. These, and other issues, will be discussed in far greater detail throughout the rest of this book, but the broad outlines of answers can be provided here.

Can't People Steal My Information Products?

Potential merchants are concerned that this framework leaves them open to information thieves. However, giving potential buyers the option of trying out your information product before making a commitment to buy is very common in offline selling milieus. For example, most bookstores provide chairs and tables for customers to peruse books before they decide to buy; car dealers routinely provide "test drives"; and music stores have "listening booths" where customers can preview music CDs before buying.

There is nothing stopping one person from downloading your software program and declining to pay for it. However, First Virtual has implemented software that monitors the rejection rates for each vendor; buyers who too frequently download information and then decline to pay will eventually have their accounts terminated. However, returns are a fact of life for merchants of any type, so the "try before you buy" approach for information goods offers an excellent method of avoiding chargebacks.

The issue of "loss" relating to information products that are delivered but not paid for is virtually moot, since there is (virtually) no additional cost borne by the merchant to make that delivery. The cost of the goods sold is almost entirely invested in the creation of the digital product, so there is no actual cost incurred when someone downloads a file and does not pay for it.

The sale of physical products, or hard goods, creates more of a problem: the buyer has to approve the expenditure before the merchant will ship it. What's more, the merchant needs to have some fairly strong indication that the sale will be made good by the underlying credit card issuer before shipping. What works for soft goods doesn't work as well for hard goods, since merchants take actual losses when they ship a pair of blue jeans or a videotape to someone who later refuses to pay for it. Starting in 1996, First Virtual provides digitally signed confirmations to merchants who request a transfer notification indicating that the underlying payment system (e.g., the credit card issuer) has authorized payment. This allows the merchant to ship the goods, confident that payment will be forthcoming.

Can't VirtualPINs Be Compromised?

It would not take overwhelming effort or expertise to compromise a VirtualPIN. They are transmitted in the clear over the Internet. Anyone sniffing (monitoring) a network over which a VirtualPIN is transmitted can capture it. However, once captured, the VirtualPIN can be used only for purchase of goods through First Virtual merchants — and only soft goods can be delivered to the thief, unless he or she can also subvert the VirtualPIN holder's e-mail.

Furthermore, since all transactions must be approved by the owner of the VirtualPIN by responding to an e-mail notification, it is unlikely that a stolen VirtualPIN will remain usable for very long after its first unauthorized use. As soon as an unauthorized transaction is recognized, the owner sends a fraud notification to First Virtual and the account is canceled.

It Seems Awfully Complicated

When the process of setting up an account and making purchases through First Virtual is first described, the first reaction is that it seems terribly complicated and a lot to do and remember. However, once you have gone through the process yourself, you will see how straightforward and simple it can be.

Though all the details of setting up accounts and making purchases are provided later in the book (Chapters 6 and 7), all that is involved in starting your account is this:

- Provide basic account information.
- Select a word or phrase for your VirtualPIN.
- Submit the application information (usually by clicking a button or pressing the Return key).
- Wait for an e-mail confirmation with instructions on what to do next.
- Make a phone call and enter your credit card payment information to enable your account for buying.
- Send in a check to enable your account for selling.

That is all — there is no software to install, no other forms to fill out, no other phone calls to make. As will become apparent in Chapters 2 and 3, other electronic commerce options require consumers to use special software that may take a considerable amount of time to install and configure properly.

Making purchases is also incredibly easy. The process goes something like this:

- Click on a "Purchase" button and download the soft good being sold.

- When you receive an e-mail notice of the transaction, send a reply of "yes" to pay for the product, "no" to refuse payment for the product, and "fraud" to indicate that you did not initiate that transaction (this invalidates your account to avoid further fraud).

That is all. The basic requirement for any consumer is that you check your e-mail regularly so fraudulent purchases can be caught quickly.

CHAPTER TWO

SECURITY ISSUES, SECURITY TOOLS

Contents

WHY THE INTERNET IS UNSECURE 38
It's the Protocols 40
Where the Risks Are 42
What the Risks Are 42
Internet Security Holes 43
A Bigger Risk 45
What It All Means 46

NEW TOOLS FOR CRYPTOGRAPHY 46
Cryptography 47
Cryptographic Objectives 48
Codes and Ciphers 50
Breaking Encryption Schemes 51
Securing Algorithms 53
Distributing Keys and Keeping Them Secret 54
The Public Key Solution 55
Public Key Implications 56
Key Distribution and Certification 58
Trusted Key Distribution and Verification 59

CRYPTOGRAPHIC APPLICATIONS 60
Encryption 60
Digital Signature 61
Nonrepudiation and Message Integrity 62

Summary Security is a major stumbling block to electronic commerce: consumers, merchants, and banks each have their own interest in securing Internet transactions, but without security no one is quick to take business online. The Internet is open — meaning transmissions can be overheard, intercepted, and forged. However, there are tools that can be used to attempt to eliminate the risks inherent in communicating over an open link. This chapter explains why the Internet is unsecure and examines the cryptographic tools used to secure it, specifically public key cryptography, digital signatures, and encryption.

WHY THE INTERNET IS UNSECURE

Despite a high level of commercialism, as of 1996 the Internet is still very much a product of the research programs from which it originated. The Internet is simply the implementation of protocols, or rules of operation, that define the way connected computers communicate with each other. When every connected system follows these rules, they can all communicate with each other — even if they use different hardware, software, or operating systems. Connected systems can even be connected to different types of networks, but as long as they all run the Internet protocols, they will be able to interoperate.

The people upon whose work the Internet is based intended to prove the feasibility of internetworking, not to produce a commercial product for internetworking. As a result, the things consumers of commercial computer products look for, such as easy-to-use interfaces and secure operations, have never been present in Internet Protocol suite specifications.

Until very recently, the overwhelming majority of people connected to the Internet were academics or researchers, and Internet traffic was restricted to not-for-profit uses. Users then, as now, were advised not to trust any sensitive information to the Internet. Most computers connected to the Internet were UNIX boxes, with the remainder being large, multiuser systems — all of which had their own security implementations. One of the most important functions fulfilled by Usenet news groups was dissemination of security information and warnings about risks uncovered in various operating systems and TCP/IP implementations. The prudent network manager used heavily monitored Internet firewalls to strictly filter data being sent in and out of the organizational network. This is still recommended now.

Securing personal computers on a network is considerably more difficult than securing UNIX workstations and mainframes. There are as many points of entry to the network as there are personal computers, PC security tools range from nonexistent to barely adequate, and the PC users themselves are notoriously lax in their security practices.

In any case, the Internet is definitely an open network. Once data is transmitted beyond the organizational network, it may be handled by any number of different intermediate computers (called routers), which make sure the data is delivered to its intended destination. Data is also likely to travel across Internet backbone networks, which move vast quantities of data over large distances. Information is vulnerable at many points, including the originating computer (which may have been tampered with at some point to subvert it), the local or organizational network (local traffic is almost trivially easy to listen to and requires little more than a connection to the same network), and some intermediate system or network out on the Internet. The same risks exist for the networks and systems on the receiving end.

Smart network managers and administrators take great care before connecting any corporate system to the Internet, implementing elaborate and extensive filtering systems and firewall networks. Before one dismisses this attitude as paranoid, it must be put in the context of other information risks:

- Long-distance telephone calling card accounts (along with personal identification numbers, PINs) are routinely looted by watchers (some using binoculars) at airports and train stations.
- Intruders routinely take advantage of unprotected systems not just to search them for valuable or interesting information, but to use them as steppingstones to further attacks on other systems.

- More than 20,000 credit card numbers stored on a computer at an Internet service provider were compromised by an intruder in early 1995.

The service provider had not implemented sufficient security to prevent the attack, which apparently had not taken advantage of any inherent Internet weakness, but exploited security weaknesses in the actual computer. The point is that property must be protected, whether it is information or has a physical existence, because immoral people will try to steal it if they possibly can. Those apparently paranoid network managers realize that any corporate resource exposed on the Internet is at risk, and the solution is eternal vigilance.

It's the Protocols

Without getting too deeply into the guts of the Internet protocols and network architecture, the Internet functions on roughly four levels. Understanding a little about the way information moves around the Internet will help explain why the Internet itself is unreliable and unsecure — but can still allow reliable and secure messages to be sent and received.

The different layers represent different kinds of interactions. They are useful when designing internetworks because they separate and distribute important functions in an efficient way. The specific type of network cable that a computer is connected to is an important aspect of the Internet traffic sent and received by that computer — but only as it concerns moving that traffic from the Internet service provider to the computer. Likewise, the computer operating system and version of e-mail software is important, but only as it relates to the display of e-mail its user receives from the Internet.

The highest layer is defined by the interaction between the end user and the network resource. Called the Application Layer, its relevant protocols define the different applications available to users in the Internet. For instance, the World Wide Web application is defined by the Hypertext Transport Protocol (HTTP), and the most common method for file transfer is defined by the File Transfer Protocol. How each Internet application works is defined by its application protocol, which prescribes how commands are passed from the user to the remote system, and how requested information is passed back to the user.

Security and reliability may both be built into the application layer, if desired. Doing so means no intermediate routers need to worry about the reliability or security of the data they transfer from network to network (which means additional computations for verifications) — they just make sure it arrives at its destination. Once the data reaches its destination, the target computer can then make sure the data it receives is reliable and secure.

By using several different layers, data can move efficiently across the Internet. The program at the Application Layer collects information (from the end user or the network resource), wraps it up (encapsulates it), addresses it to the destination resource, and passes it down to the Transport Layer. The Transport Layer wraps the data up and addresses it to the actual program running on the destination system, and then passes it on down to the Internet Layer. The Internet Layer program wraps the data up and addresses it to a particular computer on a particular network, then passes it down to the Network Layer. If the destination computer is on the same network as the source computer, the software at the Network Layer simply sends the data directly to the destination; if not (as is usually the case), the data gets sent to

an appropriate router, to be forwarded to the destination network and host.

The software operating at any given layer is concerned only with moving a data chunk to its destination at the same layer: Network Layer software moves chunks of data between connections on the same physical wire; Internet Layer software moves chunks of data between two specific computers connected to the Internet; Transport Layer software moves chunks of data between two programs; and Application Layer software moves data between a user and a network resource. When Network Layer software receives a chunk of data, it unwraps it and passes it up to the next layer; this process continues until the actual application data is unwrapped and passed to the user or network resource.

This is a very abbreviated summary of how the Internet protocols work, but it is enough to show how data moves around the Internet, as well as where some of the security risks lie.

Where the Risks Are

It should be stressed from the very start that the greatest threat to security in any organization almost invariably comes from within. Insiders have the access, they know what is valuable, and they know what is most damaging. The same goes for the Internet, at least for now: The hacker who stole 20,000 credit card numbers did not exploit any weakness in the Internet protocols, he exploited the weakness in the security of the computer where those numbers were stored.

WHAT THE RISKS ARE

In any case, there are still some serious risks that you take on when you transmit data across the Internet:

- Interception by third party (someone other than the intended recipient reads mail you send)
- Forgery (someone sends mail and signs your name)
- Modification (someone intercepts your mail, changes it, and sends it on to its final destination)

Interception of your network traffic is only a problem if you are sending sensitive information, such as credit card numbers or digital cash. However, most Internet traffic is probably of little interest to anyone but the parties involved. One sure way to keep eavesdroppers in the dark is to not speak publicly about private matters. This works as well on the Internet as it does in a restaurant.

Forgery can be a much more serious risk. The nature of the e-mail protocols makes it a relatively simple matter for someone to send a message that appears to be coming from someone else. The possibilities for mischief (at least) are infinite, from forging a resignation memo from an office enemy to signing someone up on several high-volume e-mail lists. With no physical evidence, e-mail forgery is relatively easy to get away with, which eliminates one restraining factor that might keep someone with insufficient moral compass from doing it.

Another insidious threat is that someone will intercept transmissions, modify them, and send them on to their destinations. For instance, a criminal could intercept a message from a vendor and change the payment instructions, directing payment to the criminal's account. Again, the devious mind can come up with any number of other options for mischief.

INTERNET SECURITY HOLES

Once you've secured your own computer system — using access codes or passwords, physically restricting access to it, and making sure that it is not left unattended while connected

to any remote services — you can start to worry about the risks from your Internet connection.

The first step your data takes when it leaves your computer is to a router connected to the Internet. If you are linked through an organizational Internet connection, your own system may actually be visible to anyone else connected to the Internet; more likely, though, your organizational Internet connection will sit on the other side of a firewall gateway system. Firewall gateways function by hiding organizational systems from the rest of the Internet, while still providing access for approved applications to send and receive data. Organizations that use firewalls also usually put their public access systems, such as World Wide Web servers, just outside their firewalls, and keep sensitive material off those servers.

What if you don't have a corporate connection, but rather use a dial-up connection (SLIP or PPP) to an Internet service provider across a telephone line? In theory, your computer is vulnerable to attacks any time you are connected. Your system at those times can act as a server — but only if you are running a server program.

The larger issue is what happens to your Internet transmissions when they leave (or before they arrive at) your computer. Anyone with access to the router through which you receive your Internet traffic (or the network to which it is connected) has the ability to eavesdrop on your sessions. Security depends on the integrity of participating network and system managers, as well as on their ability to keep out intruders.

As someone who has been entrusted with access to sensitive systems like these, I would like to believe that anyone who has been given that kind of access is an upstanding, moral person. However, although the vast majority of people are honest,

there will always be a few bad apples who will betray their trust for money, for power, or just for fun.

This security risk exists at every interconnection, so if you purchase your Internet service from a local reseller, chances are that your transmissions get passed from the local company to a regional company, who passes them on to Internet backbones. There may quite a few intermediate networks and systems between your computer and the computers you communicate with, each with its own support staff that must be trusted to be capable of running a secure network (to keep outside intruders out) and a moral one (to keep insiders from selling out).

A Bigger Risk

Whenever the user must provide his or her own password, attacks on individual accounts are possible, just as they are in any system that uses passwords for access. This means that customers must take as much care in protecting the passwords to their secure commerce services as they would in protecting their own wallet:

- The password should not be easy to guess (like a name or birth date).
- The password should not be written down near the computer from which it will be used.
- The user should not give out the password to anyone, ever.
- The user should not leave an active session running on an unattended, unprotected system.
- Passwords should be changed periodically.

As long as precautions are taken, and passwords protected properly, they will keep the system secure. If the passwords are

not protected, however, the only thing they provide is a false sense of security. It should also be noted that requiring users to maintain (and remember) a separate user ID and password for every commercial site they connect to makes it increasingly difficult for users to actually follow basic security principles, and more likely that they will fail to do so.

What It All Means

The bottom line is the Internet is a public network, and anyone concerned with transmission security needs to approach the Internet in the same way one would approach communicating by any other public means. Internet communications are functionally equivalent (at least as far as security goes) to communicating in a public hall. Conversations between you and your neighbor can be overheard by anyone who wants to eavesdrop; if you want to talk to someone at the opposite end of the hall, you've got to rely on intermediaries to carry the message between you.

NEW TOOLS FOR CRYPTOGRAPHY

Modern cryptography offers solutions to many of the problems of communicating securely across open networks like the Internet. This section introduces some of the basic concepts of modern cryptography, on which most online commerce schemes depend. This section simply raises some of the pertinent cryptographic issues as they relate to transmitting commercial transactions across an open channel; discussion of the actual algorithms, implementations, and the mathematical basis for private and public key cryptography are all far beyond the scope of this book. The interested reader will find

more detailed discussions of cryptographic protocols elsewhere. The following books all include discussion of the actual cryptographic algorithms and implementations:

- *Applied Cryptography,* Bruce Schneier, John Wiley & Sons, 1995
- *Network Security: Private Communication in a Public World,* Charlie Kaufman, Radia Perlman, Mike Speciner, Prentice-Hall, 1995
- *PGP: Pretty Good Privacy,* Simson Garfinkel, O'Reilly & Associates, 1995

In this section we will simply introduce the basic underlying concepts relating to the use of cryptographic techniques and their implementation in commerce systems.

Cryptography

As an individual, if you've got something "sensitive" to say to someone, chances are you can find a way to do this without resorting to secret codes: a whisper in the right person's ear, a confidential chat in a bar, or a discreet letter are all reliable ways to share a secret (keeping the secret later is another story). You've got control over who is listening, and you need not worry about anyone trying to read your mail (unless you are a criminal kingpin, revolutionary leader, or subject of some other investigation).

If you did want to protect your sensitive communications, chances are you'd try to use some kind of code or cipher, replacing the "real" words with "code" words, or shifting characters to hide the real meaning of your messages. Cryptography literally means "secret writing." It is the discipline of creating codes to enable this type of writing.

Governments and military organizations have always needed to protect their communications (lives depend on it). And since the stakes are so much higher, there is more risk that the messages will fall into the wrong hands — so there is greater incentive to hide the meaning of the message. If there were a method of passing messages that could not be detected by anyone but the intended recipient, then cryptography would be unnecessary. However, cryptography has become indispensable to organizations such as armies and navies that depend on radio transmissions, for example.

Because they offer reliable and secure communications methods such as a (relatively) sacrosanct postal service and (usually) bug-free telephone service, governments have argued that their law-abiding citizens had no need for cryptographic services. Only the government had the power to read your mail and listen to your telephone conversations, so that was OK. In an increasingly digital world, though, there are more opportunities for practically anyone to listen in — and those opportunities are more lucrative. The result has been the adoption of encryption technologies for Internet applications for the purpose of keeping transmissions private.

CRYPTOGRAPHIC OBJECTIVES

There are several objectives to be gained by using cryptographic techniques. The most obvious is to keep secrets, but there are others that can be just as important.

When you receive a signed document or letter in the mail, there are certain things about that document that you often take for granted. For instance, if the document is handwritten and signed by the author, you can be reasonably certain that the document indeed originated from that person. The

document may be addressed directly to you, both on the envelope and at the top of the document itself — assuring you that you are the intended recipient of the document. The document may be enclosed in a sealed container, perhaps signed on the seal, to assure you that no one else has seen the document. You can examine the entire document and envelope for erasures, changes, or other signs that it has been tampered with.

When you receive a message across an open network, however, you don't have these attributes to examine. Whether the message is encrypted or not, you need some way to assure yourself of the following:

- The message has not been forged, and in fact originated from the indicated author.
- The message has not been modified in transit by some third party.
- The contents of the message cannot be denied by the author.

In practice, there is no way to avoid the possibility that someone has intercepted your message and looked at it. That is where encryption can be useful — to keep anyone but the intended recipient from being able to read the message.

Cryptography as we know it uses encryption to transform plaintexts into encrypted texts. Ideally, encoding or decoding do not require too much effort, but decoding without the keys is difficult enough to discourage almost anyone from trying to do so. The fact is that encryption schemes can always be broken, if you have enough time and resources. The idea behind modern encryption methods is to make it so costly in time and resources for an interceptor to interpret a message that it is

not practical to even attempt it — while keeping it easy for an authorized recipient to read.

The strength of the encryption scheme needed is determined by how long you want to keep your secret. For example, if you're planning a surprise birthday party in two weeks, you might trust a scheme that required a month of continuous effort to break; a corporation would want a stronger method to protect long-term plans or trade secrets.

CODES AND CIPHERS

The terms "code," "cipher," "encryption," and "decipher" all have quite specific meanings. Strictly speaking, a code actually uses some method of interchanging vocabularies so that each code word represents some other noncode word. Codes require special code books which act like dictionaries; if the code book is lost, encoded text cannot be interpreted — and anyone with the code book can read encoded text.

Ciphers are the basis of encryption schemes. Ciphers act on each character of a message, transforming it according to some repeatable rule, or algorithm. Keys are special numbers which help initialize the algorithm; different keys used with the same algorithm will produce different versions of encrypted texts.

At this point, keep in mind the objective of cryptography: keeping secrets secret. As was mentioned earlier, encryption is used when you cannot guarantee that a message will not fall into the wrong hands. If the information you encrypt is consistent (e.g., your data uses a consistent format, and much of the data can be guessed based on its source or destination), then even the strongest algorithms may not be able

to protect you against an opponent who is able to combine brute force attacks with educated guesses at the plaintexts you are sending.

But really good algorithms don't grow on trees, and there are plenty of ways to figure out which one is being used, which will be discussed in the next section. So, you'll settle for a key that can be kept secure, and an algorithm that's tough to break even if you know which one it is.

Traditional ciphers use a single key, which the sender and the recipient share (and try to keep secret from anyone else). The sender runs the algorithm using the key to turn the plaintext message into an encrypted message, and the recipient runs the same algorithm in reverse (using the same key) to decrypt the message. This is known as symmetric cryptography.

BREAKING ENCRYPTION SCHEMES

Encryption schemes are vulnerable on several fronts. You can analyze encrypted text for things like word and character frequencies, or trick someone into sending some particular message and then figure out what was done to that message, or find out what the encryption algorithm is and do a "brute-force" attack on it by trying every single possible key. The last method is a completely reliable way to break any encryption scheme — as long as you have enough time.

Cryptographers accept that all ciphers are vulnerable to brute-force attacks, and they design ciphers with this in mind. The key to security is usually the cipher key size. A cipher key can be compared to a combination lock: if you have the correct key, you can unlock the message. The three-digit combination locks often found on luggage offer minimal protection, since

there are only 1,000 different options. Sometimes you'll hit on the right combination in only a few tries (for example, if the combination was "007"), and sometimes the combination will be more elusive (for example, "999"); on average, though, you'll break the lock after trying half the total possibilities. At about a second per combination, this means I can open your briefcase, on average, in about eight minutes (and it shouldn't take more than about 17 minutes).

This level of security may be acceptable for keeping your co-workers away from the donuts in your briefcase, but not for much else. Adding another digit to the lock increases the number of possible combinations by a factor of ten; doubling the number of digits to six increases the number of possible combinations to one million. A brute-force attack on a six-digit combination lock, at a second per combination, now takes an average of almost six days (and could take as long as 11.5 days). Add another two digits, and you'd need over a year and a half, on average, to break in.

Of course, with computers in the picture, you can use much larger numbers — and much more complicated algorithms. Adding to the length of the key you use doesn't necessarily make encrypting or decrypting messages more difficult if you know the key, but does make it much less practical to apply brute-force techniques. I may want to steal your credit card number, but if it would take me a hundred years using ten of the biggest supercomputers in the world running at full tilt to do it, I won't bother (since the account will undoubtedly have expired by then).

There is a risk that computing technology will improve sufficiently to make practical brute-force attacks on currently adequate encryption schemes. Increasing the size of the key makes

it more secure over a longer period of time, but it also makes it harder to implement right now. The bottom line is that a good encryption scheme must represent a compromise between security and practicality.

Encryption schemes are also vulnerable to non-brute-force attacks. Although it is possible to prove that a cipher can be broken through some application of analysis or a smart search for keys, there is no way to unalterably and conclusively prove an algorithm is secure from attack. However, making details of the algorithm public, as discussed in the next section, can help improve the odds that it's secure.

SECURING ALGORITHMS

Keeping your algorithm a secret may be a tempting way to keep the algorithm secure, but it turns out that is not the case. If your algorithm is to be used in a commercial product, it doesn't take long for it to be reverse-engineered. Someone buys the product, runs sample texts through it, and figures out what your algorithm does. Security through obscurity seldom works, particularly in commercial products: Software vendors had their copy-protection schemes defeated almost immediately after they introduced them; cable operators lost revenues when their inadequate encryption was broken and illegal cable boxes were widely distributed; early cordless telephone security features were trivially easy to defeat.

More recently, cryptographers have made their algorithms public either by publishing them in academic journals or by patenting them; in either case, one objective is to subject them to trials by fire. Mathematicians earn bragging rights, among other things, for breaking algorithms that were thought to be secure; getting credit for creating a strong encryption scheme

is a major incentive for publishing. Algorithms that can withstand direct attacks are much stronger (and more elegant) than those which fall apart as soon as you know how they work. As indicated earlier, the less you have to keep secret, the easier it is to maintain security.

DISTRIBUTING KEYS AND KEEPING THEM SECRET

Up to now we have been considering secret key algorithms: If you have the key, you can read any encrypted messages. One major weakness with this approach is that you need to have a dependable way to pass keys around to the people who need them. You have to treat the key with at least as much care as you do the messages; losing a single message may be harmful, but losing the key means losing all messages. Another weakness is that if you want to send a secure message to a group, you've either got to rely on everyone involved keeping a single key secure among them, or you've got to assign a separate key to each individual and use it for all communications.

While the simplest answer is to hand-deliver all keys, and have a single key for each pair of people who want to exchange secure messages, it soon becomes clear that this solution doesn't scale up well at all. You and I can communicate securely with a single key; add my brother to the mix, and I need one key to talk to him, one to talk to you. You need another key to talk to him; each of us now has two keys, and there are three keys in all. Adding new participants in our little secret circle adds more keys; if we were running a company and wanted to assign secret keys to our customers, we'd soon be in the business of assigning and distributing keys.

Many Internet commerce systems require that you be able to securely exchange messages with anyone, whether you know that person or not. Private key solutions are available, but by and large they require some degree of trust either in the parties

exchanging messages, or else in some intermediary agency with access to both parties' secret keys. As it happens, public key cryptographic techniques make this unnecessary.

The Public Key Solution

To simplify our discussions of cryptographic methods, rather than attempt to explain how the functions actually work we will instead imagine each function as if it were a black box that processes data. Data is dropped into a hopper at the top of the box for processing (input), and the resulting data (output) flows out of a spout at the side. An encryption function works by having *plaintext,* or unencrypted data, dumped in the top of the symmetric encryption box. The output comes out the spout as *ciphertext,* or encrypted data.

Traditional encryption methods rely on what are known as *symmetric functions*. These functions are called symmetric because they work the same way in both directions. You can run plaintext through the function to create ciphertext, and then take that ciphertext and run it through exactly the same function to turn it back into plaintext.

A *key* is required for this type of cryptographic function. The key to a symmetric cryptographic function is a piece of data that can be used to encrypt or decrypt data. Symmetric cryptographic functions use the same key to encrypt and to decrypt data: if you have the key, you can turn plaintext into ciphertext, or you can turn ciphertext into plaintext. This means that all senders and all recipients need to have the same key in order to communicate securely.

This type of cryptography is sometimes called private key encryption, because the keys must be kept private. If you lose the key, or if someone figures out your key, you must redistribute a

new key (as well as try to figure out how many of your transmissions have been compromised).

Public key cryptography relies on certain mathematical properties of large numbers that make possible one-way, or *asymmetric* functions. These functions use pairs of keys (key_A, key_B) instead of single keys to encrypt or decrypt data. Data that has been encrypted with one key can only be decrypted with the other key of the pair. Using the black box analogy, plaintext that is fed into a hopper to be encrypted with key_A comes out the spout as ciphertext. However, this ciphertext cannot be decrypted by dumping it back in the top of the key_A hopper — it must be processed using key_B to return it to plaintext again.

The pair of keys consists of a public key, which the owner distributes to anyone who asks for it and which can be made public, and a secret key, which the owner protects and gives to no one else.

Public Key Implications

Once you are able to create pairs of complementary keys, you can expand the function of your cryptographic technology. The most obvious enhanced function is encryption. You no longer need to be as concerned about secure key distribution, and you now have the ability to encrypt data to be sent to someone you do not necessarily know (or have any prior contact with). If you wanted to send me an encrypted message, you would get my public key and use it to encrypt your message. The resulting ciphertext can only be decrypted with my secret key, so only I should be able to read the contents of the message.

This is how it is possible to create an encrypted channel between a person using a secure Web browser and a secure

Web server. The Web server sends the public key linked to the merchant running the server to the secure browser. The browser then uses that public key to encrypt commercial transaction information for transmission to the server.

However, there are further implications to public key cryptography that are even more important for Internet commerce. Encrypting information is important to protect it, but it is also important for consumers to be able to verify that data sent from a merchant is accurate, or for merchants to be able to verify that transaction authorizations are valid. This is made possible by using a secret key to encrypt a message — anyone with the public key can then decrypt the message, and confirm that it was actually encrypted by the entity associated with that public key.

This is the underlying approach to digital signatures. Rather than encrypting the entire message, the message is scanned and digitally summarized (hashed). The result is a virtually unique sequence of numbers that represent the contents of the message — something like a check digit used to confirm the validity of a credit card number, but much more accurate and dependable. This hash is then encrypted using the sender's private key, and the result is appended to the message being signed. Any recipient can then find the sender's public key and decrypt the hash using that key. By performing the same hash function on the message themselves and then comparing their results with the decrypted digital signature, recipients can authenticate the message as having come from the owner of the public key.

If the decrypted hash doesn't match the hash done by the recipient on the message received, the message should not be trusted. There may have been an error in transmission, or the message may have been intercepted and modified by a malefactor. In

either case, though, the message cannot be certified to be the exact message that was sent. Nor can it be certified as having originated with the owner of the public key.

However, if the digital signature can be verified for a message, it means the recipient can be certain that the message has not been modified in transit, and that the message was indeed sent by the owner of the public key.

Key Distribution and Certification

The preceding discussion about private and public key cryptography has avoided the issue of how to manage key distribution. As with all the other aspects of cryptography, there are well-known problems pertaining to secure and reliable key distribution. To illustrate, a simple scenario:

- Bob and Alice are two acquaintances who communicate by e-mail on occasion.
- Evil Emily, impersonating Bob, sends a forged piece of e-mail to Alice, requesting a secure communication channel using public key encryption.
- Included in this forged message is Evil Emily's public key (which she represents as Bob's public key).
- Alice receives the message and encrypts a reply using what she believes to be Bob's public key (but which is actually Evil Emily's public key).
- Evil Emily receives the message, decrypts it with her own secret key, and is able to communicate with Alice while pretending to be Bob.

Of course, this scenario can be defeated through an efficient and reliable key distribution system.

Trusted Key Distribution and Verification

With the wider application of public key cryptography for the purpose of commerce, mechanisms for the trusted publication and distribution of public keys are necessary. Simply having a merchant (or customer) send a copy of a public key will not do, since a forger could sent her own public key while pretending to be someone else.

One solution is for some (respected) organization to offer key publishing services. Those who wish to can report their keys and their identities, and anyone else can find a key by looking for a person's name. To add further trust, people can have other people certify their public keys. In other words, one person (or organization) can vouch for another one by adding their own name and public key to the listing. The greater the resulting "pedigree" to your public key, the greater amount of trust others can put in your digital signature.

At the moment, however, the issue of certification authorities is still being decided by Internet standards organizations as well as by the Internet market. The problem is that anyone can generate a valid public key pair. If a criminal could cause merchants to believe that the criminal's public key was the right one to use when communicating with a bank or other Internet commerce vendor, the result would be that the merchants' encrypted transaction data could only be decrypted by the criminal.

One approach is to use a web of trust, where you exchange your public key with people directly, or get copies of public keys from other individuals who you trust are cautious enough to collect only valid keys. Another approach is to use a public, and well-trusted, forum to publish public keys. For instance, some books and articles about public key

cryptography include public keys used to digitally sign security software distributions.

CRYPTOGRAPHIC APPLICATIONS

As may already be obvious, cryptography, and public key cryptography in particular, plays a vital role in making online commerce a secure option. As has already been discussed, encryption can be used to hide sensitive data from eavesdroppers; digital signatures help to add reliability to messages sent across unreliable networks.

Encryption

Requiring the use of a key to "unlock" data is called encryption. The key can be a secret key, used symmetrically, or it can be one of a public key pair, used asymmetrically. The longer the key, the less likely it is that a brute-force attack on the encrypted data will be successful (assuming that the encryption algorithm is not susceptible to other types of attack).

Public key pairs include a private key and a public key. When sending a public-key encrypted message, the sender encrypts the message with the recipient's public key. The resulting message can now only be decrypted using the recipient's private key.

In practice, public key cryptography is very secure but very costly in terms of computer resources. As a result, it is often combined with secret key cryptography. For example, a sender can use public key encryption to encrypt a secret key to be used for bulk encryption purposes. Both participants could use a single secret key, or they could use a single key to generate

some other set of keys to use for their communication. The exchange of the secret key uses the very secure public key encryption, while the bulk encryption of the remainder of the communication would use some other encryption method.

An eavesdropper could capture the encrypted communication, and thereby attempt to break the encryption. However, with very long secret keys that are used only for one communication session and not reused, this method can be made quite secure.

Digital Signature

If the sender encrypted data using the sender's own private key, the resulting message could be decrypted by anyone who had the sender's public key. This process can't be considered a way to protect the message from anyone, since anyone with access to the sender's public key can decrypt it. However, it does offer a method of signing a document digitally.

Encrypting a message in this way will assure that it can only have come from the person whose public key will decrypt it. However, it also assures that every such message must be decrypted. As has been mentioned, since public key encryption uses lots of resources, this becomes impractical. Also, there is the problem of keeping track of and certifying public keys.

A better option for digital signatures is to use a digest function to summarize the contents of a particular message in a smaller, more manageable chunk of data. This chunk can then be encrypted using the sender's private key, and appended to the message. The recipient can then use the same digest function on the received message and use the sender's public key to decrypt the digest included by the

sender. If the two digest results match, then the message has been certified as signed. If the results don't match, then the message cannot be certified as signed.

Nonrepudiation and Message Integrity

There are two by-products of the use of digital signatures. Nonrepudiation is a cryptographic term describing the situation when the originator of a message cannot deny having sent it. Normal electronic mail is deniable, since it is (relatively) easily forged and easily modified. Electronic mail that has been digitally signed, however, is non-repudiable. If the digital signature checks out properly, the owner of the signature is the only entity capable of having signed the message.

The other important by-product of digital signatures is a guarantee of message integrity. If a message has been digitally signed and transmitted, verifying the signature also verifies that the message has been received unchanged from the source. A signed message that has been intercepted, modified, and forwarded on to its original destination will not produce a verified signature.

The ability to verify a digital signature also confirms that the signed message was delivered intact and unchanged. Furthermore, the person signing the message cannot later deny having sent it.

The existence of an accepted public key standard will mean consumers can require that their merchants send them nonrepudiable messages containing offering prices on certain products. This assures the consumers that the merchant cannot later deny the deal that was cut. The merchant, too, can ask for a

nonrepudiable purchase request from the consumer, so that later the consumer cannot deny having made the purchase.

For now, however, digital signatures can be used by Internet commerce services to verify transactions. For example, the First Virtual security-requirements option results in digitally signed transaction approvals sent by First Virtual to merchants. This level of authorization is necessary for selling hard goods, so vendors can confidently ship them.

CHAPTER THREE

SECURING INTERNET COMMERCE

Contents

THE INTERNET COMMERCE STORY, SO FAR 66
Five Internet Commerce Techniques 66
Security through Obscurity 66
Consumer/Merchant Channel Encryption 67
Digital Envelope Encryption 68
Digital Currencies 69
Offline Handling of Transaction Data 69
Representative Internet Commerce Players 70
Other Internet Commerce Actors 72

TRANSACTION SECURITY THROUGH OBSCURITY 73
The "No Security" Choice 73
Choosing No Security 74
Incomplete Security Solutions 75
Marks of Unsecure Solutions 76

THE ENCRYPTED CHANNEL APPROACH 77
How an Encrypted Channel Works 78
Advantages for Merchants 81
Advantages for Consumers 82
Weaknesses and Disadvantages 82

THE DIGITAL ENVELOPE APPROACH 83
How Digital Envelopes Work 85
Advantages for Merchants 85
Advantages for Consumers 86
Weaknesses and Disadvantages 86

DIGITAL CURRENCIES 87
How Digital Cash Works 88
Advantages for Merchants 89
Advantages for Consumers 89
Weaknesses and Disadvantages 89

EXTERNAL CHANNEL APPROACH 90
How the External Channel Approach Works 91
Advantages for Merchants 92
Advantages for Consumers 93
Weaknesses and Disadvantages 94

Summary This chapter explains the various approaches that companies and individuals have been taking to the problems of transacting exchanges over open networks like the Internet. In particular, it outlines the currently predominating techniques, secure channel between browser and server, end-to-end encryption using "digital envelopes," and keeping sensitive data offline entirely.

THE INTERNET COMMERCE STORY, SO FAR

Keeping in mind that Internet commerce is very likely to evolve considerably over the coming years, it is still useful to consider some of what has gone before. This section provides an overview to the five techniques that, so far, have predominated in Internet transactions. Also profiled here are the companies and organizations that are exerting significant influence over Internet commerce. Later sections of this chapter explain in more detail how these techniques work, and how the First Virtual system fits into the whole picture.

Five Internet Commerce Techniques

So far, it seems that most approaches to Internet commerce can fit into five categories:

- Security through obscurity (or no security)
- Consumer/merchant channel encryption
- Digital envelope encryption
- Digital currencies
- Offline handling of sensitive transaction data

Each of these approaches is summarized here and discussed in more detail later in the chapter.

SECURITY THROUGH OBSCURITY

This is the easiest, and least satisfactory, approach to doing business on the Internet. This approach may mean simply assuming that nobody is listening to your transmissions, and just sending credit card numbers in the clear — or it may mean using untested or unknown security techniques for keeping payment information secret.

Despite the lack of any well-publicized losses due to unencrypted credit card transmissions (and the relative frequency of such transmissions), it is still not a good idea to assume that sending credit card numbers unencrypted is safe. While consumers may send their credit card numbers in the clear with relative safety (their liability is limited if the card numbers are stolen), it is hardly acceptable for a merchant to encourage customers to do so.

If you have created your own codes or security routines, they are likely to have significant flaws and vulnerabilities — unless you are a professional cryptographer who has consulted other professional cryptographers while creating your security scheme. The general consensus of Internet commerce experts is that any scheme for transmitting data securely across an open network like the Internet should be submitted to public peer review. Their position is that any scheme that cannot be revealed without compromising security is not sufficiently strong to rely upon. After all, someone on the outside will eventually figure the secret out, or someone on the inside will reveal the secret.

It should be noted that even cryptographic technologies that have been developed with public peer reviews and extensive testing are also vulnerable to algorithm or implementation flaws. However, peer reviews help to detect most of the obvious flaws, and algorithms that are well known can also be presumed to be reasonably better tested than those which are kept secret.

CONSUMER/MERCHANT CHANNEL ENCRYPTION

This is the simplest way to permit direct Internet transactions between a consumer with a credit card and a merchant. There is no need to create a separate relationship, or to use any special accounts created through a third-party

Internet commerce payment system. Using the public and private key cryptographic techniques discussed in Chapter 2, the customer encrypts credit card and other transaction information that only the merchant receiving the order can decrypt.

This is the type of transaction supported by secure Web browsers and servers. It balances strengths — a wide availability of servers and browsers, and no need for additional parties to complete transactions — with some weaknesses — it may be vulnerable to cryptographic and other types of attack, and it requires a level of trust in merchants receiving credit card numbers.

DIGITAL ENVELOPE ENCRYPTION

A more comprehensive approach to Internet commerce is to involve at least one other party in the process of taking credit card payments online: the company that approves and settles the transactions. A "digital envelope" can be created that contains sensitive transaction information encrypted and sent from the consumer to the merchant, but that the merchant cannot decrypt. The consumer's software encrypts the sensitive information using the public key of the entity that will authorize the credit transaction, so that only that entity can decrypt the information. This is forwarded to the transaction "acquirer," which approves or denies the transaction in real time, in the same way credit card transactions are handled in real-world stores.

This approach removes the possibility that a merchant (or someone working for the merchant) might intercept credit card numbers improperly, but it also adds the requirement that consumers establish a "digital wallet" prior to any transactions. Finally, though it is considered less vulnerable to crypto-

graphic attacks, there is still the potential that someone may find a flaw in its algorithms or implementation.

DIGITAL CURRENCIES

Differentiated from payment systems by anonymity and direct backing by actual cash, digital cash is being implemented more slowly than payment systems. Digital cash is made possible by using cryptographic techniques to produce strings of data that can represent cash without linking that cash to any specific entity or person.

Financial institutions so far have been taking a very cautious approach to offering such products, perhaps in part because it is not clear how regulatory bodies will respond. After all, creating and distributing digital cash is tantamount to creating and distributing a new type of currency — a right that governments prefer to reserve to themselves. Anonymous digital currency would seem to leave open many opportunities for money laundering, tax evasion, and other currency infractions, such as removing large sums across international borders.

Finally, digital cash depends upon the same family of cryptographic tools used by other, non-anonymous payment systems, and thus are also potentially vulnerable to undetected algorithm or implementation flaws.

OFFLINE HANDLING OF TRANSACTION DATA

Encryption is expensive: it takes a lot of work to implement, it may require licensing software tools to program with patented algorithms, it takes extra computing cycles. Even so, if data of sufficient value is being transmitted over public networks, then someone can be counted upon to attempt to steal that data. Given these facts, some companies have chosen to provide

Internet commerce services that use alternative methods for transmitting sensitive payment data.

First Virtual is the most prominent company that uses no encryption to transmit transaction information and transmits no sensitive information over the Internet. When creating a new account, consumers must call a special telephone number and key their credit card number directly into a computerized system — a system that is not connected to the Internet.

While First Virtual avoids relying on encryption to secure the transaction process, they do use digital signatures on transaction verifications. The distinction is important, as the transactions themselves are still transmitted in the clear — addition of digital signatures to authorizations makes it possible to buy and sell hard goods, where there is a real cost attached to delivering goods that are not paid for. What is important to remember is that at no time is any sensitive information ever transmitted across the Internet. Even if someone were to intercept the transmission, they could not gain unauthorized access to the payment method being used (e.g., credit card account used to pay for a product).

Representative Internet Commerce Players

To better understand the approaches to Internet commerce, it helps to have specific examples — well-known (or relatively well-known) instances of those approaches. Using the five different approaches to Internet commerce discussed throughout this chapter, we can consider five different companies that have pioneered Internet commerce.

We will not discuss any specific company using a "security through obscurity" approach. This would be unfair to firms that began by attempting to create a secret and secure set of

algorithms and protocols, and later made them public. It would also be putting at risk the customers of those companies that do not implement any security functions at all. It should suffice to say that as of the start of 1996, some companies offering goods for sale through their Web sites would still accept your credit card number via unencrypted e-mail or unsecure Web connections.

Netscape Communications has succeeded so far in large part because they created a pair of applications supporting a secure transmission channel: the secure Web browser and the secure Web server. The browser is able to encrypt data being sent to a secure server, which is able to decrypt that data. The result is that the transaction data is not likely to be intercepted and decrypted by someone other than the intended recipient.

CyberCash, Inc., uses a form of the "digital envelope" to bring together encryption and digital signatures in a form that allows the consumer to make a purchase with a credit card number that can only be decrypted by the institution that authorizes the transaction. The distinction is important because it eliminates handling of the actual credit card numbers by the merchant — where there is significant risk of loss through outsider and insider crime. This is the approach being pursued by Visa and MasterCard, and is being implemented by Netscape in their Navigator browser during 1996.

Digital cash, called "ecash," has been developed by DigiCash bv, and was first implemented in the United States in late 1995 by the Mark Twain Bank in St. Louis. In this early incarnation, ecash accounts are relatively complicated to initiate, and are also relatively expensive: transferring cash can cost between 2% and 5% of the value transferred, and on top of that there are monthly fees that can be as high as $25 and setup fees that can be as high as $300 for commercial accounts. Given these costs, even early implementers have been cautiously signing on.

Ecash advantages include a high degree of anonymity in transactions, while some of the disadvantages are similar to the disadvantages of cash itself: you have considerably less recourse if you want to dispute a transaction. However, unlike real cash, if you lose or destroy your ecash (for example, through a hard disk crash), it may be possible to recover that loss.

Arguably the most secure, though not the most anonymous, method of doing Internet commerce is to take a procedural approach to the process and keep sensitive information offline. Though First Virtual is, so far, the most successful implementer of this approach, other companies have taken it as well. Open Market, Inc., has taken a dual-pronged approach to Internet commerce by offering secure servers as well as a more complete commerce solution that requires consumers to set up an account prior to making any purchases. While Open Market has been shipping secure servers since 1995, their commerce environment solution is not expected to be implemented (by a separate company acting as an Internet commerce provider) until sometime later in 1996.

As we will see, the procedural approach developed by First Virtual is designed to be robustly secure — meaning that security is sufficiently high to protect all participants with no single catastrophic point of failure. Because there are enough different protections against fraud built into the system, First Virtual is able to completely outline the steps that must be taken to complete a fraudulent transaction.

Other Internet Commerce Actors

The companies just mentioned are almost entirely concerned with Internet commerce; other existing companies and organizations will exert considerable influence over the course of

Internet commerce. Some of these major players include Microsoft, Visa International, and MasterCard International, not to mention organizations such as IBM, AT&T, and many others that are looking to the Internet as a new source of income.

TRANSACTION SECURITY THROUGH OBSCURITY

Don't expect companies involved in Internet commerce to give away their system security plans and firewall architectures: these are the tools they use to protect their systems against intruders. These tools protect the companies' own systems and internal processes. For example, the First Virtual computer systems that handle account payment information (credit card numbers and checking account information) do not maintain Internet links, and First Virtual will not provide you any more information about how access is provided to these systems.

On the other hand, the commerce transaction protocols for First Virtual are well documented in protocol specifications. This is because the contents of these transactions are readily available to anyone who is capable of eavesdropping on Internet transmissions. There is no way to keep the protocols secret, so there is no reason to try.

The "No Security" Choice

Because no transaction transmitted over the Internet can be guaranteed to be inviolable from interception, it is in the interest of commerce providers to make their protocols public for two reasons:

- It demonstrates to consumers and merchants that the provider believes its procedures to be sufficiently robust that they can withstand attempts by criminals with easy access to those protocols.
- It makes it easier for academicians and others with interest in Internet commerce to study the protocols and make suggestions and comments about the level of security possible using them.

However, properly implementing security through technologies such as encryption can be very difficult and expensive. Making errors in the implementation of a well-known encryption algorithm can render the implementation vulnerable. Vendors who attempt to create their own encryption algorithms may not have the facilities to do a good enough job. Making the protocols public can pose an image problem for vendors of home-grown solutions, since it may expose big security holes and embarrass those responsible.

The general consensus among Internet commerce experts, however, is that you cannot trust an encryption scheme that relies on secret and proprietary technologies. Although it may be possible to keep the protocol specifications from leaking from the company, it is not possible to keep interested parties from monitoring transactions and reverse-engineering the information exchange protocols.

Choosing No Security

There are companies offering goods for sale on their Web sites that are willing to accept your credit card number sent in the clear in a Web page form or in an e-mail message. As reliable and secure Internet commerce technologies are deployed more

widely, the numbers of these companies will continue to dwindle. They are operating on the assumption that no one is monitoring traffic arriving at their servers from the Internet, screening it for credit card numbers.

Despite several years of heated warnings against transmitting credit card numbers in the clear over the Internet, there are remarkably few documented or publicized instances of Internet-sniffing credit card thefts. There are still those who insist that sending credit card numbers over the Internet is less likely to result in a theft than using a credit card in person and generating a carbon copy that can be stolen from a garbage can or Dumpster. But the Internet is built on protocols that are unreliable and unsecure, and it is far from safe to assume that someone is not sniffing some section of the Internet over which your transmissions are carried. If enough people send their credit card numbers in the clear, thieves will undoubtedly start monitoring the Internet for them.

Incomplete Security Solutions

An incomplete or poorly implemented security solution is worse than no security solution: the existence of any measure, no matter how small, is often enough to lull users into a false sense of security. For example, the use of passwords is often instituted as a first line of defense against intruders. However for passwords to be effective, they must also be very difficult to use: they should not be easily guessed words or numbers, should be changed regularly, should not be the same as passwords to other systems, and should be checked regularly by system administrators for strength. Passwords therefore present a tantalizing weakness to criminals who would like to break into systems. They are commonly exploited to just that end, exposing all the data on the system.

Even so, users who depend on passwords to protect their data and systems would be much more careful about what information they put on a system that had no passwords and was open to anyone.

Operating systems vendors routinely issue patches, fixes, and warnings about security vulnerabilities in their offerings, and network applications are notorious for offering criminals the tools to break into systems. Network software vendors, too, have to be careful about their security implementations. For instance, Netscape implements in their Navigator software a secure channel for transmitting encrypted credit card numbers across the Internet — but in an early version, this software used a random number generator to seed the encryption process that was not sufficiently random to keep the encrypted data secure. Though a fix was produced and distributed almost immediately after the flaw was discovered, the moral of the story was that even large vendors can make errors in security implementations and that it is not a good idea to rely implicitly on the security of any particular implementation — especially if it has not been subjected to peer review.

Marks of Unsecure Solutions

When choosing a method for Internet commerce, it is helpful to examine how the commerce provider transmits transaction information, and what measures the provider deploys to keep the commerce secure. One should always beware of vendors who ask customers to trust them that their technology is safe and secure; this is especially so in Internet commerce, where in the worst case it is conceivable that a criminal could defeat the security in a way that can be automated over a wide area and/or a long period of time.

Thus, if you want to be able to trust a security implementation, particularly one that relies on encryption, you should opt for one that has been scrutinized by the widest possible audience. And since any Internet commerce system can be reverse-engineered to some extent by monitoring transmissions, you should avoid any commerce provider that does not offer its own users documentation on what data is transmitted, where it is transmitted, and how transaction security is maintained during transmission across the Internet.

THE ENCRYPTED CHANNEL APPROACH

Its seems that the use of codes and ciphers is a natural way to attempt to communicate sensitive material in a public medium. This can be as simple as a parent spelling out the word "cookie" while a toddler listens in to a conversation, or the use of pig Latin to mask meaning from those not in the know. One computer equivalent of pig Latin is the use of ROT-13, or shifting the ASCII representation of a block of text, thus rendering normal text meaningless to the casual observer (but easily returned to meaning by applying ROT-13 again).

Internet commerce, by definition, requires that information be passed between parties connected across the Internet. This information thus becomes vulnerable to interception, causing commerce providers to turn to encryption methods to keep the transaction data secure. The earliest attempts to define a secure way to transmit data via the World Wide Web was an extension to the Hypertext Transport Protocol (HTTP), called Secure HTTP (S-HTTP). In 1995, Netscape leapfrogged the open standards process working on S-HTTP by creating and implementing their own protocol, Secure Sockets Layer (SSL), in

their Navigator Web browser and Commerce Server software products. As Netscape built their market presence on their ability to offer an encrypted channel between server and browser, they submitted SSL to the Internet Engineering Task Force as a proposed standard.

Because Internet users do not, as a rule, respond well to companies attempting to deploy proprietary applications, any Internet commerce protocol must be an open one. Open standards let anyone write software for any hardware platform or operating system, and open standards intended to keep transmissions private are no exception. In 1995, many of the companies participating in the development of S-HTTP were releasing secure Web servers capable of transmitting encrypted data to and from secure Web browsers — but only Web browsers supporting S-HTTP. Meanwhile, Netscape was literally giving away evaluation copies of their secure (SSL) Web browser — none of which supported S-HTTP. The next wave of browser and server upgrades supported SSL as well as S-HTTP.

To many consumers and merchants, Internet commerce means the ability to recreate the typical credit card order online. To these people, commerce can only be reproduced by taking the same information that passes between the consumer and the merchant in a physical store (or in a telephone call or through mail-order) and encrypting it so that no one but the merchant can decrypt it.

How an Encrypted Channel Works

When a consumer uses a Web browser to get information from a merchant's Web server, the process uses the underlying Internet protocols (TCP/IP) to negotiate a connection between

the server and the browser. The browser requests specific information (as defined by URLs) and the server responds by sending that information.

When some of the information to be transmitted between the server and the browser is denoted as sensitive — for example, when the merchant wants the consumer to transmit a credit card number — a slightly different URL scheme is used. Most World Wide Web hypertext URLs are denoted in the form:

```
http://www.loshin.com/index.html
```

The URL scheme is the first part of the URL. It refers to the type of protocol to use when retrieving the resource. This scheme is typically `http:`, though other common schemes include `ftp:` for File Transfer Protocol resources, and `gopher:` for Gopher resources. When the scheme is `https:` (for SSL) or `shttp:` (for S-HTTP), the browser and the server go through a negotiation process before the resource can be sent.

The first thing that might happen is nothing: if the browser does not support the encryption protocol defined by the URL, it will simply not be able to retrieve the resource and will return a status message. If the browser supports the specified protocol, however, it begins a further negotiation with the server to determine how to proceed.

The SSL and S-HTTP protocol standards specify how the negotiation proceeds. These protocols are explained in greater detail in my book *Electronic Commerce: On-Line Ordering and Digital Money* (Charles River Media, 1996), but in a nutshell the process involves the server sending the merchant's public (asymmetric) key to the browser. The browser generates

a private (symmetric) key to be used just for that session between that browser and server pair, encrypts it using the merchant's public key, and sends it off to the server. The rest of the transaction is encrypted using the session key, which is discarded after the session.

The resulting encrypted data stream between the browser and the server is often referred to as a secure channel because it is encrypted, generally with the strongest encryption supported by both participants. Ultimately, however, the security of the channel depends on several factors relating to how strongly the protocols were implemented on server and browser, how likely it is that the underlying encryption algorithms can be broken, and how important it is to someone other than the intended recipient to decrypt the data being transmitted. For example, the export-strength version of the Netscape Navigator browser supports only 40-bit keys. Data encrypted with 40-bit keys can be "brute-forced" by individuals or groups with relatively modest hardware resources, dedicating those resources anywhere from days to weeks. This actually should be sufficient for many commerce applications, as long as the amount of time and effort required to crack a single credit card is greater than the value of the card.

If you wanted to use the 128-bit key version of Navigator, you can be reasonably sure that your credit card cannot be acquired by brute-force attempts against your transmissions — but other attempts are certainly possible. Finally, if you were planning to routinely transmit more valuable information (the formula for Coca-Cola, or the combination to your bank's safe, for instance), you would be well advised to consider some other means in addition to encryption to supplement your security measures.

Advantages for Merchants

As of 1995, there were significant advantages for merchants using the secure channel approach to Internet commerce — though by 1997 many of those advantages are likely to evaporate (see the later section on digital envelopes). The biggest draw for merchants is the size of the potential market. With estimates for the number of people browsing the Web ranging from the millions to the tens of millions, the number of users capable of making purchases using an encrypted channel is huge. One recent study suggested that 18 million people connected to the World Wide Web in the latter part of 1995; that means at least 12 or 13 million users with SSL browsers, assuming 70% used a Netscape browser (based on market share claims from Netscape). This number is likely to be higher, since vendors other than Netscape continue to add support for SSL to their own browser software.

Another advantage for the merchant is that the potential Internet consumer does not need to do anything to become an Internet consumer, as long as he or she is using a browser supporting SSL. There is no extra step of acquiring special support software, or even of setting up an account of any kind — the user just enters a credit card number and shipping information into the Web page forms to make a purchase.

Finally, one dubious advantage: the merchant retains control over a process that is very much like the traditional mail-order or telemarketing model, where credit card numbers are taken by the merchant and sent off to another company to be processed. The actual processing of credit card orders can be done manually, or it can be automated through additional software and services.

Advantages for Consumers

As already mentioned, once the consumer has the secure Web browser installed, there is nothing else to do but locate a product or service and enter payment information into the merchant's Web page forms. There is no other software to acquire, install, or configure, and there are no accounts to set up before a purchase can be made.

Weaknesses and Disadvantages

When you rely on a single method for all the security in a transaction, in this case encryption, you risk losing all your security in the event that your method can be defeated. As has been discussed elsewhere, a flawed implementation can result in this type of defeat. In theory, encryption can also be ultimately defeated through the future discovery of weaknesses in the algorithm, or through the application of a sufficiently large computer or aggregation of computers. In any case, the way that public keys are managed will also have some bearing on how secure public key encryption will be: if a merchant doing a large volume of sales does not change public keys regularly, there is a risk that criminals may, over a long period of time, successfully acquire the secret key of that public key pair.

Public key encryption algorithms have been scrutinized for flaws by computer scientists and others for close to twenty years, so fears about algorithmic weaknesses are mostly theoretical (though implementation flaws are much more likely). A much more worrisome problem is that of the security of credit card numbers once they have been received by the merchant. If the merchant stores decrypted credit-card and transaction information on a computer that is connected to the Internet, there is a significant risk that criminals will attempt to steal

that information. This is clearly a much simpler matter than trying to crack a strong encryption algorithm, and criminals have been known to accomplish it.

There are other, less problematic disadvantages to the secure channel. One is that consumers must re-enter all of their payment information every time they make a purchase. Another is that an underlying application program, in this case a World Wide Web browser, is a minimum requirement for consumers who want to make purchases over the Internet. Merchants, too, must have the facilities set up to accept credit card payments, which acts as a barrier to entrepreneurs who are starting up new operations. Finally, there is no way to manage Internet transactions — there are no standard audit trails or digital receipts or applications to keep track of your on-line expenditures.

THE DIGITAL ENVELOPE APPROACH

Assuming that a suitable encryption technology can be implemented, the biggest potential drawback to an encrypted channel for Internet commerce is the handling and storage of the payment information by the merchant. There are too many ways for that sensitive information to be jeopardized:

- The merchant's server could be compromised by a criminal attacking it over the Internet and stealing credit card numbers.
- A dishonest employee could compromise the merchant's system and steal credit cards.
- A dishonest merchant could process the transactions and never deliver merchandise ordered.

- The server could be compromised physically, by a criminal breaking into the merchant site and stealing payment data stored on the system.

The weakest link in the secure channel is the merchant; take the merchant out of the loop, and you reduce the vulnerability of the resulting Internet commerce system. This is what the digital envelope approach does. Instead of letting the merchant and the consumer negotiate an encrypted communication channel, the sensitive credit card information is encrypted and sent directly to the organization that will approve and perhaps settle the credit card transaction (called the acquirer). The merchant can initiate the transaction process, but the credit card information itself is accessible only by the acquirer — the merchant need never handle it.

The consumer uses software that encrypts sensitive payment information using the acquirer's public key, so only that entity should be able to decrypt the credit card number. The merchant acts as an intermediary in this part of the transaction, forwarding the request in its "digital envelope" to the acquirer, and waiting for a transaction approval from the acquirer before shipping the merchandise being ordered.

The first protocol for this type of commerce was developed and implemented by CyberCash, Inc., in 1995. Netscape produced their own version of a digital envelope protocol, also in 1995, but did not implement it in their Navigator browser until 1996. The credit card associations Visa International and MasterCard International, in conjunction with several other companies including Microsoft, IBM, Netscape, and CyberCash, have also moved to this type of protocol for Internet commerce. At the start of 1996, it is still not entirely clear in which direction the various players will move, but it is clear that they will ultimately support some standard digital envelope protocol.

How Digital Envelopes Work

In 1995, CyberCash, Inc. deployed a "digital wallet" software application for consumers to install on their systems. When a transaction is initiated through a Web page, the merchant's server (which runs special software to enable this type of commerce) sends a request to the consumer's browser, which opens the digital wallet application. The two programs negotiate the payment using a credit or charge card that has been configured by the consumer in the wallet. The wallet encrypts the transaction information using the acquirer's public key, then sends it on to the merchant, which forwards it to an acquirer organization to approve or deny credit. Once the result is returned to the merchant, the transaction can be completed. The entire process may take only ten or fifteen seconds in all, from start to finish.

Because this type of system is specifically intended only for commercial transactions, the United States government has approved its export with the same size key as is used in the United States: 768 bits. This is unlike the encrypted channels designed to allow unrestricted communications between any two parties, as implemented in Netscape browser and servers, for example, which are produced in two flavors: stronger, for United States use, and less strong, for export.

Advantages for Merchants

Using the digital envelope approach answers the biggest security problem for merchants, that of keeping credit card numbers secure. It means the merchant does not have to worry about how the transactions are to be processed. Also, it uses a very strong type of encryption to protect credit card numbers in transit across the Internet. Another big plus is that the

credit card associations, credit card issuers, and banks all seem to be backing this type of approach, at least from a security standpoint.

Advantages for Consumers

Once the digital wallet software has been installed and configured, most consumers will find that the process of making a purchase is very simple. Since credit card information is loaded directly from the digital wallet software, the consumer does not need to re-enter all that information every purchase. The digital wallet also includes helpful auditing features that allow the consumer to keep track of purchases made with it.

The wallet software available from CyberCash, for example, will work with just about any Web browser, and Netscape has announced plans to include a wallet in versions of its Navigator browser to be released early in 1996.

Weaknesses and Disadvantages

As with any commerce method relying on encryption as its primary means of security, the digital envelope approach is potentially vulnerable to any as yet undiscovered flaw in algorithm or implementation. A more practical consideration for merchants as well as consumers is that it requires additional software for all concerned. As of the start of 1996, there are still relatively few merchants equipped to accept CyberCash-based payments (the CyberCash client has been licensed to CompuServe as well as to Checkfree Corporation). This situation should change rapidly during 1996, however, as more vendors include the consumer software in their network applications and as more merchants become enabled.

For a merchant, the process of setting up to accept CyberCash payments can be somewhat of an obstacle, particularly with startup companies. The merchant must have a merchant banking account with a CyberCash-affiliated bank, and must install special software on the merchant's Web server.

DIGITAL CURRENCIES

As with so many other Internet commerce technologies, digital currencies are possible only through the use of cryptography. At the start of 1996, there is one provider of digital currency systems, DigiCash bv, that has actually placed its ecash(system in operation. The Mark Twain Bank, of St. Louis, has implemented ecash for general use. DigiCash ecash relies on digital coins that can be passed between any two entities to exchange value, with an intermediary bank offering clearing services to prevent coins from being spent more than once. The coins incorporate digital signatures, with a special twist to add payer anonymity, that make it possible to certify that a particular string of data actually represents some monetary value. The resulting digital currency is handy for exchanges where the payer prefers to be anonymous, though it makes more sense for expenditures on soft goods than for hard goods that may require delivery information.

So far, digital cash is not being implemented as rapidly as other forms of digital payments. For one thing, it is not clear exactly how or whether a digital currency issuer would be able to make a profit on the enterprise. The client and merchant software for DigiCash ecash has so far been distributed at no cost, while DigiCash sells the "mint" software (which creates and validates the digital coins) to banks. As a result, an issuing bank apparently needs to charge some combination

of setup fee, monthly charge, and percent of the value of exchanges.

Perhaps of more concern to potential digital currency issuers is the issue of government regulation. At the very least, some governments would not approve of losing their monopolies on issuing legal tender. Furthermore, there are problems relating to collection of taxes and regulation of currency import and export. There is sufficient fear, uncertainty, and doubt to keep the largest banks from participating in this activity, at least so far.

How Digital Cash Works

Generating digital cash is relatively simple if you don't need anonymity. The process begins when the client software generates a list of numbers to be assigned to the digital coins themselves, and then sends these coins to the bank when withdrawing money. The bank certifies that the coins are good by digitally signing them and sending them back to the client. When the client wants to spend a coin, the coin is sent to a merchant, who forwards it to the bank to verify that is has not been spent previously. The coin is then credited to the merchant's account. Encryption is used to ensure that eavesdroppers cannot grab the coins in transit.

This system is fine, but does not provide any anonymity at all; the bank can match up every transaction to every client using the digital cash system. Adding anonymity requires the client software to use a blinding factor when it sends its digital coins to the bank for certification. When the client blinds the coins, the bank cannot keep a list of coins submitted by any particular client, though they can still certify the transaction through digital signatures from the client. The bank can certify the blinded coins and send them back to the client — who then

removes the blinding factor, leaving the original coins still signed by the bank.

When the client wants to spend a coin, the coin is transmitted to the payee, who in turn forwards it to the bank. The bank certifies that the coin is a good one by verifying its own digital signature, and then credits the payee with the value of the coin. The coin itself then goes into a list of spent coins, so the bank can prevent double-spending. Since the bank never sees the coin itself before it is spent (when originally certified, the coin is in a blinded form), there is no way to link the coin to the person spending it. Anonymity of the entity receiving the payment is not as strongly protected, however, and it is not possible to place real cash into (or remove it from) the system anonymously.

Advantages for Merchants

The big advantage for merchants is the immediate clearing of all transactions. Some merchants may also wish to offer digital cash as a payment option to attract those consumers who wish to remain anonymous, or who just prefer to use digital currency.

Advantages for Consumers

Consumers who want to guarantee their anonymity when making purchases across the Internet will find digital currencies attractive.

Weaknesses and Disadvantages

Because digital currency depends heavily on cryptographic tools, it is potentially susceptible to any flaws that may be

found in the underlying algorithms or in the implementations of those algorithms. The worst-case scenario, a criminal possessing a method of creating counterfeit digital cash, is a daunting prospect to any bank considering entering the business. Even though it is highly unlikely, digital currency counterfeiting could prove catastrophic to all involved.

High cost is another disadvantage to using digital cash. As currently implemented by the Mark Twain Bank and DigiCash, you have to send in some real money to start your account. Startup fees range from as low as $11 for an individual account to as much as $300 for a high-volume commercial account. Monthly fees also vary, from as little as $2.00 for high-volume individual accounts up to as much as $25 for low-volume merchant accounts. The percent charged on money moved through the system ranges from as little as 2% for high-volume merchant accounts to as much as 5% for the entry-level individual account.

At the moment, relatively few consumers use digital cash, and relatively few merchants accept it. This makes it a somewhat unattractive option for merchants with limited resources.

EXTERNAL CHANNEL APPROACH

When people first starting transacting business over the Internet, most of the commerce tools and systems described in this book did not exist. Before real commerce was even permitted on the Internet (because of government funding, companies were not permitted to promote products on the Internet until the early 1990s), individuals used e-mail, Usenet news, and other means to buy and sell personal goods. Most of these transactions took advantage of an external channel to consummate the deal, since most indi-

viduals don't accept credit cards in payment for personal transactions.

These individuals might meet each other in person to examine the items for sale and negotiate terms, or they might send goods and payments through postal mail or delivery services. In any case, they used a channel external to the Internet to complete the transaction.

This approach is still widely used on the World Wide Web by companies that for whatever reason don't wish to institute Internet payment as an option. They advertise their goods and publish a telephone number, fax number, or postal address for submitting orders. There are other companies (some that host Internet malls) that let consumers set up accounts linked to credit cards, which the consumers call, fax, or send in by mail. All these companies avoid the problems of transmitting payment information securely on the Internet, an inherently unsecure medium.

Of the companies offering Internet commerce using this external channel approach, First Virtual has done the most to make it accessible to more consumers and to merchants of any size — as well as doing the most work on creating a complete and secure protocol for transacting business in this way.

How the External Channel Approach Works

At its simplest, the external channel approach uses the Internet to point potential customers to the merchant's telephone number or physical location. However, to be a viable and competitive option for Internet commerce, the external channel approach uses the Internet for transmitting almost all the information necessary to complete the transaction, while handling the most sensitive portion of that information (usually the credit card number) off-line.

In general, the way this approach works is that the consumer must initiate an account by sending personal information (such as name, address, phone number, e-mail address) to the commerce provider, often using the Internet. The credit card to be linked to the account, however, is sent to the commerce provider off-line from the Internet to avoid potential loss due to eavesdropping. This can be done with a telephone call, or by sending an application through the postal mail. A customer identifier, and in some cases a password, is provided to the customer to complete the account setup.

When the customer wishes to make a purchase, the consumer account identifier (and password, if present in the system being used) is used to identify the consumer to the system. Thus, no credit card numbers are transmitted across the Internet. For some systems, however, the consumer account identifier becomes nothing more than an alias for that credit card number — and the identifier itself may be vulnerable to use for fraud if it is intercepted.

The First Virtual system goes a few steps beyond this general description. Most important, it employs an extra step of authentication by the consumer through an e-mail query before any transaction can be approved. Also, the minimum amount of information necessary to any part of a transaction is sent across the Internet when a transaction is processed. For example, intercepting an e-mail message confirming a transaction will not reveal the account identifier, but will only disclose the name of the account holder.

Advantages for Merchants

The First Virtual payment system in particular is a less expensive approach to Internet commerce than the others discussed

here. Entry costs for new merchants are considerably lower than for other methods, particularly since getting set up to accept credit cards in payment can be especially difficult for new merchants without a physical storefront. Furthermore, the merchant does not have to be concerned with security issues regarding customer credit card information.

First Virtual notifies customers by e-mail whenever a transaction is made in their name, which means that there is a means of positive authentication tying the customer to the transaction. This adds a degree of safety to the process that is not dependent on cryptography.

For the first year and a half of operation, First Virtual supported sales of information products only. Now that support has been added for digitally signed transfer notifications, merchants can safely ship hard goods as well. First Virtual will, on request, provide a digitally signed notification that a transaction has been authorized for payment.

Finally, because no encryption of any kind is used in the First Virtual system, merchants can be assured that what was assumed to be safe through encryption is not compromised by an algorithm or implementation flaw.

Advantages for Consumers

Unlike other methods, which are dependent on special software, First Virtual lets consumers make purchases from any application — as long as they can remember their account identifier. Because the account identifier is considered private but not secret, its composition need not be as rigorously secure as a password. As a result, users are able to use phrases with real words, although easily guessed phrases are not advised.

The consumer can make a purchase through e-mail, the World Wide Web, ftp, or any other Internet application, from any location. Making a purchase with First Virtual is as easy as any with other Internet commerce system.

Just as merchants can be more confident about the system's security, so can consumers. Credit card theft from First Virtual's system is no more likely (and probably considerably less likely) than the same type of theft from any other off-line merchant's computer. Since this system is not connected to the Internet, it is not susceptible to break-in attempts across the Internet.

Consumers can be confident that they will be alerted almost immediately to any subversion of their personal account identifier, because they are notified by e-mail of any transaction. Since no transaction can be completed without an e-mail approval by the consumer, fraud-related costs to the consumer (as well as to the merchant) are reduced.

Finally, the credit card number is never associated with the First Virtual account, except internally at First Virtual. This means that if the First Virtual account is compromised, there is no potential for fraud using the underlying credit card — the only fraud possible would be through the First Virtual system. Once an account is known to be compromised, that account can be canceled immediately, while the underlying credit card does not suffer any loss.

Weaknesses and Disadvantages

During its first year or so of operation, First Virtual has not attained the market penetration enjoyed by some other Internet commerce systems discussed here. Consumers have

not found very many mainstream merchants, and First Virtual merchants have fewer potential customers than, for example, Netscape Commerce Server merchants. However, since the process of creating a new account is quite simple, merchants can point their customers easily to the First Virtual Web site to get them started.

Another problem that many First Virtual merchants encountered in the first year has been the holdback period. While other systems provided faster funds turnaround, First Virtual held back funds from merchants' sales for 91 days. Starting in 1996, though, qualified merchants will be able to apply for Express Merchant status. This program is intended for merchants who are already able to accept credit cards and who wish to sell hard goods. Those approved will enjoy funds availability in 3–5 days. Details about applying for this program are discussed in more detail in Chapter 6.

The original limitation on the sale of hard goods (such sales were forbidden by the First Virtual terms and conditions until December 16, 1995) was also a problem for merchants whose products could not be turned into information products. Modifications to protocols First Virtual uses to manage Internet transactions have made it possible for merchants to confidently sell and ship hard goods. Details of these modifications are explained in Chapter 4, and the implementation of this new service is discussed in Chapter 5.

One common objection people make to the First Virtual system on first hearing about it is that it sounds very complicated. First Virtual requires users to check their e-mail regularly, and customers must respond to a confirmation request message any time they make a purchase. However, once people have actually gone through the process of making purchases with First Virtual, they realize that it sounds more

complicated than it actually is. To put the issue in its proper perspective, consider how you would explain to a time traveler from the 1940s how to usa a debit card or ATM card to pay for groceries: it would very likely come out sounding more complicated than using First Virtual's system.

PART TWO

FIRST VIRTUAL:
The Company, Its Products and Services

CHAPTER FOUR

THE FIRST VIRTUAL APPROACH TO INTERNET COMMERCE

Summary The birth of the First Virtual organization is interesting, and the objectives of the startup are also interesting as they are in harmony with the culture of the Internet as it was. This chapter tells that story, as well as explaining the underlying concepts and issues related to the Green Commerce Model. Also included here is more detail on the First Virtual organization, their offerings, and how they've been doing in the first year and a half or so.

Contents

THE BIRTH OF FIRST VIRTUAL 100

HOW FIRST VIRTUAL WORKS 101
- Creating an Account 102
  - Account Requirements 103
  - Submitting the Application 103
  - Terms and Conditions 103
  - Making a Purchase 104
- Making a Sale 105

FIRST VIRTUAL PROTOCOLS 105
- The Green Commerce Model 107
  - Cardholders and Cardholder Accounts 109
  - Green Commerce Transactions 110
  - Funds Transfer 111
  - Cardnumber Inquiries 114
  - Transfer Inquiries 114
  - Chargebacks 115
  - Green Commerce Server Capabilities 115
  - Cardholder Account Application . 115
  - Account Maintenance 116
  - Account History Requests 116
- Application/Green-Commerce MIME Content-Type 117
  - Simple MIME Exchange Protocol (SMXP) 118
  - Simple Green Commerce Protocol (SGCP) 118

SELLING HARD GOODS WITH FIRST VIRTUAL 119
- Added Security Measures 119
- Selling Hard Goods vs. Information Products 119
- Digital Signature Key Management 120
- Validating Digital Signatures 121

THE BIRTH OF FIRST VIRTUAL

First Virtual started out at Los Angeles International Airport. Lee Stein, an attorney providing management and advisory services to an exclusive entertainment-industry clientele, met Einar Stefferud, a University of California, Irvine, professor and 20-year member of the Internet Engineering Task Force (IETF). Just before Christmas 1993, both men were on their way to New York. Stein planned to meet his friend and business partner, renowned rocker Peter Gabriel, at a national press conference for the release of his multimedia CD-ROM video, "Explora."

Stefferud was quietly sitting in a corner, connected to the Internet via his laptop and a wireless modem, something Stein had never seen before. Striking up a conversation with Stefferud, Stein asked what the gadget was and how it worked. While Stefferud explained how the wireless modem worked, Stein also got his first look at the Internet.

They continued their conversation all the way to New York. "We happened to be on the same plane so we sat together," said Stein. "For five hours I listened and learned all about the Internet — where it came from and where it was going." Stein was particularly interested in how the huge volume of information passing across the Internet was paid for, asking the crucial question: "How do people pay for all this information?" Stefferud's answer was simple: "Right now, they don't."

To Stein, the financial impact was undeniable. Recognizing that his entertainment industry clients were selling information, Stein understood that the trick to making money on the Internet would be to create a market for information.

"Let's take an example I call the 'joke of the day,'" says Stein, who is First Virtual's founder, President and CEO. "What if

you, an Internet user, could get a joke through e-mail to share with customers and colleagues a couple times a day for a penny a day? Now let's say all 20 million Internet users subscribe to a joke a day. That's gross sales of $200,000 a day, $1.4 million a week."

"That's when I made the distinction between the movement of goods and services. With goods you have costs of inventory, but with information services you have virtually no cost of inventory."

The "Information Society" is what Stein sees in the future. "For the Information Society to come about, information must be cheap, the cost of inventory must approach zero and responsibility for collection of funds must shift from the financial institution to the merchant. First Virtual changes the model of commerce, by moving the risk to the merchant, or seller of information, instead of the financial institution. The risk is negligible, because the cost to replenish inventory is irrelevant with electronic information transactions. There are no losses to recoup."

HOW FIRST VIRTUAL WORKS

The First Virtual payment system uses Internet protocols and applications to allow participants to buy and sell without exposing sensitive information to prying eyes. Some of the details of these protocols and how they work are explained later in this chapter — but you don't need to know anything about protocols to use the First Virtual system.

Designed to be used by anyone with even the most minimal Internet connection, the First Virtual system is a set of procedures that have been implemented across a variety of different applications. For example, you can apply for a First Virtual

account using e-mail, using telnet, or using the World Wide Web. The information you provide is the same, but in each case the method of getting the information to First Virtual is different. The same applies to selling through First Virtual. Whether the sale is made through a World Wide Web server, through e-mail exchanges, or through an ftp server enabled to accept First Virtual payments, the same information passes between buyer and seller and between seller and First Virtual in each case.

The second half of this book gives the details of creating a First Virtual account (Chapter 6), making a purchase (Chapter 7), and making sales (Chapters 8 and 9). In this section we give a brief preview of the three basic functions of an Internet commerce system and how First Virtual handles them: creating an account, making a purchase, and making a sale.

Creating an Account

There are basically four steps in the First Virtual account creation process:

- You must get an application form from First Virtual, fill it out, and submit it using the Internet.
- Upon receipt, First Virtual sends you an e-mail acknowledgment with further instructions to complete your application.
- You must provide First Virtual with payment information by telephone (for credit card payment) or by postal mail (for payments to sellers' accounts).
- First Virtual sends you e-mail acknowledgment of your account status and activates your account.

Although an immediate response is not always guaranteed, the First Virtual servers are able to respond to account requests

quickly, and the automated telephone system that accepts your credit card number is available 24 hours a day, 7 days a week.

ACCOUNT REQUIREMENTS

Unlike many other Internet payment and commerce systems, First Virtual has minimal requirements for its users:

- A valid Internet e-mail address (this address must belong to one individual and cannot be a shared address; the owner must check it for mail regularly so unauthorized account use is caught).
- A valid credit card for making purchases, and a checking account for accepting payments (for merchants only).
- The user must be an adult (over 18 years old).

There is no special software needed for buyers, and sellers can use the First Virtual InfoHaus service to sell their information products without having to own their own Internet servers.

SUBMITTING THE APPLICATION

The First Virtual account application is completed and submitted using whatever Internet application you want. For example, if you have a Web browser that supports the use of screen forms, you can fill out an application and submit it through the World Wide Web. You can also request a copy of the application and send the completed application back to First Virtual using e-mail, or complete your application interactively by connecting to the First Virtual telnet server.

TERMS AND CONDITIONS

There are three terms and conditions documents for First Virtual's services. In addition to spelling out the legal terms

and conditions of using the First Virtual service as a buyer, as a seller, and as a user of the InfoHaus, they include considerable information about how to use those services and how to resolve issues arising from use of those services. These are not dry legal documents with lots of fine print. First Virtual has drafted them as a very accessible series of questions and answers about the services.

These documents are further discussed in Chapter 5, and are reproduced in full in Appendix C.

MAKING A PURCHASE

The mechanics of making a purchase using the First Virtual payment system are detailed in Chapter 7. Once the buyer has located a seller and chosen a product to buy, the process is a simple one:

- The buyer gives a valid First Virtual account identifier (called a VirtualPIN) to the seller in order to pay for the chosen product.
- The seller sends the transaction information (including the VirtualPIN and amount of the transaction) to First Virtual for approval.
- First Virtual sends an e-mail transaction notification to the buyer, and waits for approval from the buyer before charging the buyer's credit card.
- The seller delivers the product purchased to the buyer (in the case of information products, the delivery may take place before the seller gets approval back from First Virtual; for hard goods, the merchant may wait for approval from First Virtual prior to delivery).

As with applying for a new First Virtual account, making a purchase with First Virtual depends on processes rather than specific applications. For example, the only application-

specific process is the transaction notification, which requires the use of e-mail. The purchase itself can be made over the Internet using the World Wide Web or an ftp session, or it can even be done by hand, in person.

Making a Sale

Selling, of course, is the flip side of buying. However, the First Virtual seller has more to do than the buyer. The seller must set up an Internet server capable of getting buyer information and generating the transaction information needed by the First Virtual servers, and delivering that information to those servers. That server must also be capable of delivering the information product purchased, or else of getting delivery information for hard goods.

The burden on sellers is much lighter than it might be, however, for two reasons. First Virtual provides access to free software and scripts that can be used to First Virtual enable your own servers. For those sellers who don't have their own servers, First Virtual offers the InfoHaus service. InfoHaus is a hosting service from which startup merchants can sell their information products for an additional 8% commission to First Virtual (in addition to the standard 2% and other transaction fees).

Chapter 8 explains how to use the InfoHaus service to sell your information product, while Chapter 9 explains how to use the scripts and software provided by First Virtual to sell information products or hard goods from your own servers.

FIRST VIRTUAL PROTOCOLS

The First Virtual payment system depends on a systematic approach to the different tasks related to Internet commerce.

The way these tasks are accomplished with the First Virtual system is defined in three specification documents. The first document, "The Green Commerce Model," defines an approach to Internet commerce for information merchants that puts the burden of risk on the merchant (because there is a vanishingly small cost to information merchants when goods are not paid for). The result is a method of Internet commerce that keeps costs very low for all involved, in particular for new merchants.

The "Green Model" paper defines the outlines of how transactions occur in such a framework, including an overview of how participants in such a framework are identified, how payments are made between participants, and how the other related tasks of an Internet commerce system flow occur. The May 1995 revision of this document is only twenty-two pages, and it is easily approached by the general reader.

The actual details of the First Virtual implementation of this model require considerably more exposition. These details are included in the document "The Application/Green Commerce MIME Content-Type." Each type of interaction among buying and selling participants and First Virtual servers is described and explained here. You can read here about exactly what data is being transferred between the buyer and the seller when a transaction is made, exactly how account update data is sent from a buyer to the First Virtual servers, and exactly what information is transferred when the current status of a transaction is requested.

Finally, these transactions must be carried over the Internet using some protocol to define the way they are carried. The document that describes this protocol is "The Simple MIME eXchange Protocol (SMXP)," spelling out a method for communicating between entities over the Internet using Multipurpose Internet Mail Extensions (MIME) and e-mail. Finally, the Simple Green Commerce Protocol (SGCP) is an application of

SMXP using the application/green-commerce protocol. SGCP is described in a brief appendix to the application/green-commerce document.

One could argue that since the First Virtual system is also defined by the MIME protocol document, as well as by relevant Internet e-mail protocols, these protocols should also be described here — but these protocols are in general use for many purposes beyond Internet commerce. By the same extension, one would be able to argue that you need to understand how electricity is delivered to a cash register in a store to understand how to transact a sale in person.

The three First Virtual specification documents are available on the included CD-ROM, as well as on the First Virtual Web site; they are summarized in the sections to follow.

The Green Commerce Model

This model defines the approach to Internet commerce that First Virtual pursued in its first year or so. The model itself explains how transactions between participants in an Internet commerce system are completed; it does not specify how those transactions are settled, nor does it put any other theoretical limits on how payments to buyers or sellers are made. This means that there is no fundamental reason not to allow buyers or sellers to use any type of payment medium: credit cards and direct deposit checking accounts, debit cards, digital currencies, or any other method (although only the first two are currently implemented in the First Virtual system).

Originally intended simply for the sale of information, this model defines a method of putting the risk of failed transactions on the entity involved that can best afford it: the information merchant.

Since the information does not have a significant cost of delivery, and the failure of a single sale does not preclude reselling exactly the same information to others, the merchant effectively loses nothing when a potential customer takes delivery but does not buy. On the other hand, it is not good to force customers to pay for information products with no recourse in the event that the product is unsatisfactory. Customers who believe they have been cheated will not be likely to make future purchases. The same goes for the entity handling the settlement of the transactions: the merchants and the customers may be happy, but the credit card acquirer (or other entity offering transaction settlement) might not be.

By reducing the risks to the merchant as much as possible, under this model it is expected that the potential costs due to loss are covered by the additional opportunities offered by the possibility of selling to anyone connected by e-mail to the global Internet.

This model is defined as allowing any participant to act either as a merchant or a buyer, and the transactions are defined as being permitted through store and forward (e-mail) messages using the "application/green-commerce" format discussed in the next section, or directly and interactively through the use of the Simple Green Commerce Protocol, as discussed later in this chapter.

The reader should note that while the Green Commerce model is the basis for the First Virtual payment system, the two are not identical, but rather parallel. The Green Commerce model attributes relate directly to First Virtual payment system attributes, but they don't always use the same names. For example, while the Green Commerce model refers to account identifiers as "cardholder numbers," the same identifier in the First Virtual system is called a "VirtualPIN." However, the procedures and interactions described in the Green Commerce model relate directly to First Virtual procedures and interactions.

The Green Commerce model describes how participants' accounts are identified and structured. It also describes how transactions and other functions are handled by sending messages between participants and a Green Commerce server, which is maintained by the organization offering the commerce system. The model remains relatively vague on details of implementation and policies: the implementation is described in other documents, and the policies are the business of the organization providing the commerce service.

CARDHOLDERS AND CARDHOLDER ACCOUNTS

This model calls the participating buyers and sellers "cardholders," each of which must have an associated account, and each of which is identified by an associated cardnumber. A cardholder account is defined by the information with which it is associated, and which is required to open the account:

- An Internet e-mail address (required for sending transaction confirmations).
- A "state" or status: this can be only one of "active," "seller-only," "suspended," or "invalid."
- A "pay-in" method to indicate how the cardholder pays money into the system, e.g., a credit card.
- A "pay-out" method to indicate how the cardholder is to receive money from the system for sales, e.g., a direct deposit checking account. This is only required for those wishing to sell with the system.
- The currency in which the cardholder makes payments in and out of the system.

This information is associated with the cardholder's cardnumber, but it cannot be derived from that cardnumber. In a way, the cardnumber acts as a pseudonym for the cardholder, as well as an alias for the cardholder's payment methods.

The cardnumber is an alphanumeric string that must be:

- Uniquely identified with a particular cardholder account (only one cardnumber for each account, and only one account for each cardnumber).
- Easy to type and to read by a human (to avoid entry errors when making purchases).
- Relatively difficult to guess based on the identity of the cardholder entity (should not be someone's name, favorite color, birthday, etc.).
- Not related in any way to the payment methods associated with the cardholder account (e.g., there must be no way to figure out a credit card number based on the cardnumber).

The model defines cardnumbers as "bidirectional," meaning that all cardholders may engage in buying or selling, and explicitly states that the terms "merchant" and "buyer" are relative to the direction the money flows. For example, an individual may use the same cardnumber to make a purchase and to make a sale; in the first case, the cardholder is acting as a buyer, in the second case, the cardholder is acting as a merchant. By the same token, a cardholder making a contribution to a non-profit organization is called the buyer and the non-profit organization is called the merchant, even though no product is being purchased.

GREEN COMMERCE TRANSACTIONS

Eight types of transactions are defined in the Green Commerce model:

- Transfer of funds between cardholders.
- Cardnumber status inquiries.
- Funds transfer status inquiries.
- Chargebacks for disputed transfers.

- Request for Green Commerce server capabilities.
- Application for a cardholder account.
- Account maintenance and attribute changes.
- Account history requests.

Transactions in this model are completed through the exchange of messages between cardholders and a Green Commerce server. Each message is identified by a combination of a "verb" referring to the type of transaction ("payin," "payout," "status," "inquiry," etc.) and a "modifier" referring to what the message is actually doing ("-request" to indicate a request, "-query" to indicate that a "-response" message is required from the recipient).

While the exact mechanics of what information is contained in each of these messages is spelled out in the application/green-commerce MIME content-type, the Green Commerce model explains the overall interaction between cardholders (acting as buyer and seller) and the Green Commerce server through which transactions are made.

FUNDS TRANSFER

This is the most important process in the model: it defines how the cardholder buyer pays for products purchased from a cardholder merchant. The process starts when the buyer provides the merchant with a cardnumber. The merchant then sends a "transfer-request" message to a Green Commerce server, including the buyer and merchant cardnumbers, a transfer type, a brief description of the transaction, the transfer amount and the currency being used, and an optional merchant transaction identifier.

When the Green Commerce server receives this request, it sends out a "transfer-query" to the e-mail address associated with the buyer's cardholder account. This message includes a unique

transaction identifier number as well as the transfer type, description of the transaction, transfer amount and currency, and the merchant and buyer names. Optional information may include the merchant transaction identifier, and if there is currency translation (if the buyer and seller use different currencies) the original currency and amount are also noted.

The process must now await a response from the buyer; if no response is received in a certain time period or after a certain number of transfer-query messages have been sent to the buyer, the cardholder account changes status to "suspended." The buyer must respond with a "transfer-response" message indicating the transaction-identifier and the willingness of the buyer to permit funds to be transferred. The options available are either "yes" or "no" to indicate approval or refusal of the transfer, or "fraud" to indicate that the buyer denies having initiated the transaction.

When the Green Commerce server receives the "transfer-response" from the buyer, it sends out a "transfer-result" message to the merchant. This result contains much the same information contained in the transfer-response message, along with the buyer's response. If the buyer responded with a "yes," the transaction is added to the server's settlement queue for the buyer; if the answer is "no," the buyer may get a service charge added to the server's settlement queue. Buyers who respond "no" more than a certain number of times after a certain number of transactions may find their accounts suspended. If the buyer responds with "fraud" then their account enters the invalid state.

Settlement of transfers occurs when the Green Commerce server checks its settlement queue for each cardholder, eventually consolidating the transactions that are outstanding into a single actual transaction. When a transaction is ready to be settled, the server sends a notification message to the buyer

that a pay-in is about to be made to the seller; when the settlement cycle completes, the funds are transferred and a pay-out notification is sent to the seller.

These transfers generate notification messages, and may generate failure notification messages in the event that the attempts to settle transactions fails. The process of transferring funds is illustrated in Figure 4-1. The Green Commerce server acts as an intermediary between the buyer and the seller, and also between the cardholders and their pay-in and pay-out systems.

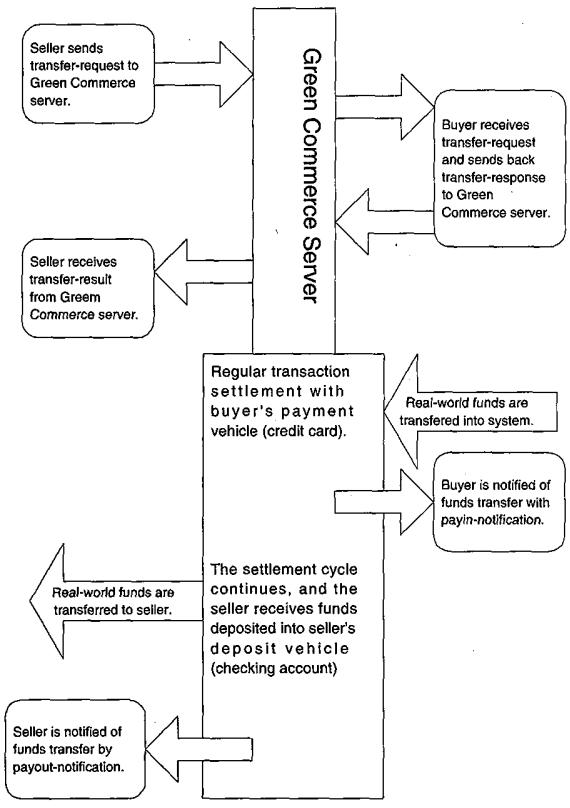


FIGURE *The Green Commerce server mediates transactions between the buyer and seller, and also handles the transfers of funds between cardholders and their pay-in or pay-out mechanisms.*

CARDNUMBER INQUIRIES

Cardholders acting as merchants are likely to want to verify that a buyer's cardnumber will be a valid one. This type of verification is a two-step process: the merchant sends an inquiry request with the buyer's cardnumber to a Green Commerce server; the Green Commerce server returns an inquiry result indicating the current state of the cardholder's account.

As mentioned previously, the status can be one of four:

- "Active" means the account is valid and enabled for buying or selling.
- "Seller-only" means the account is valid but enabled only for selling.
- "Suspended" means the account has been temporarily suspended because the cardholder has not paid for a high enough proportion of purchases initiated or because the cardholder has not responded to transfer-queries for a recent purchase.
- "Invalid" indicates that the account is not a valid one: this may mean an entry error has occurred, or the account has been invalidated due to a "fraud" response by the cardholder.

TRANSFER INQUIRIES

There are times when a merchant wants to check on the status of a funds transfer. The Green Commerce model allows the merchant to send a status-request message to a green commerce server that includes the transaction-identifier number; the server will respond with a status-result message that indicates the last message sent by the server relating to that transaction. The response can indicate either that the server is

waiting for a response from the buyer, or that a response has been received (and include the results of that response).

CHARGEBACKS

Sometimes a transaction that has been approved within the Green Commerce system needs to be reversed — for example when there is a dispute over a charge to a credit card. Because the settlement process occurs external to the commerce system, when this happens the Green Commerce server generates messages to notify the buyer (payin-chargeback-notification) as well as the merchant involved (payout-chargeback-notification). These messages indicate the transaction identifier and the amount and currency of the chargeback.

GREEN COMMERCE SERVER CAPABILITIES

It is conceivable that not all Green Commerce servers available to a cardholder will support all types of transactions or currencies. Cardholders can get a list of supported transactions and currencies from a server by sending a "capabilities-request" to the server; the response is called a "capabilities-result."

CARDHOLDER ACCOUNT APPLICATION

There are two processes in applying for a cardholder account: getting the application, and submitting the completed application. The first transaction occurs when the applicant sends an "application-request" to a Green Commerce server; the response is to send back an "application-result" message that includes something like a form for the applicant to fill out.

Once the application is completed, the applicant submits it as a "newacct-request" to a Green Commerce server. The server responds by sending back a "newacct-result" message indicating

the status of the application. This message may include the actual cardnumber to be assigned to the cardholder, if the application is accepted.

ACCOUNT MAINTENANCE

Routine account maintenance, such as modifying certain cardholder account information, is necessary to any commerce model. The Green Commerce model handles this as it would any other transaction. Making changes to the cardholder account information is a multistep process: the cardholder first sends an "initchg-request" message to a server with the cardnumber of the account. The server responds by sending back an "initchg-result" message containing the cardnumber and user-modifiable account parameters in a form for the cardholder to fill out.

Once the "initchg-result" message is filled out with the new information, the cardholder sends it to the server as a "chgacct-request." The server responds with a "chgacct-query" that is similar to the purchase verification message. The cardholder must respond to this query with a "chgacct-response," choosing from "no," "yes," or "fraud" to indicate whether the indicated changes should be made. As with purchases, if the cardholder indicates "no," no changes are made (it is assumed the user made an error or decided against the change); if the cardholder indicates "yes," the changes are made and a "chgacct-result" message is sent by the server indicating the changes made. If the cardholder responds "fraud," the server invalidates the account on the strength of the cardholder indicating that someone else made the request for a change.

ACCOUNT HISTORY REQUESTS

Cardholders wishing to retrieve messages relating to their recent activities can send a "history-request" message, with their card-

number, to a Green Commerce server. The server in turn responds with copies of recent messages sent from the server.

Application/Green-Commerce MIME Content-Type

The Green Commerce model for Internet commerce, as described by the founders of First Virtual, is relatively easy to handle. The defining document is only a relatively sparse 22 pages, including a number of ASCII graphics demonstrating data flows, and can be found in the accompanying CD-ROM.

"The Application/Green-Commerce MIME Content-Type" document defining how the Green Commerce model is actually implemented appears more daunting. At almost 100 pages, this document starts out by defining terms and syntax usages. This is standard for Internet specification documents, but it may quickly frustrate the general reader.

The bulk of this document, which is also included in the accompanying CD-ROM, describes every single possible transmission used in the course of a Green Commerce transaction. In the most recent version of this document, almost three dozen transaction types are defined, ranging from the initial request to transfer funds between two account holders, through the notifications relating to payments sent to buyers and sellers, to requests for information about the capabilities of a Green Commerce server (e.g., which currencies and transaction types are supported).

Other important information included here is definitions and specifications for the information to be included in Green Commerce transactions, including the formal names for transaction attributes and the composition of the values of those attributes.

This document also defines how the transactions are to be communicated between participating entities. Because it defines a MIME content-type, the method of transport over the Internet is assumed to be e-mail. The participants' e-mail readers need not be capable of handling MIME enclosures, as long as they can format their e-mail messages in the same way that MIME enclosures are formatted: the content is more important than the format in which the content is displayed. The MIME enclosures associated with each transaction must include the information necessary to process each transaction, and it must be included in the defined format in order to be processed.

SIMPLE MIME EXCHANGE PROTOCOL (SMXP)

Using MIME structures to handle commerce transactions makes it easy for those with the most basic Internet access (e-mail only) to buy and sell. However, those potential consumers and merchants with more complete Internet access may prefer to operate interactively. As a result, Marshall Rose and Nathaniel Borenstein, two of First Virtual's founders, devised a method for adapting MIME formats to a more interactive protocol. Called the Simple MIME Exchange Protocol (SMXP), it defines a method of using MIME formats in Internet applications other than e-mail. This document is also included in the companion CD-ROM.

SIMPLE GREEN COMMERCE PROTOCOL (SGCP)

The application of the SMXP protocol to the Green Commerce model, using the Green Commerce MIME content-type, is called the Simple Green Commerce Protocol. This protocol is very simply explained in an appendix of "The Application/Green-Commerce MIME Content-Type" document as an Internet application using the TCP transport protocol (as in the "TCP" of "TCP/IP").

SELLING HARD GOODS WITH FIRST VIRTUAL

The original version of the Green Commerce model specifically targets information products — products that can be transmitted as data across an open network like the Internet. An intrinsic part of the model places the greatest risk on the merchant, making it probable that consumers dissatisfied with the product will not pay for it. However, the implementation as defined in the latest version of "The Application/Green-Commerce MIME Content-Type," allows for the possibility of using the Green Commerce model to buy and sell hard goods.

Added Security Measures

The key modifications to the specification are relatively small, and the implications of the changes are not explicitly spelled out. The most important change is simply the addition of a possible value for the SECURITY-REQUIREMENTS parameter used in the funds transfer requests that initiate a transaction. This parameter had previously been defined, but the only valid value had been "none." Now, a new value for this parameter has been added:

```
x-pgp-transfer-notification
```

If the merchant specifies this value under SECURITY-REQUIREMENTS, the transaction is processed slightly differently.

Selling Hard Goods vs. Information Products

When selling hard goods, the merchant needs to be much more careful about risks involved with nonpayment. After all,

goods and delivery charges are lost when a product is shipped but not paid for. Merchants selling hard goods need greater assurance that their sales are approved prior to shipping them.

First Virtual adds the x-pgp-transfer-notification option security requirement to enable sales of hard goods. What it means is that the merchant is requesting a nonrepudiable (undeniable) notification that an acquirer has approved the sales transaction, meaning that the credit card has been approved for that particular transaction. The notification includes a standard PGP (Pretty Good Privacy) digital signature from First Virtual, so the merchant can feel comfortable in shipping the product.

Adding the digital signature is necessary because without it, criminals could purchase goods from merchants and forge notifications from First Virtual, causing the merchant to ship goods to a customer whose credit card was not being charged. Digitally signing these notifications removes this potential attack, and results in a transaction very similar to other "card not present" transactions, like telephone or mail orders.

Digital Signature Key Management

Using digital signatures requires two keys: one published, one kept very secret. First Virtual merchants using this option need access to the public key of the pair so they can certify notifications as coming from First Virtual. First Virtual needs to keep the private key a secret; otherwise, someone might be able to use it to forge authorizations from First Virtual. This is the source of a major risk for any type of digital signature process: if money can be made by compromising a private key, someone may try it.

Compromising a typical digital signature key pair used by a private citizen would not normally be worth the effort: brute-force attacks might require a vast array of high-powered com-

puters and a lot of time. However, the private key that First Virtual uses to sign transfer notifications could be worth a lot of money to someone able to steal it. Such a criminal could order many different products from many different First Virtual vendors, and then send those vendors forged transfer notifications. First Virtual has addressed this unlikely scenario through proper key management.

First Virtual acknowledges that there is a possibility (however unlikely) that some criminal may acquire sufficient computer power to successfully forge their digital signature. Such forgery would require considerable time, no matter how powerful the computers. So, rather than create a single key pair and wait for it to be compromised, First Virtual publishes a new key every month. Further checks are instituted throughout each month so attempts at forgery can be identified immediately. Also, the public keys are published through well-trusted and verifiable methods, so merchants can be certain that some criminal has not attempted to subvert the system by publishing a fake key.

Validating Digital Signatures

You don't need to be a handwriting analyst to verify a digital signature, but you do need special software that is capable of performing Pretty Good Privacy (PGP) functions. Freeware versions of PGP are available from various servers on the Internet, one version for use in the United States and another for international use (although both can interoperate on the same data). A commercial version called ViaCrypt is also available from ViaCrypt, a division of Lemcom Systems, Inc.

More information about getting and using PGP software is included in Chapter 5.

CHAPTER FIVE

FIRST VIRTUAL PRODUCTS AND SERVICES

Contents

THE FIRST VIRTUAL ORGANIZATION 124
A Virtual Corporation. 124
Using Automation 125
First Virtual Products and Services. 126

TERMS AND CONDITIONS 127
Getting the Terms and Conditions Documents. 128
Buyer's Terms and Conditions. 129
Seller's Terms and Conditions. 129
InfoHaus Seller's Terms and Conditions 130

BUYERS' SERVICES 130
Account Requirements 130
Account Creation 131
Buying Privileges 132
Customer Support Services. 132

SELLERS' SERVICES 133
Account Creation and Requirements . . 134
Selling Privileges 135
Customer Support Services. 135

WHY THE 91-DAY HOLDBACK PERIOD? 136

THE INFOHAUS SERVICE 137
Storefront Creation and Requirements . 138
Storefront Management. 138
Rights and Responsibilities 139
Customer Support Services. 139

REACHING FIRST VIRTUAL 139
Contacting First Virtual via the World Wide Web. 140
E-mail Addresses 141
Automatic E-mail Responder 141
Special Addresses for Sellers 141
Special InfoHaus Addresses 142
Other Internet Resource Addresses . . . 142
ftp 143
Telnet. 143
First Virtual Users Mailing List. 144
How To Subscribe To the FV-Users List. 144
Unsubscribing From the FV-Users List. 145
Participating In the FV-Users List . . 145
Reaching a Human. 146

Summary This chapter explains specific First Virtual offerings, briefly introducing the concepts of sellers' and buyers' accounts, the InfoHaus, what you get, and what it costs. The chapter also gives overviews of the Terms and Conditions documents that govern First Virtual transactions. Also provided here are contact information such as automatic e-mail responses that include First Virtual information documents, telnet and ftp servers, Web servers, and real-world First Virtual contact information.

THE FIRST VIRTUAL ORGANIZATION

As might be expected from the company's name, First Virtual started out as a "virtual" organization: rather than maintaining a single physical plant and requiring everyone on the payroll to show up at the same location for work every day, First Virtual founders and early employees were spread out across the United States. Relying on electronic and digital communications to stay in touch with employees, First Virtual from its birth depended on a high level of automation coupled with the use of technology to leverage resources for solving business problems.

The story of the First Virtual organization's first year or so of operation is told in the document "Perils and Pitfalls of Practical CyberCommerce," included on the companion CD-ROM and first presented at the Frontiers in Electronic Commerce conference in Austin, Texas, in October 1995.

A Virtual Corporation

Relying on electronic means of communication, including phone, fax, and especially e-mail, meant that physical locations were, in a way, irrelevant. Indeed, the company didn't set up real-world offices until fifteen months after it was founded — which meant that the First Virtual payment system had already been operational for eight months. Four of the principals were located in different regions (San Diego; Silicon Valley; Orange County, California; and New Jersey), and none were interested in relocating. Employees, consultants, and systems resources were likewise located and supported across the country. As the organization grew, a main

office was established in San Diego, though First Virtual still retains the flavor of a virtual organization.

Using Automation

Leveraging the technologies for First Virtual has meant in large part using automation to support customers, at least for first-level problems. Over time, the First Virtual team has developed a set of clear, complete, and comprehensive documents relating to practically every aspect of the organization and their services. From lists of frequently asked questions, to how-to guides for buying, selling, and using the InfoHaus, to "white paper" style documents addressing issues such as security of Internet commerce, First Virtual has attempted to anticipate as many customer inquiries as possible and make the answers accessible.

Automation, once in place, is inexpensive to support. If there is a sudden burst of interest in First Virtual as a result of a news story, for example, the e-mail servers are unlikely to be so busy that people can't get through. With human operators, that could happen, frustrating some of the potential customers. The same idea applies to explaining how to use the First Virtual payment system: it may be easier for some people to understand spoken instructions from another human, but if the instructions are sufficiently simple (as with First Virtual's system), then a well-written set of instructions is far less expensive to maintain than a battery of customer support staffers.

The flip side of the coin is that leveraging resources through automation means that while the relatively simple problems are easily handled, First Virtual clients who have more complicated

problems or who may need extra handholding won't always be able to get the immediate attention they may expect.

First Virtual Products and Services

Simply, First Virtual offers a medium of exchange for values over the Internet. This means accounts for buyers who wish to purchase products, and accounts for sellers who wish to sell products over the Internet. First Virtual services are summarized in Table 5-1.

To keep things simple for buyers, there is only one type of buyer's account, and you can use it to make any kind of purchase. There is a one-time fee of $2.00, and the only requirements are that the buyer be 18 years old or older, have a valid credit card, and have their own personal (not shared) e-mail account.

Sellers have more options. The basic seller's account costs only $10 to start up and requires that the seller be 18 years

TABLE 5-1 *First Virtual services and charges, in a nutshell.*

Service	Startup fee	Fees	Notes
Buyers account	$2.00	None	Switching credit cards (including expired ones) requires an additional setup fee
Sellers account	$10	2% of sales amount and $0.29 per sale; $1.00 processing charge for fund deposits	Requires a checking account; 91-day funds holding period
InfoHaus storefront	None	Normal FV fees plus 8% of sales amount; $1.50/Mbyte of data stored monthly	
Express Merchant	$250 application fee	Normal FV fees	Discounts may be possible based on past performance

old or older and have a valid checking account that can accept direct deposits. This type of account allows sales of any type of product over the Internet, but includes a 91-day funds holding period to avoid losses through chargebacks. While some merchants may find this holding period a burden, First Virtual must use it to avoid potential losses due to fraud — and by using it they are able to offer merchant services to all comers without costly credit checking, all for $10. These issues are discussed in more detail later in this chapter.

Sellers who don't want to (or can't) maintain their own Internet servers can use the First Virtual InfoHaus service. This is an Internet hosting service, on which sellers can store their information products and offer them for sale without the expense and effort associated with managing their own servers. You upload your data to the InfoHaus, and buyers can browse your products (as well as those of other InfoHaus merchants) through the First Virtual Web site (or by other methods). Instructions for using the InfoHaus to sell your products are included in Chapter 8.

Express Merchant status is a value-added service for merchants who can qualify for it. Express Merchants get sales proceeds credited to their accounts within 3–5 days instead of being subject to the 91-day holdback period. With a $250, nonrefundable application fee, it is intended for merchants who are able to qualify independently for merchant banking services to enable them to accept credit card payments.

TERMS AND CONDITIONS

First Virtual has created a set of well-written and easy-to-understand Terms and Conditions documents to avoid disagreements

over exactly what services First Virtual provides, what their responsibilities are and what their customers' responsibilities are. These documents use a "Q&A" format and plain English, as well as examples and clarifications for any points that may need them. It is important that you read the Terms and Conditions document relevant to each First Virtual service you plan to use. The most recent versions of these documents are included in Appendix C.

Getting the Terms and Conditions Documents

Although First Virtual does not intend to modify these documents frequently, you should get the latest version directly from them before using any First Virtual service. Table 5-2 shows how to retrieve these documents, using various Internet applications. If in doubt, the best resource will be the First Virtual Web site. At this writing, the most recent Terms and Conditions revision was December 16, 1995. You can subscribe to a Terms and Conditions changes notification mailing list by sending e-mail to the address:

```
fineprint-changes-request@fv.com
```

The message need not have any subject or body; when any changes to the First Virtual Terms and Conditions documents are made, you will be notified through this mailing list.

TABLE 5-2 *Getting First Virtual terms and conditions documents.*

Service	World Wide Web	E-mail
Buyer	http://www.fv.com/pubdocs/fineprint-buyer.txt	fineprint-buyer@fv.com
Seller	http://www.fv.com/pubdocs/fineprint-seller.txt	fineprint-seller@fv.com
InfoHaus	http://www.fv.com/pubdocs/fineprint-infohaus.txt	fineprint-infohaus@fv.com

Buyer's Terms and Conditions

This document provides an excellent introduction to the First Virtual payment system for buyers. It explains how to reach First Virtual (and how First Virtual reaches its customers), as well as requirements for becoming a First Virtual buyer. Section 4 explains how the system works, including the VirtualPIN and sales notification queries. Most other relevant issues are covered, too, such as First Virtual fees (Section 6), buyer's responsibilities (Section 7) and risks (Section 8), First Virtual's disclaimer of warranty (Section 9), dispute resolution (Sections 10 and 11), changing or terminating the agreement (Sections 12 and 13), and agreement validity (Section 14).

The complete Buyer's Terms and Conditions document is included in Appendix C.

Seller's Terms and Conditions

Much of the first part of this document resembles the Buyer's Terms and Conditions, including definitions and contact information, and description of the First Virtual payment system (Sections 1 through 4). Section 5 explains what can be sold through First Virtual, and what shouldn't be sold; Section 6 covers sellers' fees. Sellers' responsibilities are explained in Section 7, including chargeback issues. As in the buyer's document, the last few sections cover things like risks (Section 8), First Virtual's disclaimer of warranty (Section 9), dispute resolution (Sections 10 and 11), terminating or changing the agreement (Sections 12 and 13), and agreement validity (Section 14).

The complete Seller's Terms and Conditions document is included in Appendix C.

InfoHaus Seller's Terms and Conditions

The InfoHaus Terms and Conditions document shares similar language with the other Terms and Conditions documents, but is slightly shorter — after all, you must be a First Virtual seller to become an InfoHaus merchant. The first few sections define the participants (Section 1) and explain how to make contact between First Virtual (Section 1) and the merchant (Section 2). Section 3 explains how to open an InfoHaus merchant site, while Section 4 covers what can be sold (information only, no hard goods). InfoHaus fees are explained in Section 5; merchant responsibilities and risks are covered in Sections 6 and 7, respectively. The document concludes with First Virtual's warranty disclaimer (Section 8), dispute resolution (Section 9), and agreement termination, changes, and validity (Sections 10 through 12).

The complete InfoHaus Terms and Conditions document is included in Appendix C.

BUYERS' SERVICES

Using the First Virtual payment system as a buyer is quite a simple matter. Most buyers will set up their account and use it to buy products, period. Account setup is discussed at greater length in Chapter 6, while using First Virtual to make a purchase is covered in Chapter 7.

Account Requirements

First Virtual's payment system requires some mechanism to get value from buyers to sellers. As of early 1996, this means

a credit card. The underlying protocols can support any number of other types of payment mechanisms, but only credit card payment is currently supported, although this may change in time.

The credit card is charged $2.00 to set up the buyer's account; this charge is assessed only one time per credit card, but if the buyer wishes to switch to a different card the charge is assessed again. This includes updating an expired credit card — so if you have several cards to choose from, you can save a little money by using the one with the most distant expiration date.

A personal e-mail account is also required; First Virtual must have some way to send a message to an account holder and only that account holder. The e-mail account cannot be a shared one, and the account holder is expected to check into the account for messages regularly and frequently.

Finally, the account holder must be an adult (18 years old or older) so that the agreement between the account holder and First Virtual can be valid.

Account Creation

Creating a First Virtual account enabled to make purchases requires getting a minimal amount of account information to First Virtual. This can be initiated through a variety of different Internet applications, including e-mail, telnet, and the World Wide Web. Once the data has been provided to First Virtual, confirmation of the application is provided no more than a day or so later (much faster in most cases). The account holder must enable the account with a telephone call linking the account to the credit card being used.

Buying Privileges

First Virtual buyers can use their account to purchase information, goods, services, or subscriptions, or even to make donations to good causes. For the buyer, the process is simple: give the merchant a valid VirtualPIN, and respond in the affirmative when the e-mail notification query arrives. Buyers may be given the option of examining information products prior to purchase. While this is at the discretion of the merchant, it is advisable to permit it, especially for lower-priced items. Some goods — particularly hard goods — may not be delivered until after an e-mail verification response has been received. Subscription items are shipped as they become current (and completion of subscriptions can be contingent on approval of the original transaction).

A buyer's privileges can be revoked through termination of the account if the buyer attempts to defraud anyone with the account, if the buyer indicates that the account has been used for a fraudulent transaction when responding to a transaction query, or if the buyer declines too many transactions (or too high a proportion of transactions) based on formulas comparing the average approval ratings of the products being purchased. Any First Virtual account holder can transfer value to any other account holder, but pointers to merchants selling products through First Virtual are available on the First Virtual Web site and through the InfoHaus service.

Customer Support Services

One of the most precious commodities in the implementation of Internet commerce is knowledge wielded by a human. There are endless seas of information available online in the form of files, but relatively few people are

knowledgeable about any given topic. Internet commerce companies do not usually have the human resources and infrastructure that banks and credit card companies have for taking and answering questions over the telephone. The costs of these facilities drive the cost of the credit cards themselves.

First Virtual is no exception. Rather than invest heavily in these resources, they have chosen to deploy their information online using as many different formats as possible (and as practical) to provide answers to the different questions that users invariably raise. As a result, if you have a question, you can probably answer it yourself — if you are able to connect to the First Virtual Web site and browse through their documentation (or request the appropriate document via e-mail).

In fact, First Virtual encourages its users to take advantage of these resources before escalating a request for help into a request for help from a human. Details on retrieving First Virtual documents by e-mail, as well as getting a question or problem to a human, are detailed later in this chapter.

SELLERS' SERVICES

Short of mixing up a pitcher of lemonade and selling drinks on your front lawn, First Virtual may be the most inexpensive way to start up selling your own products. For a minimal investment of time and only $10 setup fee, you can be selling your product to anyone who can send and receive Internet e-mail. That's the good news; the (apparently) bad news is that First Virtual offers little more than the infrastructure for doing business. They do not certify merchants through credit checks;

they do not test or verify claims for products sold by their merchants; they do not take any responsibility for the merchants' sales or for their losses due to nonpayment.

This is for a good reason: if First Virtual participated any more than they do in the commerce they enable, costs would rise rapidly.

The setup fee is paid with a check drawn on the account to which the merchant wishes to have sales proceeds deposited. Sellers do not have to be enabled for making purchases, but doing so requires a credit card (and a $2.00 charge). The reason is that a credit card is a more reliable method for getting paid than a checking account, particularly if the checking account balance is too low.

Account Creation and Requirements

Since the First Virtual protocols make little distinction between buyers and sellers, sellers' accounts are created much like buyers' accounts. As mentioned before, all First Virtual account holders must be 18 years old or older and have a valid, personal e-mail account.

Creating a First Virtual account enabled to make sales requires getting a minimal amount of account information to First Virtual. This can be initiated through a variety of different Internet applications, including e-mail, telnet, and the World Wide Web. Once the data has been provided to First Virtual, confirmation of the application is provided no more than a day or so later (much faster in most cases). The account holder must enable the account to sell by mailing a check for $10 to First Virtual; the check is used to enable direct deposit for the proceeds of any sales.

The biggest difference is that sellers have the option of enabling their accounts for selling only, by not providing a credit card number and only sending a check for $10 to First Virtual. However, any First Virtual account has the potential to buy and sell, as long as the account holder provides a pay-out mechanism such as a credit card number (to buy) and a pay-in mechanism such as a checking account number (to sell).

Selling Privileges

The most important part of being a First Virtual seller is that you can receive payment for selling your product through the Internet. There is actually no reason a "regular" (buyer's) First Virtual account cannot be used to sell — except that there is no acceptable mechanism for crediting a credit card when a product is sold. The chief benefit available to sellers is the ability to have funds credited to a checking account.

Sellers can set up storefronts on their own Internet servers or on First Virtual's InfoHaus storefront hosting service. It is also possible to accept First Virtual payments through other media — there is no reason that you can't use a First Virtual account to pay for items purchased in a store, over the telephone, or with smoke signals. As long as the necessary transaction information can be exchanged with the First Virtual servers (and as long as the buyer and seller still check their e-mail regularly), it doesn't much matter how the merchant gets the VirtualPIN and makes the sale.

Customer Support Services

As mentioned earlier, the First Virtual customer support staff relies on a large body of written information that sellers can

consult to answer their questions and resolve their problems. Sellers' questions are often more complicated than buyers' questions, since they usually involve setting up storefronts or unraveling accounting issues. However, it turns out that the vast majority of the time spent on customer support is spent supporting a relatively small number of merchants. While First Virtual does not currently charge for basic support services, there is always the possibility that they will implement some basic level of service for all merchants, with added charges for merchants who want more support.

Sellers may still request a human response to a problem or question that is not answered in the First Virtual library, as described later on in this chapter.

WHY THE 91-DAY HOLDBACK PERIOD?

In a perfect world, we would not have to worry about dishonest people trying to rip us off. Unfortunately, this world is not perfect. Those interested in doing Internet commerce can either design systems that attempt to screen dishonest people out, or they can design systems that will not be affected (too much) by them.

The First Virtual team designed a system that will not be affected too much by dishonesty, thus saving the time and effort (and costs) associated with trying to screen out the thieves. From forbidding the transmission of credit card numbers over the Internet to using positive verification of all transactions, First Virtual has designed a system that is not susceptible to large-scale, automated fraud.

One of the most important mechanisms preventing fraud is the 91-day holdback period. Rather than restricting who can sell

by requiring expensive credit checking (for example, Express Merchant status requires paying a $250 application fee), First Virtual lets anyone sell. The result is that without the holding period something called the "Regulation Z" scam is possible. Credit Card Regulation Z requires your credit card bank to reverse charges on goods that haven't been delivered, as long as the request to make the chargeback comes in within 90 days of the original charge.

All a criminal would have to do is set up a seller's account, set up a separate buyer's account, and then make purchases from the seller's account using the buyer's account over the course of three months. Just before the 91-day limit, the criminal would contact the credit card issuer and ask them to charge back all the payments due to nondelivery of goods.

If First Virtual did not hold back the funds, the criminal could clean out the checking account, and First Virtual would be responsible for the chargebacks. With the 91-day holding period, however, First Virtual can keep everyone honest and can let all comers set up as sellers.

THE INFOHAUS SERVICE

It may only take $10 and a few minutes to setup as a First Virtual merchant, but creating an Internet presence through an Internet server can be much more costly in time and money. You need a computer to run your server software, and the server software itself (along with supporting operating-system and networking utilities). You might be able to put a package together for as little as $1,000 using an older PC and shareware/freeware implementations. However, you also need an Internet connection service which might cost anywhere from $50 monthly on up to thousands — plus the hardware to connect to that service.

First Virtual offers an alternative: the InfoHaus storefront hosting service for information merchants who aren't able or don't want to deal with the hassles of setting up their own Internet servers. First Virtual account holders can set up to sell through the InfoHaus for next to nothing in out-of-pocket expenses.

Storefront Creation and Requirements

Creating an InfoHaus storefront is not as easy as opening your First Virtual account, but if you can read and follow instructions, you should be able to create and stock your Internet shop in an afternoon. The most important limitation, however, is that the InfoHaus is for selling information only: this means data only (text, pictures, audio, or video, even software programs). As long as the product can be delivered digitally, you can sell it over the InfoHaus.

There are a variety of methods of initializing, configuring, and stocking your InfoHaus storefront using various Internet applications such as e-mail, telnet, and ftp. These are all discussed in greater detail in Chapter 8, but simply stated, the merchant needs to associate a store name with a VirtualPIN, provide brief product and store descriptions, stock the store with data files, and price the products.

Storefront Management

The simplest type of storefront uses a very simple default description format to link to listed products through the merchant's business name. More elaborate storefronts can be created by uploading HTML files (Hypertext Markup Language — the format used by World Wide Web documents) to the InfoHaus server.

Rights and Responsibilities

InfoHaus merchants can sell just about any type of information, but there are some limits. InfoHaus merchants cannot sell anything that is illegal, or that infringes patents, trademarks, or copyrights. This means you can't sell pictures you scanned into digital form from a magazine, or copies of software programs you bought elsewhere, or copies of articles or books written by someone else — unless you have permission from the owners of those properties to do so.

In order to avoid conflict with the Communications Decency Act passed in early 1996, InfoHaus merchants are not allowed to sell adult materials.

Customer Support Services

InfoHaus merchants, as First Virtual account holders, can use First Virtual support services already described to answer questions and solve problems raised by their use of the system. In addition, there will be questions and problems raised by the use of the InfoHaus itself. One additional service provided is an e-mail list subscription for those interested in discussing problems and issues relating to the InfoHaus. You can subscribe through the InfoHaus for $1.00. Details on how to subscribe are included in Chapter 8.

REACHING FIRST VIRTUAL

As a virtual corporation, reaching First Virtual is a lot easier to do over networks than in the real world. E-mail is the primary tool, although there are telephone numbers for those who need

to speak to someone. This makes a lot of sense, since even though there are ways to get postal mail to First Virtual, by definition all of their customers have and use e-mail regularly.

Customers and potential customers are most likely to get their first contact with First Virtual through the World Wide Web. First Virtual's Web site has a wealth of information about their system and services, and it is not overloaded with slow-loading graphics images.

First Virtual also maintains a telnet server for account creation and maintenance and other services, as well as an ftp server for retrieving information files and for uploading products to the InfoHaus.

Contacting First Virtual via the World Wide Web

The First Virtual Web site is located at:

```
http://www.fv.com/
```

Here you will find the latest information about First Virtual, as well as a gateway to the InfoHaus, pointers to other First Virtual merchants, complete information about using First Virtual, documentation of the First Virtual protocols, First Virtual utilities and programming interface, and much more. Table 5-3 shows some other URLs of interest within the Web site.

TABLE 5-3 *URLs for First Virtual account application and InfoHaus.*

Task	URL
Apply for an account	`http://www.fv.com/newacct`
Browse the InfoHaus	`http://www.infohaus.com`

E-mail Addresses

If you just want to know the basics about First Virtual, such as how to set up an account or how to use the system to buy and sell, you can get what you need by e-mail. Simply send an e-mail message to one of First Virtual's automated e-mail information addresses (no subject or body is necessary).

AUTOMATIC E-MAIL RESPONDER

First Virtual has set up a server to automatically respond to your e-mail address with the requested information. Table 5-4 shows these addresses.

TABLE *Automated e-mail responder addresses for First Virtual information.*

Document	Address
Account Application	apply@card.com
General Information	info@fv.com
InfoHaus Information	infohaus@fv.com
InfoHaus Seller's Guide	infohaus-guide@fv.com
FV Buying Guide	buying-guide@fv.com
FV Selling Guide	selling-guide@fv.com
Terms & Conditions	fineprint@fv.com

SPECIAL ADDRESSES FOR SELLERS

Messages to the addresses listed in Table 5-5 are all processed automatically. They are used by sellers for various functions discussed at greater length in Chapter 9.

TABLE 5-5 *Special e-mail addresses for First Virtual sellers.*

Function	E-mail address
Submit an application/green-commerce MIME entity for processing	`sgcs@card.com`
Find out what transactions are currently supported	`capabilities@card.com`
Check whether an account is valid (with the account ID in the Subject line)	`inquiry@card.com`
Submit a transaction for processing	`transfer@card.com`

SPECIAL INFOHAUS ADDRESSES

Messages to the addresses listed in Table 5-6 are processed automatically for InfoHaus buyers and sellers for various functions discussed at greater length in Chapter 8.

TABLE 5-6 *Special e-mail addresses for InfoHaus buyers and sellers.*

Function	Address
Submit InfoHaus transactions	`mimeserver@infohaus.com`
Subscribe to an InfoHaus periodical	`subscription@infohaus.com`
Search the InfoHaus database	`search@infohaus.com`
Retrieve a free or for-pay item from the InfoHaus	`retrieval@infohaus.com`
Purchase a for-pay item from the InfoHaus	`buy@infohaus.com`
Buy an item from the InfoHaus using its QuickBuy number	`quickbuy@infohaus.com`

Other Internet Resource Addresses

Redundancy through parallel Internet application interfaces is an important feature of the First Virtual system. If you

don't have access to the World Wide Web, you can still order information through e-mail from the InfoHaus service. The same goes for those with nongraphical Internet access: you can use ftp to retrieve files containing First Virtual documents, and you can use telnet to perform account creation and InfoHaus storefront management functions.

FTP

Much of the information that is available on the First Virtual World Wide Web server is also available through ftp. Table 5-7 includes some pointers to these documents and software.

TABLE 5-7 *ftp server addresses for First Virtual documents.*

Document	ftp Address
General information	`ftp.fv.com/pub/docs/`
User documentation	`ftp.fv.com/pub/docs/`
Technical specifications	`ftp.fv.com/pub/docs/`
Free software	`ftp.fv.com/pub/code/`
Browse InfoHaus storefronts	`ftp.infohaus.com/infohaus/by-seller/`
Upload information products	`ftp.infohaus.com/infohaus/incoming/`

TELNET

Telnet is an Internet application that allows interactive terminal sessions between a user and a remote computer. First Virtual uses telnet to provide account and transaction services, some of which are shown in Table 5-8. These functions will be discussed at greater length in Chapters 6 through 9.

TABLE 5-8 *Telnet addresses for First Virtual and InfoHaus functions.*

Function	Telnet Address
Apply for an account	`telnet.card.com`
Check validity of an account	`telnet.card.com`
Check status of your account	`telnet.card.com`
Initiate a transaction	`telnet.card.com`
Maintain your InfoHaus shop	`telnet.infohaus.com`
Add products to your shop	`telnet.infohaus.com`

First Virtual Users Mailing List

Mailing lists provide a valuable way to interact with a group of people sharing an interest. First Virtual maintains this mailing list for its users to discuss issues, problems, and other relevant topics. A good deal of its value comes from the participation of First Virtual's own staff in list discussions. This is a good forum for asking questions about the how, what, and why of buying and selling with First Virtual.

HOW TO SUBSCRIBE TO THE FV-USERS LIST

Subscribing to the FV-users list is easy. Just send an e-mail message to the address:

```
fv-users-request@fv.com
```

The subject of the message look like this:

```
subscribe user@company.com
```

Of course, you should enter your own e-mail address where it says "user@company.com"; there is no need for any text in the body of the message.

Once your subscription request is received, you will receive a message confirming that you have been subscribed with instructions on how to participate in and unsubscribe from the list.

UNSUBSCRIBING FROM THE FV-USERS LIST

You are likely at one time or another to want to unsubscribe from the FV-users list. Whether it is because you've advanced to a level beyond that of most list discussions, or because you just can't keep up with all your e-mail and need to reduce the load, it is vital that you unsubscribe yourself correctly. All too often, subscribers send their unsubscribe requests to the list rather than to the list server address. This results in everyone on the list getting a copy of the unsubscribe request, and it will not get you unsubscribed.

To unsubscribe, send an e-mail message to the address:

```
fv-users-request@fv.com
```

The subject of the message look like this:

```
unsubscribe user@company.com
```

Of course, you should enter your own e-mail address where it says "user@company.com"; there is no need for any text in the body of the message.

PARTICIPATING IN THE FV-USERS LIST

Newcomers to any mailing list are urged to attempt to listen for a while before posting; however, you should feel free to post any questions you have about First Virtual that you can't find answers for in the Web pages. To post a message to the list, send it to this address:

fv-users@fv.com

A descriptive subject is a good idea, as is a read-through of your message for errors and meaning. Remember, there may be a lot of people reading your message who know you only by what you submit to the list.

Reaching a Human

In the event that you can't find an answer to a question in the FAQs or elsewhere on the First Virtual Web site, you can send an e-mail message to one of the addresses listed in Table 5-9.

TABLE 5-9 *Reaching a human at First Virtual, using these e-mail addresses.*

Function	E-mail Address
Corporate Sales and Support	corp-sales@fv.com
Marketing	marketing@fv.com
Media/Press	media@fv.com
Web Site Administrator	webmaster@fv.com
Human Help	humanhelp@fv.com

You can also reach First Virtual by phone at the numbers listed in Table 5-10.

TABLE 5-10 *First Virtual telephone numbers.*

Function	Telephone number
General Information	+1 (800) 570-0003
International Press	+1 (307) 638-3688
Media Relations	+1 (619) 234-1300
Headquarters	+1 (619) 793-2700

For sending postal correspondence, First Virtual's headquarters are at the following address:

First Virtual Holdings Inc.
11975 El Camino Real
Suite 300
San Diego, CA 92130

PART THREE

BUYING AND SELLING WITH FIRST VIRTUAL

CHAPTER SIX

OPENING YOUR FIRST VIRTUAL ACCOUNT

Summary This chapter explains, first in general terms and then step by step, the process of starting a new First Virtual account, by e-mail, by World Wide Web and by telnet session. Also discussed are differences in setting up buyers' and sellers' accounts, how to retrieve the First Virtual terms and conditions documents, and how to get your payment information to First Virtual. Finally, other First Virtual account administration procedures are outlined.

Contents

THE FIRST VIRTUAL ACCOUNT PROCESS 152
Methods for Initial Contact 152
Providing Some Information Online . . . 153
Different Applications, Identical Followup 156
Providing Some Information Offline . . . 157
Buying and/or Selling 158
Waiving the Holding Period for Merchants 158

SIGNING UP BY WORLD WIDE WEB 159
Connecting to the First Virtual Web Site 159
Filling in the Application Form 160
What Follows 164

SIGNING UP BY TELNET 164
Connecting to the First Virtual Telnet Server 164
Answering Application Questions 167
Reviewing and Submitting the Application 170
What Follows 173

SIGNING UP BY E-MAIL 174
Getting the E-mail Application 174
Filling in the Application Form 174
Submitting the Application Form 180
What Follows 181

ACCOUNT VERIFICATION AND FOLLOWUP 181
E-mail Confirmation of Application . . . 182
Responding by Telephone for Buyers . . 186
Responding by Mail for Sellers 187
Finishing the Process 188

GETTING EXPRESS MERCHANT STATUS 188

ACCOUNT MAINTENANCE 190
Tracking Your Account Status 190
Making Changes 191

THE FIRST VIRTUAL ACCOUNT PROCESS

Setting up an account to buy or sell with First Virtual is a relatively simple matter — just send them your basic information over the Internet. Payment information for buyers, in the form of a credit card, is sent through an automated telephone interface. Payment information for sellers, in the form of a checking account, is carried in an actual check sent by postal mail to First Virtual. First Virtual offers three ways to get that basic information to them across the Internet: via World Wide Web, via interactive terminal session (telnet), and via e-mail.

Methods for Initial Contact

You can't just call First Virtual and start an account with them: at a bare minimum, you must be able to send and receive Internet e-mail. While you can do almost any First Virtual function using e-mail, most people will prefer a more interactive or graphical interface. Table 6-1 shows the Internet address information for each of the different methods of starting your account.

TABLE 6-1 *First Virtual account application addresses.*

Internet Application	Address
e-mail	apply@card.com
telnet	telnet.card.com
World Wide Web	http://www.fv.com/newacct/index.html

Applying for your First Virtual account over e-mail allows you the leisure of reviewing the application, and considering (and

checking) the answers. Using the First Virtual telnet server for an interactive terminal session is a good choice for those using character-based user interfaces, or for those who don't have access to World Wide Web browser software. Applying through the form on the First Virtual World Wide Web server may be the easiest route for those with graphical user interfaces and access to the World Wide Web.

No matter how you apply, you must provide the same information, described in the next section. After submitting an application in any form, potential First Virtual account holders proceed by e-mail, as described in the section after next.

Providing Some Information Online

All First Virtual account applicants are asked for the following information:

- Full-Name
- Email-Address
- Notification-CC
- Phone-Number
- Street-Address
- Street-Address-2
- City
- State
- Postal-Code
- Country
- ID-Choice
- Address-Redistribution
- MIME Capability

Not all of these are self-explanatory, and there are additional restrictions and requirements for the way some are entered in the application form. Clarifications on each of these follows.

- **Full-Name:** This is your First Virtual name; it does not necessarily have to be your actual legal name. It is simply the name by which other First Virtual customers refer to you (merchants use the buyers' names in transactions; buyers use merchants' names). You can use a corporate name, a pseudonym, or a nickname — as long as it is no longer than 30 characters.

- **Email-Address:** This must be your own, personal, Internet e-mail address — an address that you monitor regularly, of the form `username@domain.com`. The entire address must be no longer than 80 characters (including the @ sign).

- **Notification-CC:** All First Virtual e-mail transactions and notifications are sent automatically to your main e-mail address, but you have the option of having notification copies sent to an additional e-mail address. As with your main e-mail address, this address must be of the form `username@domain.com`, and the entire address must be no longer than 80 characters (including the @ sign). This might be an alternative personal e-mail address, or an accountant, or the finance department of your company. This is not a required option, and may be omitted.

- **Phone-Number:** A telephone number is necessary in the event that First Virtual must make a direct contact with the person making the application. It must be entered in standard international format, starting with a "+" sign, followed by country code, area code, and phone number. For example:

+1 212 555 1212

The phone number should in no case exceed 40 characters.

- **Street-Address and Street-Address2:** These are for the billing address associated with the credit card account you will be using to pay for First Virtual purchases (or the mailing address associated with the checking account to be used for accepting payments from First Virtual sales). This should include the street number, street name, and apartment or suite number. Neither of these fields can exceed 30 characters, and Street-Address2 should be used only if the street address is longer than that.

- **City:** The name of your city or locality, maximum of 30 characters in length.

- **State:** The name of your state, province, or region, in no more than 30 characters.

- **Postal-Code:** Your postal delivery code — for example, ZIP code in the United States. No more than 9 characters.

- **Country:** Use a two-letter country code to indicate your country (for example, US for the United States or CA for Canada).

- **PIN-Choice:** PIN stands for Personal Identification Name here, and First Virtual recommends you choose an easy-to-remember name or phrase — but not your name, or a password to some other system (or any other secret information), or anything that might be easy to guess. The PIN must be at least 8 characters long, but no longer than 24 characters (letters or numbers). When the account is activated, First Virtual adds a 4-letter word to the beginning

of your chosen PIN to create your VirtualPIN. The VirtualPIN is what you use to initiate a First Virtual purchase, so you would not want to make it public knowledge (though it is not, strictly speaking, a secret).

- **Address-Redistribution:**. On occasion, First Virtual customers may receive e-mail about products that seem to match the customer's interests, based on previous purchases. First Virtual does not sell customer records or e-mail addresses as mailing lists, but they may at some point do direct marketing in this way (perhaps in conjunction with third parties). Applicants may choose not to have their e-mail addresses used in this way by refusing this option.

- **MIME-Capability:** If you can accept MIME (Multipurpose Internet Mail Extensions) e-mail, choose this option. MIME mail from First Virtual may be easier to deal with, but you should choose this option only if you are certain your e-mail reader can handle MIME.

Different Applications, Identical Followup

Whether you submit your application by e-mail, through an interactive telnet session, or by filling out the World Wide Web application form, First Virtual responds to your application with an e-mail confirmation, as shown in Figure 6-1. The only account information included in this reply is your name, e-mail address, and your chosen PIN. This message also includes very specific instructions for how to go about activating your account.

In addition to those instructions, the message includes an e-mail address for additional information about First Virtual, as well as explanations of account fees. The entire message is

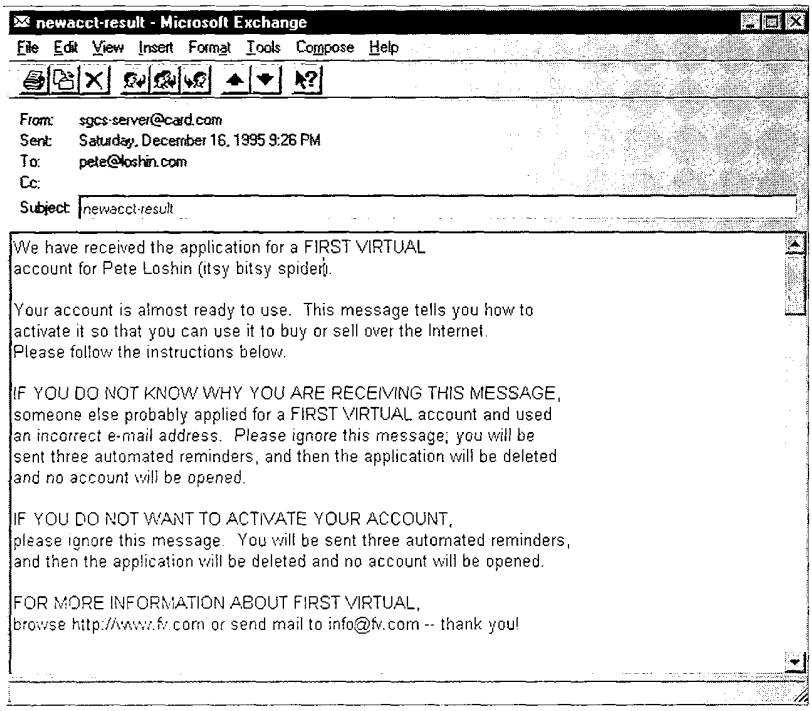


FIGURE 6-1 *The first portion of the e-mail confirmation First Virtual sends in response to your application. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

reproduced later in this chapter, in the "Account Verification and Followup" section.

Providing Some Information Offline

The First Virtual account is activated by providing First Virtual with payment information: a credit card number for paying out for purchases and/or a checking account for paying in for sales made through the system. Detailed instructions are provided in the "Account Verification and Followup" section later in this chapter, explaining the process of entering a credit card number and First Virtual account application number by

telephone and sending in a check to cover the costs of setting up a seller's account.

Buying and/or Selling

You can open a First Virtual account and enable it for buying only, for selling only, or for both buying and selling. If you wish only to make purchases, you must provide First Virtual with a credit card number (and accept a $2.00 charge on that account to cover costs). If you wish only to make sales through First Virtual, you must provide First Virtual with a check (for $10 to cover costs) drawn on the account to which you want sales proceeds to be deposited.

Part of the attraction of the First Virtual system is the ease with which one can become a seller as well as a buyer. Prospective Internet merchants need not apply for a special merchant account at a bank — all they have to do is write a check. After that, all proceeds from First Virtual sales (minus transaction costs and fees) are deposited regularly into that checking account.

Some merchants will prefer to enable their accounts for sales only, although if you plan to use the InfoHaus service to sell your products, you have to provide First Virtual with a way to bill for data storage fees. Alternatively, you may open two separate accounts, one for selling and one for buying, to take care of the InfoHaus fees.

Waiving the Holding Period for Merchants

Up until the start of 1996, all First Virtual merchants were subjected to a holding period of 91 days — proceeds of any sales made through First Virtual were held for three months to

avoid potential for losses reported by consumers after checking their credit card bills. This was a sore point for many merchants who had to deliver their goods immediately but who couldn't get paid for three months, causing cash flow issues for them. However, starting early in 1996, First Virtual has made it possible for merchants to make special applications for a waiver of this holding period.

SIGNING UP BY WORLD WIDE WEB

Considering that the World Wide Web has been, perhaps, the most compelling reason for most new users to get connected to the Internet, using it as an entry point for electronic commerce is only logical. First Virtual provides a Web form application that is easily filled out and submitted through just about any World Wide Web browser.

Connecting to the First Virtual Web Site

The First Virtual Web server address is:

```
http://www.fv.com
```

You can enter this address directly in your Web browser, and then cruise through the First Virtual Web pages to arrive at the application form; you can also go directly to the application form at the Web address:

```
http://www.fv.com/newacct/index.html
```

This page includes the basic instructions for applying for a First Virtual account, and scrolls down through several screens full of information. The top of the page is shown in Figure 6-2. In addition to links to more details about First Virtual, the terms

and conditions of a First Virtual account, and details about special promotions, there are links that can be clicked on to open the account through an e-mail message or a telnet session.

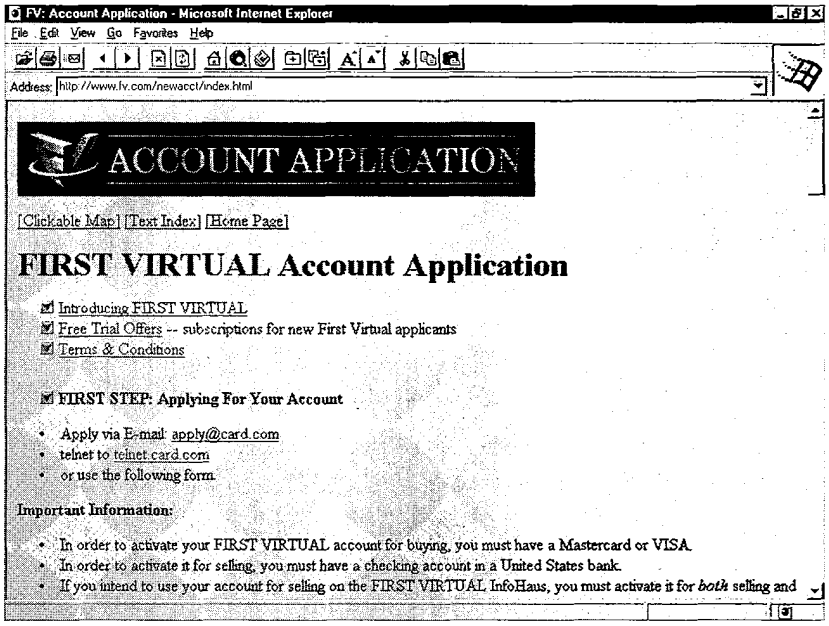


FIGURE 6-2 *The top of the First Virtual World Wide Web application form. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

Sharp-eyed readers will notice that not all questions are exactly the same in the various application methods. Readers are also likely to find that the applications they encounter may differ slightly from those displayed here: this is to be expected as the different forms and formats are modified over time.

Filling in the Application Form

Scrolling down the page reveals more instructions, as well as the first fields to fill in on the account application, as shown in

Figure 6-3. Each of the pieces of information discussed in the first section of this chapter has its own field on the form. Where there are special instructions (as with the telephone number field), they are spelled out on the form. More information about each field — for example, why it is required, or what format it must take — can be retrieved by clicking on the field name.

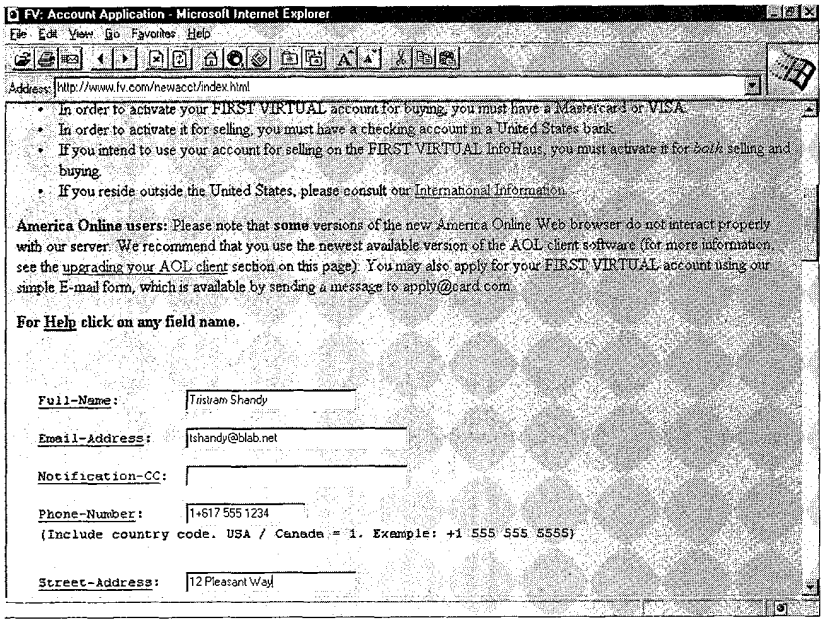


FIGURE 6-3 *The first entry fields in the First Virtual World Wide Web account application form. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

Paging further down reveals more fields, as shown in Figure 6-4. Again, the form includes fields for entering application information as described earlier in this chapter. When entering country code, you must use a standard two-character code — if you don't know the correct code, you can click on the field name (Country) for explanation of that field, and then click on another link to a list of valid country codes.

Two fields, the options for address redistribution and MIME e-mail, use Yes/No pull-down choice fields.

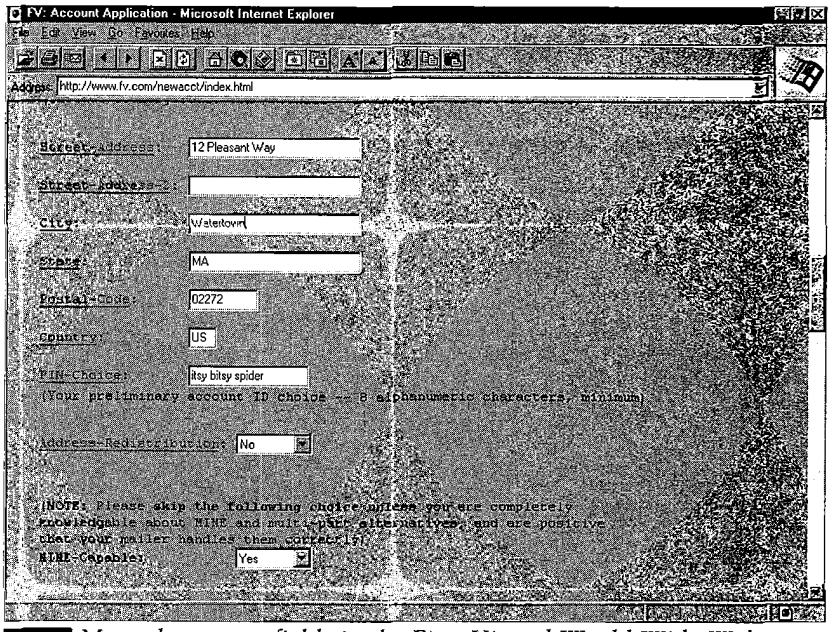


FIGURE 6-4 *More data entry fields in the First Virtual World Wide Web account application form. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

Page down once more for the last application questions, as shown in Figure 6-5. There may be special offers available to new First Virtual account holders; in any case, the applicant is urged to check all entries (particularly the e-mail address) for accuracy and completeness, and the form can be submitted by clicking on the "SUBMIT FORM and FREE OFFERS request!" button.

There is still more information on the application form page, as shown in Figure 6-6 — in particular, a description of what comes next in the application process and how to activate your account for buying and/or selling (described in the next section).

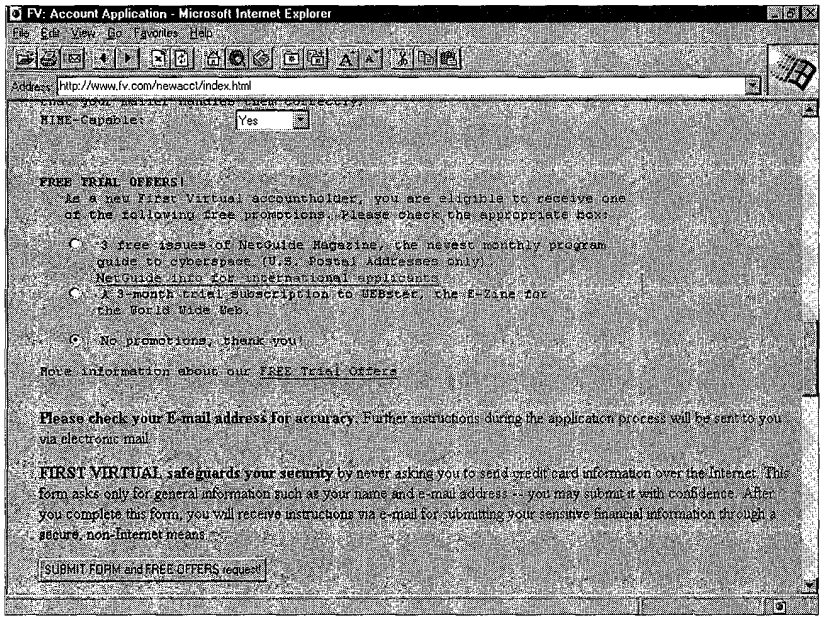


FIGURE 6-5 *Finishing up the First Virtual World Wide Web account application form. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

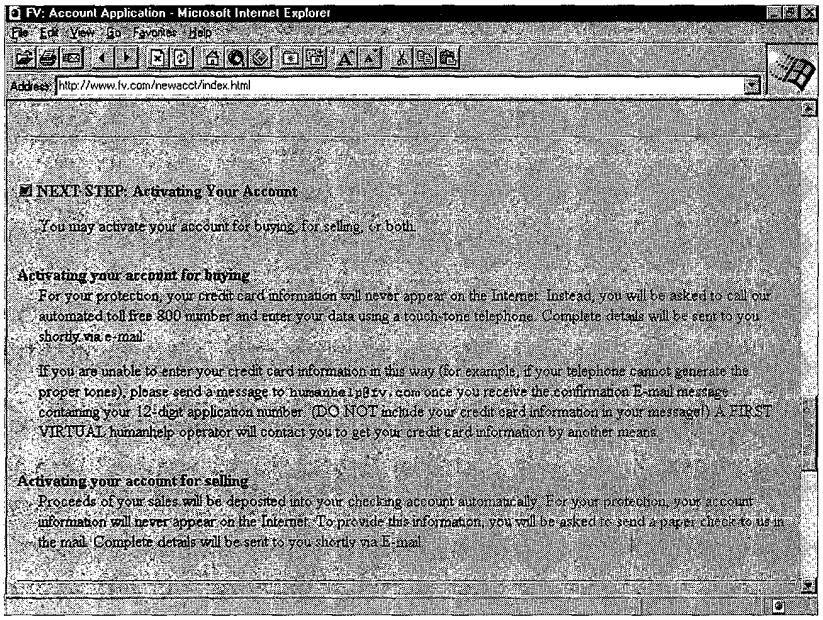


FIGURE 6-6 *The First Virtual World Wide Web account application form includes instructions for the next step. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

What Follows...

Once your application is received, notification is sent to your chosen e-mail address; details on the contents of that message are provided in the "Account Verification and Followup" section later in this chapter. As discussed earlier, you can then enable your account for buying, for selling, or for both.

You are also urged to get a copy of the "fineprint" documents: the terms and conditions of your First Virtual account. First Virtual recommends that you do not initiate any transactions through their service before you review and accept these terms and conditions. The "Account Verification and Followup" section provides pointers for locating these documents (for buyers, for sellers, and for InfoHaus merchants).

SIGNING UP BY TELNET

Telnet is an Internet application for remote terminal sessions. The person using the telnet client connects to a remote host (running telnet server software) and then is able to interact with that remote host as if connected by a terminal. For those users who have access to the Internet, but who do not have access to World Wide Web browser software, or who share access to the Internet through a multiuser system, applying for a First Virtual account by a telnet session has advantages.

Connecting to the First Virtual Telnet Server

The first step is to initiate a telnet session with the First Virtual telnet server. The way this works depends on how

your version of telnet works, but in any case you somehow enter the name of the remote host you want to start a session with:

```
telnet.card.com
```

The next step, once the connection is opened, is to log in. To apply for an account, enter the user ID:

```
fv
```

No password is required. The opening screen is shown in Figure 6-7. The first prompt asks if you are running an X11 window server. Unless you are logging on from a Unix workstation, you are not likely to be running that software — most people using personal computers will answer "N" (for "no") to this prompt.

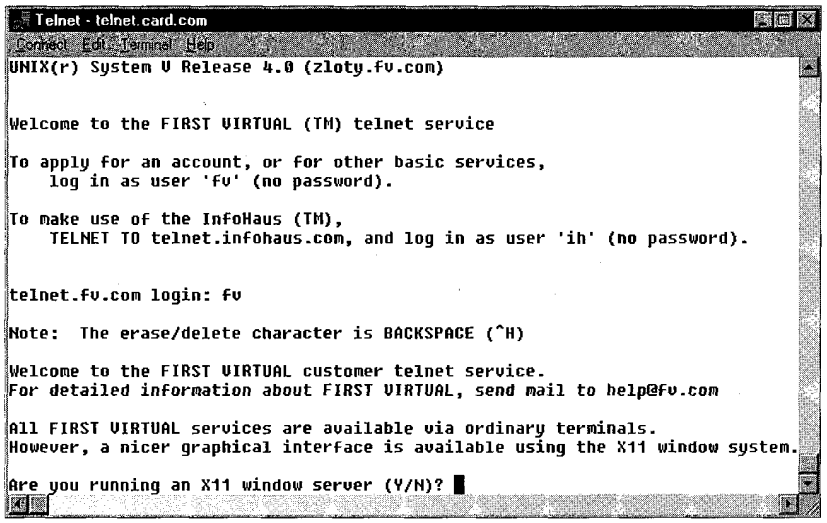


FIGURE 6-7 *The opening screen when initiating a telnet connection to the First Virtual server. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

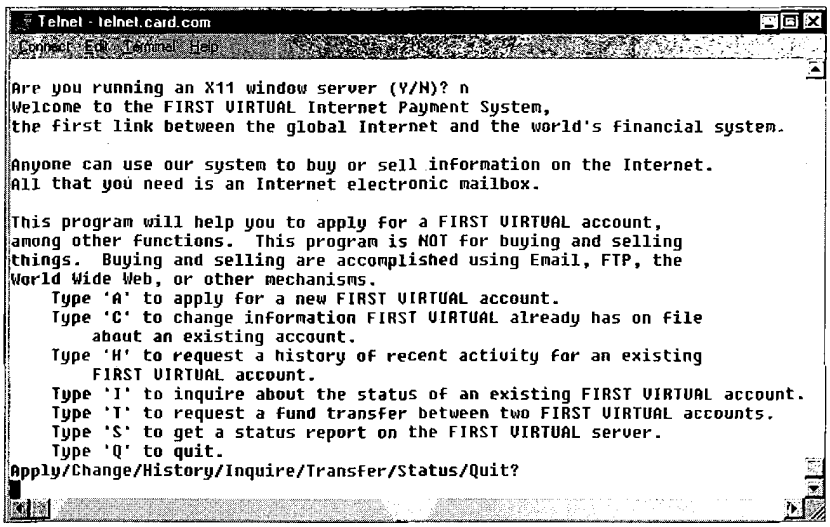


FIGURE 6-8 *Choosing a function from the First Virtual telnet server. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The telnet interface can be used for more than just applying for a new account, and details on the other options can be found in the last section of this chapter. These options are displayed in Figure 6-8 and include:

- Applying for a new account.
- Changing account information for an existing account (e.g., change of address).
- Getting historical activity for a specific account.
- Inquiring about the status of an existing account (e.g., is it a valid account).
- Transferring funds between one First Virtual account and another one (e.g., to make a payment).
- Receiving a report on the status of the First Virtual server (e.g., is the server up and running).

For now, type the letter "A" (for "apply") and press the enter key to proceed.

Answering Application Questions

As with the other methods of applying for a First Virtual account, the telnet server provides explanatory material while requesting customer information. The same information listed in the first part of this chapter is collected interactively; for more details about each item, you are referred there (see also the illustrations provided here for details). As shown in Figure 6-9, the first question asks for your full name, after providing a brief explanation of the First Virtual system.

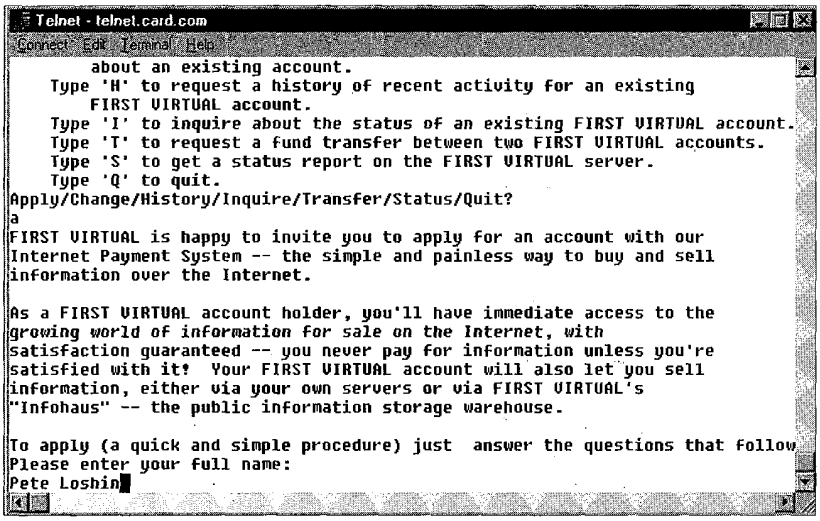


FIGURE 6-9 *Entering your full name while applying for a First Virtual account. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The next prompt is for your e-mail address. Further notes or comments about e-mail addresses may be included, as in Figure 6-10, which in this instance explains what to do if your e-mail gateway does not properly forward messages from First Virtual. If you are unsure of your e-mail gateway, you can try finishing the application normally. If you get a response from First Virtual, you can assume your gateway

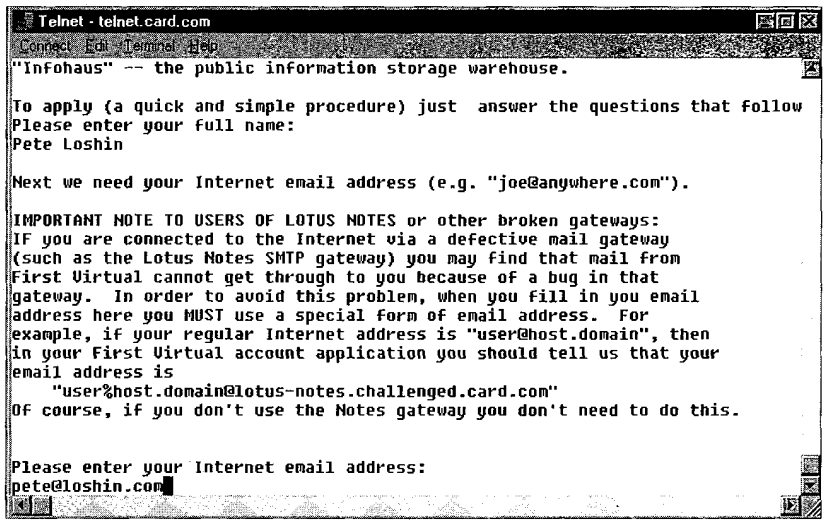


FIGURE 6-10 *Entering your e-mail address while applying for a First Virtual account. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

operates normally. Otherwise, you should check with your network or e-mail administrator.

The next few prompts, as shown in Figure 6-11, are for your address and telephone number. These are self-explanatory, with only two things to watch out for: don't enter your country telephone code, and don't enter your city name on the second line of your street address.

The next item requires a bit more thought: the account ID, or PIN (as described earlier). PINs must be longer than 8 characters, but shorter than 30 characters; the best ones are easy to remember, but not easy to associate with the owner. Figure 6-12 shows a sample account ID, "itsy bitsy spider," though punctuation or spaces between words are ignored by the processing system. Also shown are the prompts for the default currency (U.S. dollars) and default transaction language (EN, or English).

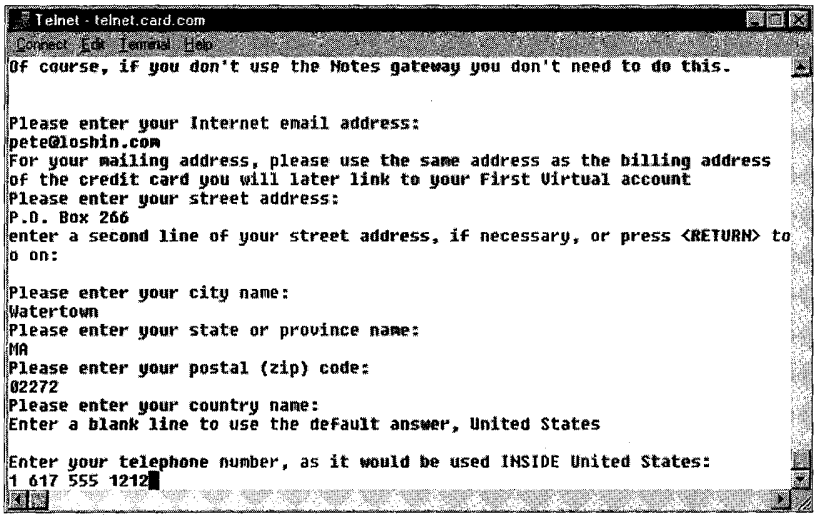


FIGURE 6-11 *Entering your address and telephone number while applying for a First Virtual account. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

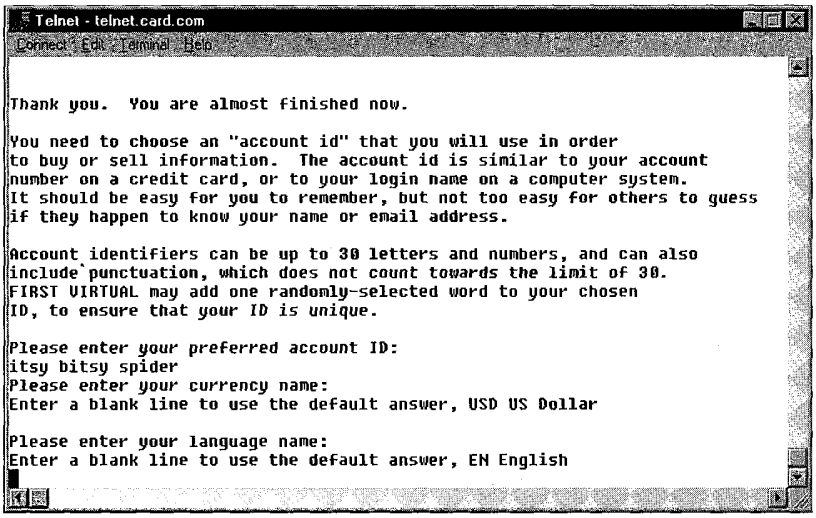


FIGURE 6-12 *Entering your personal identification name, and choosing default currency and language, while applying for a First Virtual account by telnet. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The last prompts for account information are shown in Figure 6-13 and include the option for an e-mail address to send copies of First Virtual notifications, and the option to withhold your e-mail addresses from First Virtual mailing lists.

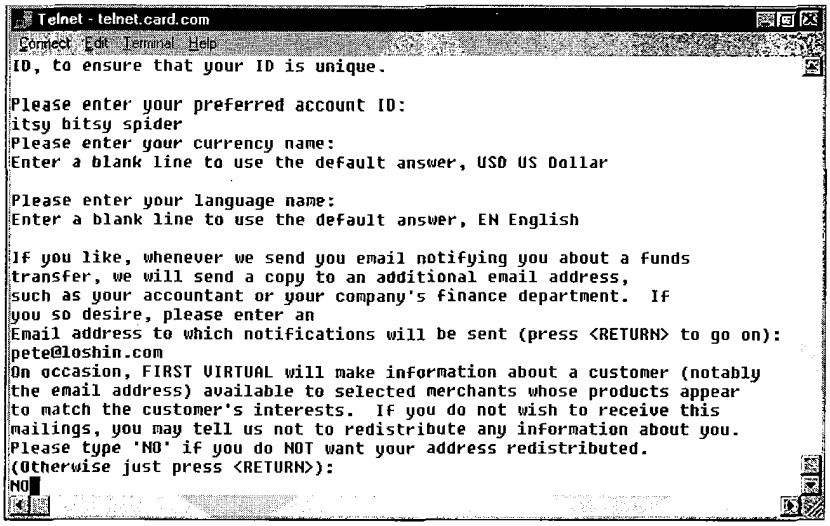


FIGURE 6-13 *Entering an additional e-mail address for notification, and choosing to be excluded from First Virtual merchant mailings. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

When all account information prompts have been completed, you can move on to the next step, reviewing and submitting your application.

As mentioned earlier, not all questions are exactly the same in different application methods. Readers are also likely to find that the applications they encounter may differ slightly from those displayed here: this is to be expected, as the different forms and formats are modified over time.

Reviewing and Submitting the Application

Once you have finished answering all the application questions, the remote system displays all your answers, as shown in

Figure 6-14. If the answers are all correct, you simply type "S" (for "send") to have your application submitted. If you need to make any changes, type "E" (for "edit") and follow instructions for making corrections. Of course, if you don't want to continue, type "Q" (for "quit") to terminate the telnet session.

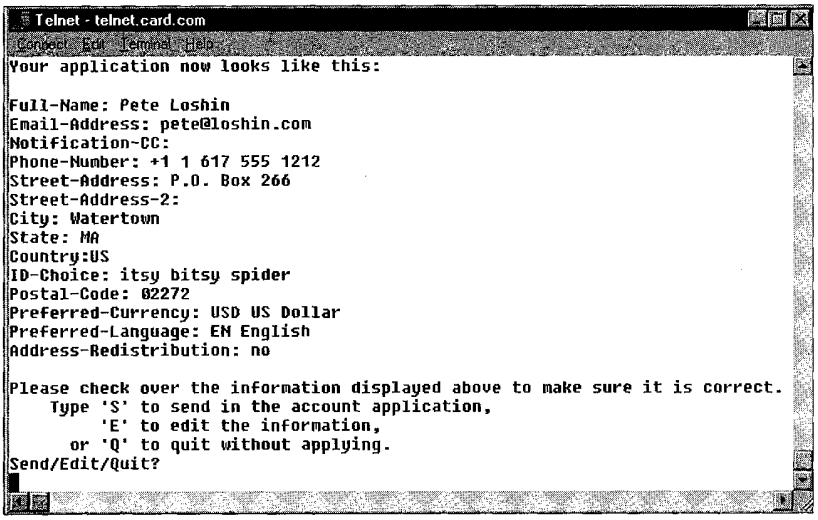


FIGURE 6-14 *Reviewing your answers to the First Virtual telnet application prompts. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

After you have chosen to send your application to First Virtual, more information appears, explaining how to get copies of the terms and conditions of your First Virtual account, as shown in Figure 6-15.

One last screen contains the exact contents of the application just submitted. You may wish to print this out for future reference; an example is shown in Figure 6-16.

Once the application process is complete, a final note reminding you to get the "fineprint" (terms and conditions) document is followed by the same menu of choices that was provided at the beginning of the telnet session, as shown in Figure 6-17.

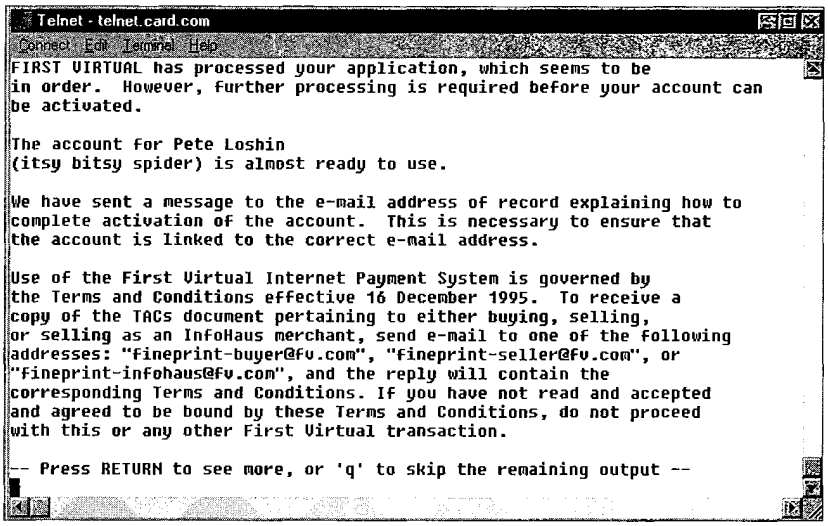


FIGURE 6-15 *After submitting an application, the First Virtual server explains what comes next. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

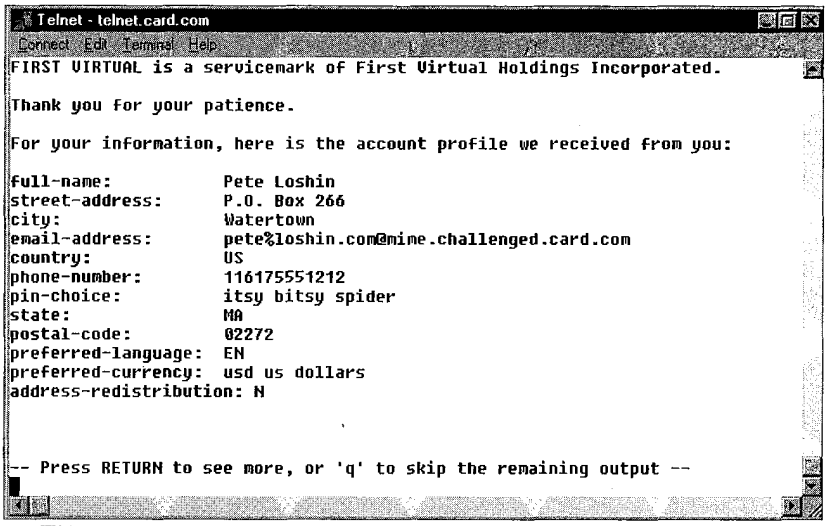


FIGURE 6-16 *Reviewing the just-submitted account application information via telnet. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

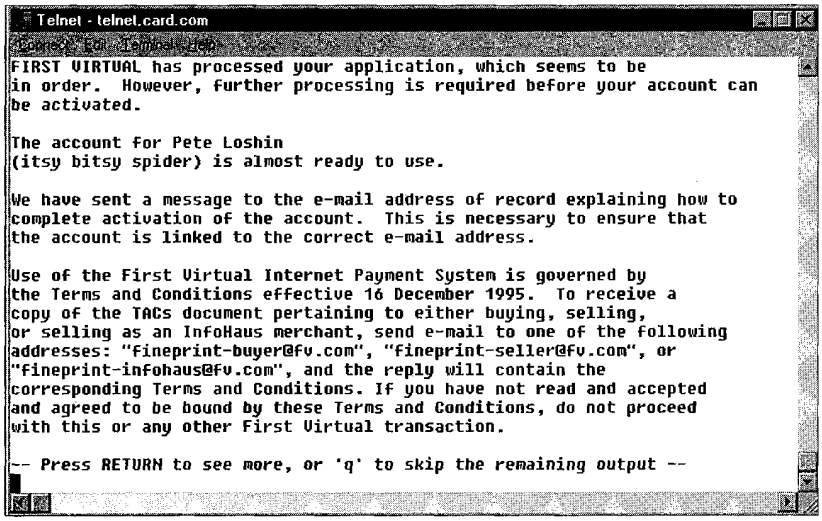


FIGURE 6.17 *Once the application is complete, you can do other First Virtual functions. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

What Follows...

Once your application is received, notification is sent to your chosen e-mail address; details on the contents of that message are provided in the "Account Verification and Followup" section later in this chapter. As discussed earlier, you can then enable your account for buying, for selling, or for both.

You are also urged to get a copy of the "fineprint" documents: the terms and conditions of your First Virtual account. First Virtual recommends that you do not initiate any transaction through their service before reviewing and accepting these terms and conditions. The "Account Verification and Followup" section provides pointers for locating these documents (for buyers, for sellers, and for InfoHaus merchants).

SIGNING UP BY E-MAIL

The lowest common denominator of Internet access, e-mail is the basic unit of communication for First Virtual. Just about any First Virtual function, from buying to selling to managing an InfoHaus shop, can be taken care of through an e-mail message. Applying for a First Virtual account by e-mail is a simple matter of sending off a request for an application, filling it out, and following instructions.

Getting the E-mail Application

To get an e-mail application for a First Virtual account, nothing more than an e-mail message to the following address is required:

```
apply@card.com
```

It is not necessary to put anything in the body of the message you send, nor is a subject required. This address responds automatically to messages it receives by sending out a text-only application form in an e-mail message. The e-mail version of the application is shown in Figures 6-18 through 6-22, and discussed in the next section.

Filling in the Application Form

The best way to proceed is first to read the application form. Further instructions are provided in the body of the application on lines that begin with the "#: " characters (the pound sign, colon, and space). These lines are ignored by the system that receives your application. Each line that is processed contains a field name (for example, "Full-Name") followed by a colon.

You "fill out" the form by adding your information to these lines. Each response should be on the same, single, line following the field names; don't use the Enter key to break a line. Your e-mail reader may wrap a line if it extends beyond the default page width, but as long as you don't explicitly add a carriage return, your application should be processed correctly.

The values to be entered are described in the text of the application message (in Figures 6-18 through 6-22 below), as well as earlier in this chapter. It is especially important to proofread your e-mail application before submitting it, so as to avoid errors that may delay your application.

```
Thank you for requesting an application. To apply, please reply to
this message (or send e-mail to "newacct@card.com").
In your reply, simply place everything between the two lines
that say "===CUT HERE===" into the body of your reply message.

Then, fill in all the information requested before sending the
message.
Please keep each of your answers on the single lines which do
not have "#: " at the beginning.

After we receive your application, we will send you e-mail asking you
to
use a touch-tone phone to enter your VISA or MasterCard number to
activate your account for buying. At the present, we support only
these
two payment methods; so, if you cannot use either, we will not be able
to
activate your account.

You should also send e-mail to the address "fineprint@fv.com" to
receive the latest terms and conditions governing your use of
First Virtual's Internet Payment System.

Thank you for your cooperation.
```

FIGURE 6-18 *The first part of the e-mail version of the First Virtual application. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The first part of the e-mail version of the application form, shown in Figure 6-18, simply explains what to do with the

form: cut out the portion of the message appearing between the lines that say "===CUT HERE===" and paste it into your response. This response can be sent either as a reply to the message containing the application, or to the address:

```
newacct@card.com
```

The applicant is also urged here to get a copy of the terms and conditions of the First Virtual account.

```
==================CUT HERE==================
#:
#: FULL NAME  - Please enter your full name, by which you will
#: generally be described to other First Virtual customers.
#:
#: e.g.,
#:
#: Full-Name: Joe Internaut
#:
#: This may be a corporate identity, or even a nickname, but it should
#: be recognizable and memorable. It may be no more than 30
#: characters.
#:
Full-Name:
#:
#:
#: E-MAIL ADDRESS  - Please enter your Internet e-mail address.
#:
#: e.g.,
#:
#: Email-Address: internaut@cyberspace.fv.com
#:
#: This address may not exceed 80 characters including
#: the "@" sign.
#:
Email-Address:
#:
```

FIGURE 6-19 *Entering your full name and e-mail address in the e-mail version of the First Virtual account application. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The next part of the account application, shown in Figure 6-19, is for entering your name and e-mail address. Note that the

explanatory material is preceded by the symbols "#:" while the parts that you must fill out begin with the name of the information item you need to provide. The next section, shown in Figure 6-20, is for filling in an e-mail address for an extra notification address and your telephone number.

```
#:
#: NOTIFICATION -CC  - If you like, whenever we notify you
#: by e-mail about a funds transfer, we will send
#: a copy to an additional e-mail address, such
#: as your accountant or your company's finance department. If
#: interested,enter such an e-mail address below. If you have no
#: need for additional e-mail addresses to get your First Virtual
mail,
#: then leave the below entry blank.
#:
Notification-CC:
#:
#:
#: PHONE NUMBER  - Please enter your phone number using
#: the international format, i.e.,
#:
#: +country-code area-code local-number
#:
#: The country code for Canada and the US is "1", so an example
#: might be
#:
#: Phone-Number: +1 201 555 1212
#:
#: It is very important that you enter this number correctly, since we
#: may have to call you in order to finish processing your
#: application.
#:
Phone-Number:
#:
```

FIGURE 6-20 *Entering an extra notification address and your telephone number in the e-mail version of the First Virtual account application. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The next section is for your address, including street and number, city, state or province, postal code and country, as shown in Figure 6-21.

```
#:
#: STREET ADDRESS  - Please enter your street address, including
#: any necessary apartment numbers, etc.. Do NOT include town,
#: state, country, or postal code.
#:
#: e.g.,
#:
#: Street-Address: 1776 K Street, NW
#:
#: Note that this should be the same as the billing address of the
#: credit card which you will later link to your First Virtual
#: account. This may be no more than 30 characters per line.
#:
Street-Address:
Street-Address-2:
#:
#:
#: CITY  - Please enter the name of your city or locality, in no
#: more than 30 characters.
#:
#: e.g.,
#:
#: City: Washington
#:
City:
#:
#:
#: STATE  - Please enter your state, province, or other relevant
political
#: subunit of your country, in no more than 30 characters.
#:
#: e.g.,
#:
#: State: DC
#:
State:
#:
#:
#: POSTAL CODE  - Please enter your postal code (ZIP code in the US).
#:
#: e.g.,
#:
#: Postal-Code: 20006
#:
Postal-Code:
#:
#:
#: COUNTRY  - Please enter the two-letter code for your country
#: (if you don't know the two-letter code, enter your country's
#: name and we'll try and figure it out).
#:
#: e.g.,
#:
#: Country: US
#:
Country:
#:
```

FIGURE 6-21 *Entering complete address data in the e-mail version of the First Virtual account application. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

Figure 6-22 shows the last section of the message, where you are asked for a personal identification name (PIN) for the account ID. PINs must be longer than 8 characters but shorter than 30 characters; the best ones are easy to remember, but not easy to associate with the owner. Punctuation or spaces between words are ignored by the processing system. Also here, you state whether you wish to accept distributions from First Virtual merchants, and whether your e-mail reader is MIME-capable.

```
#:
#: PIN-CHOICE  - Please enter a preliminary choice for your account
#: ID. It must be between 8 and 24 characters in length made up of
#: letters and/or numbers. (Spaces and punctuation will be ignored.)
#:
#: e.g.,
#:
#: PIN-Choice: something you choose
#:
#: This identifier should NOT match your Full-Name. It should be
#: something that is easy for you to type and remember, but relatively
#: hard for other people to guess; it should NOT be the same as
#: your password on any computer system, or any other secret
#: information (such as the PIN for a bank card).
#:
#: This will NOT be your account ID.
#:
#: FIRST VIRTUAL will create your final account ID, called a
#: VirtualPIN, by adding a 4-letter word to the beginning of this PIN
#: Choice. You will be sent your VirtualPIN via e-mail. When making
#: purchases, you must use your VirtualPIN as your account ID, NOT
#: the PIN-choice you specify here.
#:
PIN-Choice:
#:
#:
#: REDISTRIBUTION  - From time to time we make selected
#: customers' e-mail addresses available to merchants whose products
#: appear to match the customers' interests. If you do not wish us to
#: redistribute your e-mail address for this purpose,
#: please remove the "#: " at the
#: beginning of the next line (the first three characters).
#: Address-Redistribution: no
#:
#:
#: MIME CAPABILITY  - Please skip the following choice unless you are
#: completely knowledgeable about MIME and are positive that your mailer
#: handles it correctly. If your mailer is MIME-capable, then you can
```

```
#: receive your e-mail from First Virtual in MIME format. Many
messages
#: that we send you in MIME form will be multipart/alternative and
have
#: non-text attachments, so if your mailer is not set up to receive
MIME
#: mail but you tell us it is, your mailer will not be able to display
#: the mail we send it.
#:
#: If you are ABSOLUTELY POSITIVE that your mailer can accept MIME
#: messages, then remove the "#: " on the next line.
#: MIME-Capable: Yes
#:
==================CUT HERE==================


Please ignore anything that appears after this line.
```

FIGURE 6-22 *The e-mail version of the First Virtual application form. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

As mentioned earlier, not all questions are exactly the same between different application methods. You are also likely to find that the applications you encounter differ slightly from those displayed here. This is to be expected as the different forms and formats are modified over time.

Submitting the Application Form

You must send your filled-out application to First Virtual. One way is to just send it as a reply to the original application message from First Virtual. In any case it must be sent to this address:

```
newacct@card.com
```

The message will be processed by the First Virtual computer at the other end, and the same process described previously will begin — you will get a notification from First Virtual that your account is ready to be activated.

What Follows...

Once your application is received, notification is sent to your chosen e-mail address; details on the contents of that message are provided in the "Account Verification and Followup" section later in this chapter. As discussed earlier, you can then enable your account for buying, for selling, or for both.

You are also urged to get a copy of the "fineprint" documents: the terms and conditions of your First Virtual account. First Virtual recommends that you do not initiate any transactions through their service before reviewing and accepting these terms and conditions. The next section provides pointers for locating these documents (for buyers, for sellers, and for InfoHaus merchants).

ACCOUNT VERIFICATION AND FOLLOWUP

The first thing that happens after submitting your First Virtual account application, assuming that your application is in order, is that you receive an e-mail message at your main e-mail account. The start of this message was shown in Figure 6-01; the entire message is reviewed completely in this section.

If you choose to enable your account, you will either telephone First Virtual and enter your credit card number and your First Virtual application number to enable your account for buying, or mail a check with your application number in the Memo line to First Virtual to enable your account for selling. First Virtual sends this notification message three times, to make sure that it gets through to you despite any transient faults in your e-mail account or intervening Internet services. If you choose not to activate your account for some reason, you can simply ignore the notification messages. If no

response is received, First Virtual cancels the application — so if you apply for an account and don't check your e-mail for a week or so, you will have to reapply.

However, you should also be sure to get a copy of the appropriate terms and conditions documents before continuing. Pointers to these documents are provided later in this section.

E-mail Confirmation of Application

Depending on variables such as the current loads on the relevant systems, you should get an e-mail confirmation from First Virtual anywhere from minutes to hours after submitting your application. The first part of this confirmation message will look something like Figure 6-23; this introduction explains what the message is about, and why it is being sent.

```
We have received the application for a FIRST VIRTUAL
account for Pete Loshin (itsy bitsy spider).

Your account is almost ready to use. This message tells you how to
activate it so that you can use it to buy or sell over the Internet.
Please follow the instructions below.

IF YOU DO NOT KNOW WHY YOU ARE RECEIVING THIS MESSAGE,
someone else probably applied for a FIRST VIRTUAL account and used
an incorrect e-mail address. Please ignore this message; you will be
sent three automated reminders, and then the application will be
deleted
and no account will be opened.

IF YOU DO NOT WANT TO ACTIVATE YOUR ACCOUNT,
please ignore this message. You will be sent three automated
reminders,
and then the application will be deleted and no account will be
opened.

FOR MORE INFORMATION ABOUT FIRST VIRTUAL,
browse http://www.fv.com or send mail to info@fv.com  - thank you!
```

FIGURE 6-23 *The first section of the First Virtual application confirmation message. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The next section of the message, shown in Figure 6-24, explains how to activate your account for purchases. A toll-free number is provided for calling within the United States, and another number is provided for international calling. This section explains that it is necessary to transmit a credit card number over a telephone link rather than over the Internet. It explains the procedure, as well as the $2.00 charge for opening a First Virtual account.

This section also explains what happens after you enter your credit card number and application number into the automated telephone system. You should receive a further confirmation message within a day indicating that your application has been completely processed.

```
ACTIVATING YOUR ACCOUNT FOR THE PURCHASE OF INFORMATION

First, we need to know how to bill you when necessary.

To avoid exposing your credit card number on the Internet, you need to
call us on the telephone and enter the number of the credit card you
want
us to use to pay for your purchases.

To activate your account for the purchase of information, please use a
touch-tone phone to call

    from inside the US: (800) 383-8332

    from outside the US: +1 770 333-0500

Prior to calling, please be ready to supply:

    - the number and expiration date of a VISA or MasterCard
    credit card that you are authorized to use.
    (We will charge your credit card a set-up fee of $2.00,
    two US dollars, to recover our costs for establishing
    your account. Each time you need to update this information,
    e.g., when your credit card expires and you get a new one,
    you'll automatically be asked to update this information,
    which will again cost $2.00  - so, if you have several credit
    cards, you should consider using the one with the latest
    expiration date.)

    - your application number, 9606-9999-9999
    (This application number is used for this phone call
```

```
    and for when you activate your account for the sale
    of information, and may be discarded afterwards.
    This number is NOT your First Virtual account
    identifier, and may not be used to buy or sell
    information.)

An automated system will ask you for this information.

Your account will then be activated for buying information over the
Internet  - we'll bill your credit card at regular intervals for the
purchases that you approve via e-mail.

    PLEASE NOTE: We will send you e-mail indicating that your
    account is operational, most likely within two hours after
    you have called us. But due to technical factors beyond
    our control, account activation can take as long as 24 hours.
    We are working on reducing this delay, but ask you to be
    patient if your account is not activated immediately.

    If you have waited 24 hours and have still not received
    an e-mail confirmation, you can check the status of your
    application by mailing findappl@card.com with your
    application number, 9606-9999-9999, in the subject heading.

You may later fully activate your account to sell information over the
Internet.
```

FIGURE 6-24 *The second section of the First Virtual application confirmation message, explaining how to enable the account for buying. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The next section of the message explains how to activate your account for selling only, as shown in Figure 6-25. The charge for setting up a seller's account is $10.00 and must be paid by a check drawn on the account to which the proceeds of sales are to be deposited. The check is to be made out to "First Virtual Holdings Incorporated" and sent to address listed in the text of the message.

This section also explains that processing of the seller's account should take no more than ten days. It gives instructions on how to determine whether the check was received at First Virtual.

```
ACTIVATING YOUR ACCOUNT FOR SELLING ONLY

Alternatively, if you do not wish to buy information over the
Internet, you may activate your account solely for the sale of
information. To do this, please choose a US checking account into
which you would like us to deposit your funds. Then, write out a
check on that account for $10.00 (ten US dollars, to cover our paper
processing expenses), made payable to:

    First Virtual Holdings Incorporated

Please write your application number on the check, in the "memo"
section, to ensure that the correct First Virtual (TM) account is
linked to your checking account. Your application number is:

    9606-9999-9999

Then, please mail the check to:

    First Virtual Holdings Incorporated
    POB 168004
    Rocky River, Ohio 44116

The banking information on the check will tell us how to pay you for
the information sales you make over the Internet!

    PLEASE NOTE: You will receive an email message indicating your
    account is operational within 10 days. If you do not hear from us,
    your mail may have been lost. By mailing findappl@card.com with
    your application number, 9606-9999-9999, in the subject heading,
    you will hear back as to the status of your application.
```

FIGURE 6-25 *The third section of the First Virtual application confirmation message, explaining how to enable the account for selling. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The last part of this message, shown in Figure 6-26, explains how to get copies of the First Virtual account terms and conditions documents, outlining how the account may be used.

```
Use of the First Virtual Internet Payment System is governed by
the Terms and Conditions effective 16 December 1995. To receive a
copy of the TACs document pertaining to either buying, selling,
or selling as an InfoHaus merchant, send e-mail to one of the
following
addresses: "fineprint-buyer@fv.com", "fineprint-seller@fv.com", or
```

```
"fineprint-infohaus@fv.com", and the reply will contain the
corresponding Terms and Conditions. If you have not read and accepted
and agreed to be bound by these Terms and Conditions, do not proceed
with this or any other First Virtual transaction.

FIRST VIRTUAL is a servicemark of First Virtual Holdings Incorporated.

Thank you for your patience.

Please ignore anything that appears after this line.
```

FIGURE 6-26 *The last section of the First Virtual application confirmation message, explaining how to get the First Virtual terms and conditions documents. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

Responding by Telephone for Buyers

As with all the other systems for applying for a First Virtual account, the telephone system is automated and includes complete instructions. You need a touch-tone phone, as well as your application number (included in your application confirmation message) and a valid Visa or MasterCard account number and expiration date.

Dial the number listed in your account application confirmation message any time of day or night, and an automated system responds. The first part of the message explains that you need to be sure your application was completed, and that if you have not done so, you should send e-mail to the address:

```
apply@card.com
```

To continue, you are prompted to press "1." The next prompt asks for your application number; enter that in through your telephone's touch-tone keypad. Next, you are prompted for the application number from your confirmation message.

The system then explains that a $2.00 charge for initiating your First Virtual buyer's account will be applied to your credit card, and you are prompted to enter your Visa or MasterCard number.

You are next prompted to enter month and year the card expires; this is to be entered as four digits, two digits for the month and two for the last two digits of the year.

Once the process is complete, the system explains that you will receive a confirmation by e-mail indicating that your account is set up to make purchases through First Virtual.

Responding by Mail for Sellers

Enabling your account for selling requires that First Virtual have somewhere to send you the proceeds of your sales (minus their fees). Using a checking account is the easiest way to do this: First Virtual pays sales proceeds directly into your account. First Virtual combines the process of getting your checking account information with the process of paying the minimal costs of setting up your seller's account by having you mail a check for $10 drawn on the account into which you wish to have your sales proceeds deposited.

The e-mail message confirming that your account application has been received includes an address to send your check to. Including the account application number on the check helps to ensure that the payment is associated with the correct account.

If you are enabling your account for selling only, you may still receive a total of three copies of the application confirmation if your check is not received immediately at First Virtual. Once

the check is received, you will get an e-mail message confirming the new status of your account as being seller-enabled.

Finishing the Process

Once your payment has been received (either your credit card number by phone or your check in the mail), First Virtual e-mails you notification of your VirtualPIN. This is the PIN you specified in your original application with a four-character word and hyphen prepended. For example, if as your PIN you chose:

```
itsy-bitsy spider
```

First Virtual might assign you the VirtualPIN of:

```
rock-itsy-bitsy spider
```

Further information about your account is also included in this message, as well as pointers to more useful information.

GETTING EXPRESS MERCHANT STATUS

The basic First Virtual merchant account is probably the fastest, easiest, and least expensive route to Internet commerce, especially for new merchants. However, one of the most onerous costs, particularly to merchants selling hard goods, is the 91-day hold that First Virtual puts on payments to merchants. The reason for the long hold period is to keep chargebacks to a minimum (they tend to be costly), as well as to keep fraud levels well below those of other "card not present" credit card transaction situations (like telephone and mail order).

Most hard goods vendors cannot function with a 91-day hold period on funds from sales revenue. As was explained in the last section of Chapter 4, merchants wishing to sell hard goods can do so using digital signatures. In conjunction with this new capability, First Virtual introduced a special program especially for merchants who have already been approved to accept credit card payments and who wish to sell hard goods.

First Virtual has teamed with First USA Bank, one of the largest credit card acquiring banks, to offer this value-added service for merchants. It is called the Express Merchant program. Prospective Express Merchant participants must go through the same application process as any other First USA merchant, including paying a $250 (nonrefundable) application fee. There is no monthly fee for the merchant, who pays the same First Virtual charges (2% of the sale, plus $0.29 per sale) that other merchants pay. The big difference is that Express Merchant sellers have proceeds from their sales credited to their accounts within 3–5 days of the transaction approval.

Introduced in the first part of 1996, the Express Merchant program makes it practical for established merchants to sell hard goods over the Internet with the First Virtual payment system. First Virtual expects to be able eventually to allow the participating merchant's sales records to affect their service. For example, newer merchants, who are less likely to be able to qualify for a merchant banking account when they start, may eventually be able to use their First Virtual sales record to apply for Express Merchant status. Existing merchants may eventually be able to qualify for discounted transaction fees based on their prior performance.

Applications for Express Merchant status can be downloaded through the First Virtual Web site.

ACCOUNT MAINTENANCE

Things don't always stay exactly the same, nor does everything always work right. If you don't receive e-mail notification of your First Virtual account activation or modification, you may want to follow up with a request for your current status.

Should your status change (address, phone number, e-mail address, or other changes in information provided to First Virtual), you will need to inform First Virtual. When your credit card expires, you will also need to update your account. These procedures are simple, though modification of account information calls for payment of an additional charge of $2.00.

You may also want to make a payment transfer between two accounts, or just check on recent transactions. All of these functions are easy to do, using First Virtual's e-mail system and telnet server.

Tracking Your Account Status

To follow up on an account's status, send e-mail to the address:

```
findappl@card.com
```

Include the application number in the subject of the e-mail message, and First Virtual will reply with whatever current information they have about your application.

You can also check up on your account status by connecting to the First Virtual telnet server at:

```
telnet.card.com
```

Log in as user "fv" (as described earlier and illustrated in Figure 6-7), and continue the opening menu. Enter the letter "I" to inquire about the status of your application.

You will next be prompted for the VirtualPIN of the account being queried. This option is not available for accounts that have not yet been assigned a VirtualPIN. The server will respond either that the account is valid or that it is invalid; if the account is valid, the preferred currency will also be displayed.

Making Changes

Credit cards expire, and people change their addresses, their banks, and their names. To make a change to your account, you have the option of connecting to the First Virtual telnet server at the address:

```
telnet.card.com
```

Log in as user "fv" and choose the option "C" to make changes to your account. You will have to enter the complete VirtualPIN to identify the account you wish to change. You can then do the following changes:

1. Cancel your account
2. Change your sensitive financial information (credit card number, etc.)
3. Change your personal information (name, address, phone, etc.)
4. Change your preferred language
5. Change your preferred currency
6. Change your optional account settings
7. None of the above (make no changes)

Choose the desired modification, and you will be prompted through the process.

You can also initiate a change in your account by sending e-mail to the address:

```
initchg@card.com
```

You will then receive e-mail with detailed instructions for making the desired modifications.

CHAPTER SEVEN

BUYING WITH FIRST VIRTUAL

Summary This chapter steps the reader through the process of making a purchase using First Virtual, using an actual purchase to demonstrate how transactions are initiated, billed, and fulfilled.

Contents

THE TRANSACTION PROCESS 194
A SAMPLE PURCHASE 195
TRANSACTION COMPLETION 199
PRODUCT DELIVERY 206
BUYING HARD GOODS 207
BUYING BY E-MAIL AND FTP 208
Buying by ftp 208
Buying by E-mail 209

Making a purchase using the First Virtual payment systems is easy, as long as you are able to read and follow instructions and read your e-mail regularly. The transaction examined in this chapter shows how to purchase a subscription to the InfoHaus news list — a good value for anyone interested in using the First Virtual InfoHaus — but the process will be similar for any other product, with only a minor difference when buying hard goods.

THE TRANSACTION PROCESS

As has been discussed elsewhere, the transaction process starts with the merchant offering a product for sale. Providing a VirtualPIN to the merchant is just about all the consumer

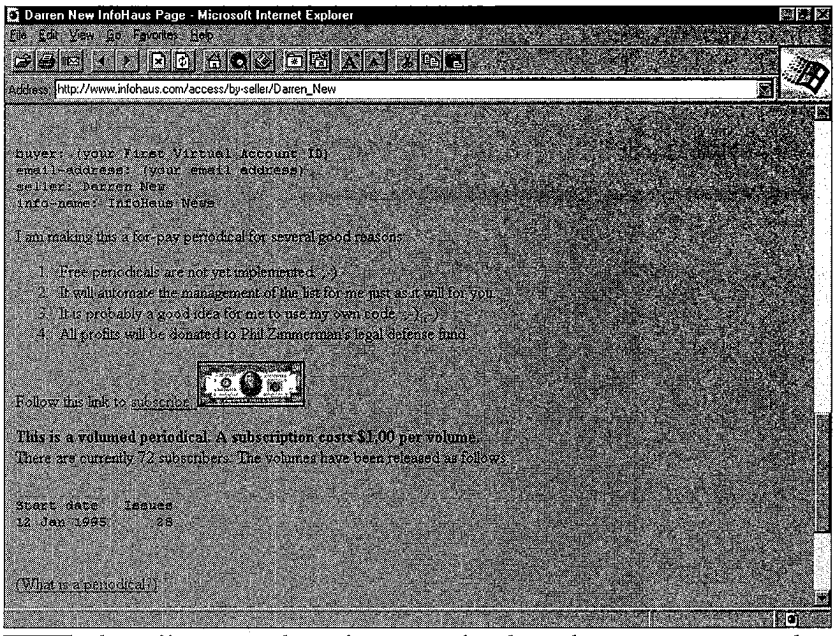


FIGURE 7-1 *This offering on the InfoHaus is for the InfoHaus News e-mail list. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

needs to do once a product is selected for purchase. The merchant may also request some kind of delivery information if the product requires it (hard goods as well as information products delivered by e-mail).

Figure 7-1 shows a typical offering on the InfoHaus: the InfoHaus News e-mail mailing list. Nothing can happen until a merchant sets up an Internet storefront for consumers to browse and buy from. This page includes a description of the product as well as the product's price. There is also a link from the offering screen to a transaction page with forms for the consumer to fill in with required information.

A SAMPLE PURCHASE

Once you decide to purchase a product, follow instructions. In this case, the consumer needs to follow the link associated with the image of the $20 bill shown on the InfoHaus Web page — there is also a text-only link for text-only browsers. The resulting order page is shown in Figure 7-2. On a World Wide Web page, using a Web browser supporting forms, the process is simple (as described on the page): simply enter a First Virtual Account ID (VirtualPIN), and an e-mail address for delivery of the subscription. When you are done, you click on the "BUY" button, and the merchant can submit the transaction to First Virtual for completion.

What happens if your browser doesn't support forms, or if you don't want to make the purchase directly from the Web page? Figure 7-3 shows further instructions provided on this page for submitting a transaction by e-mail. All that is necessary to initiate a transaction is enough information to identify

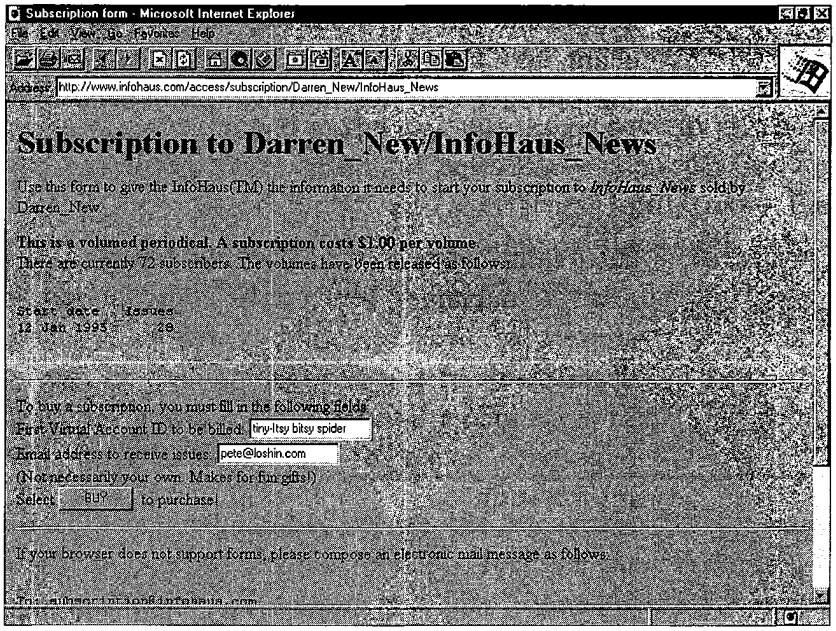


FIGURE 7-2 *Paying for a product using First Virtual's payment system. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

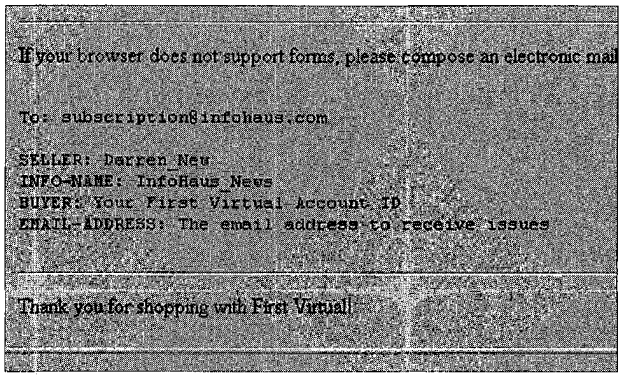


FIGURE 7-3 *Instructions for making a First Virtual purchase by e-mail. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

the seller, the product ("InfoHaus News"), and the buyer (VirtualPIN). In this case, an e-mail address is required because the product is delivered through e-mail.

When the consumer fills in the blanks correctly when buying a subscription, a "Congratulations" screen will appear, as shown in Figure 7-4. For other types of information products, the consumer's browser will simply retrieve the product file; if the product is a text file, the text will be displayed. Other types of files that can be processed by the consumer's browser will be presented to the consumer immediately (such as graphics or audio products). Program files can be saved to disk.

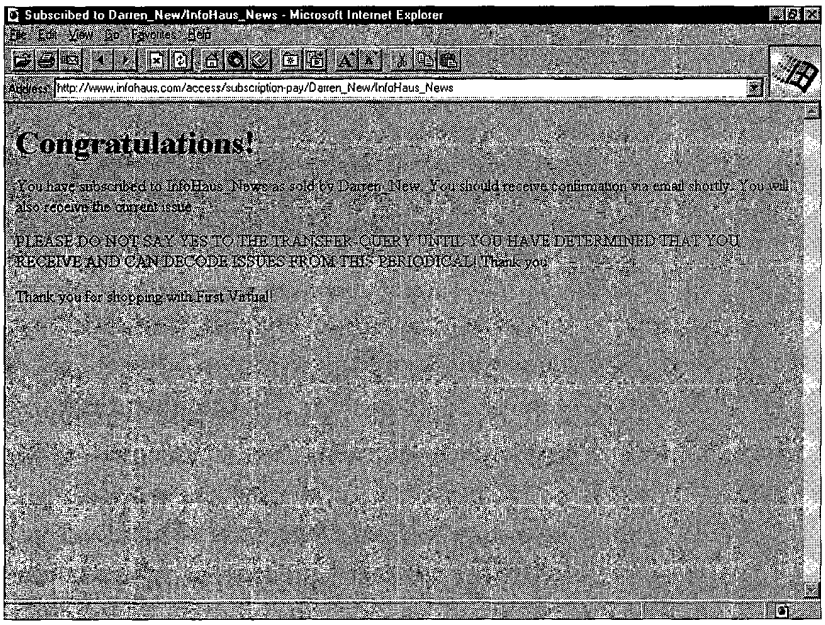


FIGURE 7-4 *Buyers of subscription products get this type of screen when their VirtualPIN is accepted. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

In the event that you enter an invalid VirtualPIN, you may see something like the screen shown in Figure 7-5. This type of response is made possible when the merchant's store automatically checks on VirtualPIN status using the cardnumber status function as defined in the Green Commerce protocol (see Chapter 4).

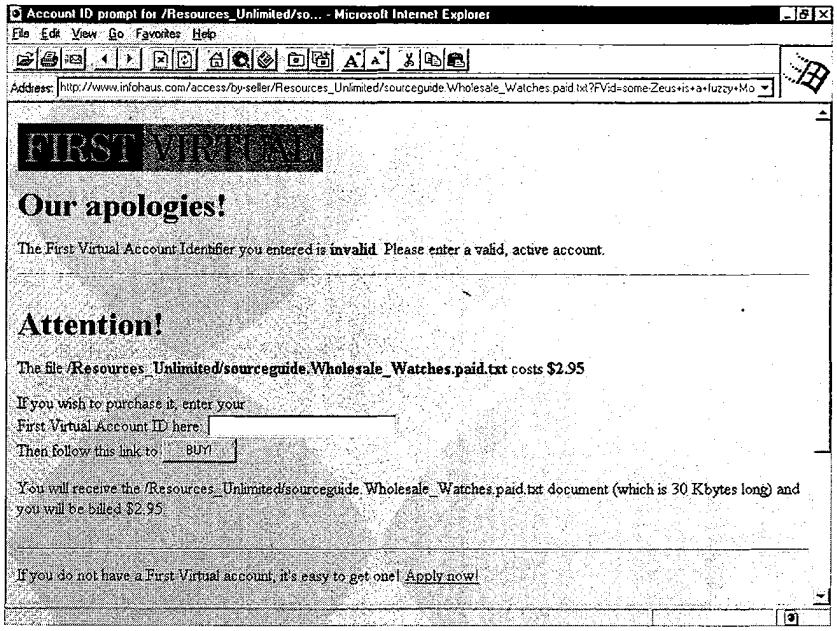


FIGURE 7-5 *If you enter an invalid VirtualPIN you may see something like this when attempting to make a purchase. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

While it is possible to initiate the transaction through an Internet application such as the World Wide Web or telnet, as well as by e-mail, completing the transaction requires an e-mail response from the purchase. This is an important part of First Virtual's security measures: while it may be relatively easy (in theory, at least) to initiate a transaction using a stolen VirtualPIN, completing the transaction requires that the criminal be able to do several things:

- Somehow determine the e-mail address associated with the VirtualPIN.
- Divert e-mail intended for that address, and pass along all of that e-mail *except* for transaction queries from First Virtual relating to the fraudulent transactions.
- Forge e-mail from the customer to approve the fraudulent transaction.

The reader should take note that e-mail from First Virtual relating to transactions will include transaction identifiers but not VirtualPINs — and if you initiate your transaction through the World Wide Web, you would not need to include your e-mail address near your VirtualPIN. By minimizing the amount of information that can be connected to the consumer, First Virtual is able to reduce the potential opportunities for fraud.

TRANSACTION COMPLETION

From the time a customer initiates a transaction to the time the item purchased is actually paid for, First Virtual sends out three different messages to the consumer:

- A **transfer query**, to determine whether the transaction should be completed (did the customer wish to pay for the item ordered).
- A **transfer result**, indicating what the result of the transfer query was (whether the customer decided to accept or decline the item purchased).
- A **payin-notification**, a message indicating that the consumer's credit card is being charged for a certain amount (a payin-notification may include charges from multiple transactions).

The customer need only act on the first type of message; the other two types of messages are largely informational and do not require any action on the part of the customer. The exception is the case in which the customer suspects misuse of the First Virtual account in question (for example, the customer does not recall making the purchases indicated). In these cases, the customer is urged to contact First Virtual as soon as

possible to make them aware of the problem and cancel the account to avoid further problems.

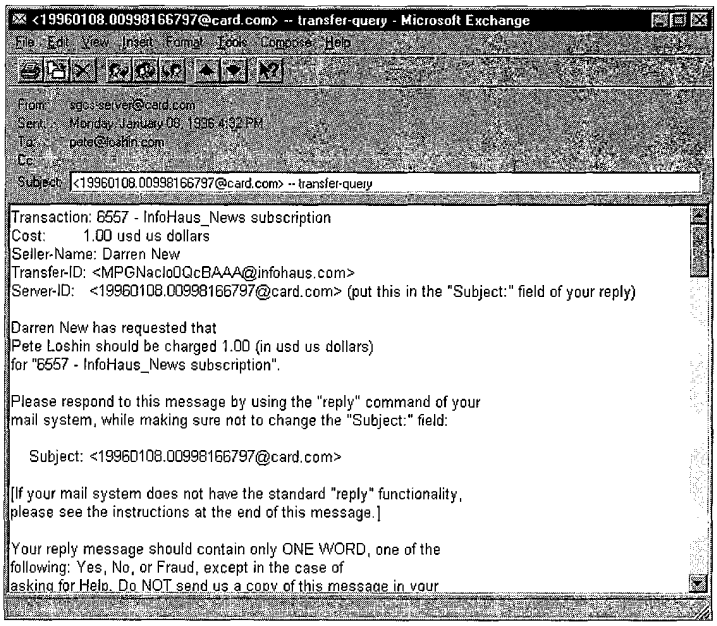


FIGURE 7-6 *A transfer query from First Virtual, received by a consumer after initiating a First Virtual transaction. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The form these messages take will obviously vary depending on the system and software you use for e-mail; Figure 7-6 shows how it might look. While the form varies, the content will remain roughly the same, with a sample message reproduced in full in Figure 7-7. These messages include information about the particular transaction, as well as complete instructions on what to do in response to the message. The reader is urged to read the instructions included in this message, as they clearly explain the possible actions the customer can take in response to the transfer query.

Transaction: 6557 - InfoHaus_News subscription
Cost: 1.00 usd us dollars
Seller-Name: Darren New
Transfer-ID: <MPGNacIo0QcBAAA@infohaus.com>
Server-ID: <19960108.00998166797@card.com> (put this in the "Subject:" field of your reply)

Darren New has requested that
Pete Loshin should be charged 1.00 (in usd us dollars)
for "6557 - InfoHaus_News subscription".

Please respond to this message by using the "reply" command of your mail system, while making sure not to change the "Subject:" field:

Subject: <19960108.00998166797@card.com>

[If your mail system does not have the standard "reply" functionality, please see the instructions at the end of this message.]

Your reply message should contain only ONE WORD, one of the following: Yes, No, or Fraud, except in the case of asking for Help. Do NOT send us a copy of this message in your reply. Please pick the appropriate word choice from the following four situations:

1) "Yes" - You received the information you requested and wish to keep it. The information matches your expectations and therefore you intend to pay for it.

   By answering with the single word "Yes", you authorize us to charge your account 1.00 usd us dollars.

2) "No" - You attempted to purchase the information, but it never got to you, or was corrupted. Or you did receive the information but it was not what you expected and intended to pay for.

   By answering with the single word "No", you decline the request for payment for one of the above reasons.

3) "Fraud" - You did NOT purchase this information and you did NOT receive it. Until now, you were unaware of this transaction. Because you never saw this information, and are now asked to pay for it, you suspect someone has STOLEN your First Virtual account ID.

   By answering with the single word "Fraud", you are informing us of this serious situation and are authorizing your account to be

IMMEDIATELY shut down.

****** PLEASE NOTE ******
If you do say "Fraud", we will IMMEDIATELY and
PERMANENTLY cancel your account. Just like
reporting a credit/debit card stolen, this
action closes your account. You will need to
open a whole new account to make any future
purchases through First Virtual.

4) "Help" - Your situation does not fit any of the three
options above. You have a problem or question that
needs specific help from us.

By responding with "Help" and then describing your
problem in your reply message, the text that follows
the word "Help" will be forwarded to our
human help at 'humanhelp@card.com'.
From there it will be read by a human being and
personally responded to.

This message was provided by the transaction's originator:

On 8 Jan 1996, you requested a subscription
to a volumed periodical on First Virtual's InfoHaus(TM).
The periodical is being sold by Darren_New
under the name InfoHaus_News
for 1.00 USD US Dollars.
Issues will be delivered to pete@loshin.com.
(Please ignore the code number in the description.)

For information on unsubscribing, changing your
email address, or receiving bounced back issues,
send email to scribe@infohaus.com.

PLEASE DO NOT SAY YES TO THIS QUERY UNTIL YOU HAVE
RECEIVED THE FIRST ISSUE AND HAVE DETERMINED THAT
YOU CAN DECODE IT! Thank you.

Thank you for your patronage!

Keep in mind, when you reply directly to this message
(response@card.com), your mail will be read
by an automated process looking for one of the four
words, Yes, No, Fraud, and Help. No human will read this
message unless you respond "Help," in which case the following
text will be forwarded to a human.

Use of the First Virtual Internet Payment System is governed by
the Terms and Conditions effective 16 December 1995. To receive a

```
copy of the TACs document pertaining to either buying, selling,
or selling as an InfoHaus merchant, send e-mail to one of the
following
addresses: "fineprint-buyer@fv.com", "fineprint-seller@fv.com", or
"fineprint-infohaus@fv.com", and the reply will contain the
corresponding Terms and Conditions. If you have not read and accepted
and agreed to be bound by these Terms and Conditions, do not proceed
with this or any other First Virtual transaction.

FIRST VIRTUAL is a servicemark of First Virtual Holdings Incorporated.

IF YOUR MAIL SYSTEM CANNOT CONSTRUCT REPLY MESSAGES
in the standard Internet manner, you may answer this message by
sending a message like this:

    To: response@card.com
    Subject: <19960108.00998166797@card.com>

The body of your message should contain only one word,
one of these three words: Yes, No, or Fraud, except in the case of
asking for Help. We realize that this is unpleasant to do by hand, but
it is
unavoidable if your mail system does not construct replies correctly.
You might also consider asking your system administrator to upgrade
your mail system.

IF YOUR MAIL SYSTEM CANNOT CONSTRUCT MESSAGES
WITH SUFFICIENTLY LONG SUBJECT LINES, send a
message to response-challenged@card.com with
the first (and only) lines in the message being the following two
lines:

Server-ID: <19960108.00998166797@card.com>
Authorization: yes (or no or fraud or help)
```

FIGURE 7-7 *A sample First Virtual transfer query, reproduced in full. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

When the customer receives this message, responding "yes" as shown in Figure 7-8 will result in the transaction being completed — the customer's credit card will eventually be charged for the transaction, and the merchant will eventually receive payment. This message is a simple reply to the original transfer query as received from First Virtual; if the customer's e-mail software has problems generating such a reply, the body of the transfer query will guide the user.

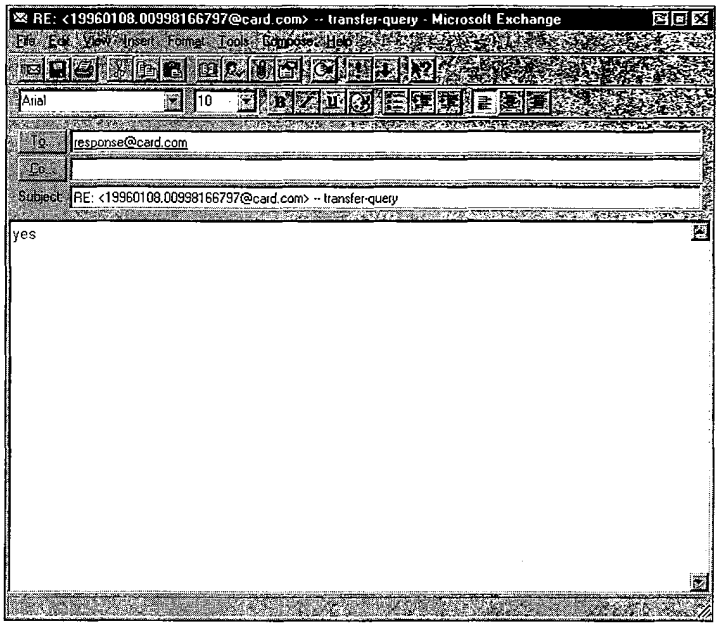


FIGURE 7-8 *Composing a response to a First Virtual transfer query indicating acceptance of the transaction. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

After the customer responds to a transfer query by accepting the transaction, First Virtual will send the customer a copy of a transfer result message that is also sent to the merchant. The text of this message is shown in Figure 7-9. It explains that the customer has authorized the transaction, but that the buyer's credit card has not yet been charged.

```
Transaction: Item 5950 6.95
Cost: 10.70 usd us dollars
Buyer-Name: Pete Loshin

Pete Loshin has authorized the transfer of
10.70 (in usd us dollars) to Dawn Time Inc.
for "Item 5950 6.95".

The buyer's credit card has NOT yet been charged for this purchase.
You will receive payment (reduced appropriately by our service charges),
once the buyer's credit card has been charged, and the Settlement
```

```
Date has been reached.

Use of the First Virtual Internet Payment System is governed by
the Terms and Conditions effective 16 December 1995. To receive a
copy of the TACs document pertaining to either buying, selling,
or selling as an InfoHaus merchant, send e-mail to one of the
following
addresses: "fineprint-buyer@fv.com", "fineprint-seller@fv.com", or
"fineprint-infohaus@fv.com", and the reply will contain the
corresponding Terms and Conditions. If you have not read and accepted
and agreed to be bound by these Terms and Conditions, do not proceed
with this or any other First Virtual transaction.

FIRST VIRTUAL is a servicemark of First Virtual Holdings Incorporated.


Please ignore anything that appears after this line.

- fv
Content-Type: application/green-commerce; transaction=transfer-result

Buyer-Name: Pete Loshin
Seller-Name: Dawn Time Inc.
Amount: 10.70
Currency: usd us dollars
Transfer-Type: info-sale
Server-ID: <19960202.04234982017@card.com>
Description: Item 5950 6.95
Authorization-Result: yes

Use of the First Virtual Internet Payment System is governed by
the Terms and Conditions effective 16 December 1995. To receive a
copy of the TACs document pertaining to either buying, selling,
or selling as an InfoHaus merchant, send e-mail to one of the
following
addresses: "fineprint-buyer@fv.com", "fineprint-seller@fv.com", or
"fineprint-infohaus@fv.com", and the reply will contain the
corresponding Terms and Conditions. If you have not read and accepted
and agreed to be bound by these Terms and Conditions, do not proceed
with this or any other First Virtual transaction.

FIRST VIRTUAL is a servicemark of First Virtual Holdings Incorporated.
```

FIGURE 7-9 *A transfer result message received by the consumer after accepting a transaction (replying "yes"). Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

Should the customer respond with a "no," the transaction will not be processed, and both the customer and merchant will receive a transfer result message, as shown in Figure 7-10.

```
Transaction: sourceguide.Wholesale_Watches
Cost: 2.95 usd us dollars
Buyer-Name: Pete Loshin
Transfer-ID: <3608615.21675.0@buyers.infohaus.com>

Pete Loshin DECLINES the transfer of 2.95 (in usd us dollars)
to RESOURCES UNLIMITED
for "sourceguide.Wholesale_Watches".

Please ignore anything that appears after this line.

 - fv
Content-Type: application/green-commerce; transaction=transfer-result

Buyer-Name: Pete Loshin
Seller-Name: RESOURCES UNLIMITED
Amount: 2.95
Currency: usd us dollars
Transfer-Type: info-sale
Server-ID: <19960201.01798286461@card.com>
Description: sourceguide.Wholesale_Watches
Transfer-ID: <3608615.21675.0@buyers.infohaus.com>
Authorization-Result: no
```

FIGURE 7-10 *A transfer result message received by the customer when a transaction has been declined (the customer answered "no"). Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The meat of these messages is clear, although clearly there are additional pieces of information carried within the message. This "extra baggage" may be displayed in your e-mail reader depending on how it handles MIME enclosures, and how it is configured to deal with those enclosures.

PRODUCT DELIVERY

The customer should be aware of what is being purchased, and how and when it will be delivered. Information sellers have several different options for delivering their product to customers:

- They can deliver immediately, prior to requesting a VirtualPIN — a purely voluntary payment.

- They can deliver only after the customer provides a VirtualPIN — the customer may accept or decline the transaction after reviewing the material and receiving a transfer query from First Virtual. This is the preferred option for most information merchants.
- Periodical subscriptions can be delivered just like real-world publications, with the first issue delivered free of charge and subsequent issues delivered only after payment (or a "yes" response to a transfer query) is received.
- Big-ticket information products can be withheld until the customer accepts the transaction.

Fulfillment information required from the consumer ranges from nothing, when the consumer downloads a file directly from a server, to an e-mail address when the product is to be delivered by e-mail (as with e-mail subscriptions), to postal addresses, phone numbers, and other contact information for delivery of more complicated products or postal mail delivery of hard copy subscriptions.

BUYING HARD GOODS

The process of purchasing hard goods through First Virtual is identical to the process of purchasing information goods — at least for the purchaser. There are a couple of slight differences; for one thing, the transfer-type attribute of the transaction will not be "info-sale," which is the default value, but will be "goods-sale" to indicate that the item being purchased is hard goods.

Another major difference is that the merchant does not ship out the product until a "yes" response has been received from the customer. Some information sellers may also wait for a positive response before shipping their products.

Information sellers have the option of withholding their product until the transaction is accepted, but they are generally urged to allow the consumer to "try out" the information before making a commitment to pay. Hard goods sellers, on the other hand, stand to lose the cost of their goods as well as the cost of shipping if they deliver products without an assurance of payment.

BUYING BY E-MAIL AND FTP

Not everyone has access to the World Wide Web. Some have Internet access through applications such as ftp; others have no direct access at all, using e-mail for indirect Internet access. These users are still potential customers if you sell your product through First Virtual. Details on using ftp vary from system to system, with further variations depending on the software being used; more details on using ftp are available in many books, magazine articles, and the Internet.

BUYING BY FTP

When connecting to a First Virtual-enabled ftp server, use the user ID:

```
fvftp
```

Don't use "anonymous" as the user ID, as is normally called for when doing anonymous ftp. For the password, use your VirtualPIN.

Once you have logged on in this way, you should be able to browse the server's directories freely. Any time you attempt to retrieve for-pay information (whether a directory listing or an

actual file), the server will return a message indicating what the charge will be. Charges will be made to your account only after you have approved them by e-mail, later.

BUYING BY E-MAIL

If you need instant gratification, buying by e-mail is not going to be for you. This process is simplest if you are buying from the First Virtual InfoHaus (see Chapter 8 for more details about selling through the InfoHaus), but it is not impossible with other First Virtual-enabled ftp servers (the process requires using an intermediate system which accepts e-mail messages with ftp commands as the body).

While not impossible, buying by e-mail from the InfoHaus can be a tedious, three-step operation. The customer should have some idea of a keyword, product name, or merchant name, or else an extra step is added.

If you don't have any idea of what you want to look at on the InfoHaus, you can send a blank message (no subject or body necessary) to the address:

```
search@infohaus.com
```

In return, you will get an error message telling you that you should have entered some kind of search criterion to narrow down what you are looking for. More important, the message will list merchant names ("sellers"), product categories ("topics"), and keywords ("keywords") that you can use to narrow your search.

The next step is to send another message to the "search" address, this time including one or more search criteria in the body of the message. These criteria are listed in Table 7-1.

TABLE 7-1 *Search options for e-mail shopping through the InfoHaus.*

Criterion	Description
Seller:	Name of InfoHaus merchant.
Keyword:	A keyword designated by the merchant to describe the product.
Topic:	A descriptive term for the merchant/product.
Date:	To retrieve items only stocked since the date indicated, using the form "DD MMM YY" where day and year are numbers, and the month is a three-letter abbreviation.

A sample search message would be addressed to "search@infohaus.com" and the body of that message would look something like this:

```
Seller: Pete Loshin
Date: 01 JAN 96
```

This search would return any items sold by the merchant "Pete Loshin" and checked into the InfoHaus for sale since January 1, 1996. In response you would receive a listing of items in the InfoHaus that meet the criteria you set in your initial search message. For example, you might see something like this:

```
Your search of First Virtual's Infohaus(TM)
has found the following seller/info-item pairs:

Pete_Loshin Part1.First_Virtual_Book
Pete_Loshin Part2.First_Virtual_Book
Pete_Loshin Part3.First_Virtual_Book
Pete_Loshin Part4.First_Virtual_Book
```

This is essentially a short listing of the files that meet your criteria. After this list, very basic information provided by the merchant is included for each item, including a price and a very short description of the item. If you want to know more about the items returned by your search, move on to the next step, which is to send a message to the address:

```
retrieval@infohaus.com
```

The body of the message should look something like this:

```
Seller: Pete Loshin
Info-name: Part2.First_Virtual_Book
Part: free
```

In reply to this message, you will receive the "free" part of the item listed, usually a more complete description of the item being sold. You may choose to purchase the item, which means having it downloaded to you — you will still have the option of declining the sale if once you receive it, if you decide it is not what you expected (or is not worth the asking price). To make a purchase, send another message to the "retrieval@infohaus.com" address, with the body looking something like this:

```
Seller: Pete Loshin
Info-name: Part2.First_Virtual_Book
Part: paid
Buyer: pork-three little pigsfeet
```

It is important to note here that the "part" is "free" in the first case (to get the description of the item) and is "paid" when you are ready to make the purchase. Also, when making a purchase, you enter your VirtualPIN on the last line so your First Virtual account is charged for the item being purchased.

"Quickbuy" numbers add some refinements to the e-mail buying process, but they require some extra steps from the merchant and are described in more detail in Chapter 10.

CHAPTER EIGHT

SELLING ON THE INFOHAUS

Summary This chapter begins with a full description of the InfoHaus, and continues with a detailed description of the processes of setting up, configuring, and stocking the InfoHaus storefront, followed by specific walkthrough examples of doing those processes using e-mail, telnet and ftp.

Contents

INTRODUCTION TO THE INFOHAUS 214
Why the InfoHaus? 214
How It Works 216
It's Not Just for the World Wide Web 216
What It Costs 217

SETTING UP YOUR STOREFRONT 218
Opening Your InfoHaus Storefront 218
Setting up a Storefront Using Telnet 219
Setting up a Storefront Using E-mail 225
Stocking Your Store 227
Preparing Your Information Products 228
Uploading Products by ftp 232
Uploading Products by E-mail . . . 233
Checking in Products by Telnet . . . 233
Installing Products by E-mail 235

ADDING HTML TO YOUR INFOHAUS STOREFRONT 238

INFOHAUS PERIODICALS 240
Subscribing to a Periodical 241
Creating Periodicals 241
Adding Issues to a Periodical 242

INTRODUCTION TO THE INFOHAUS

First Virtual offers the InfoHaus storefront hosting service to its merchants who prefer to have someone else manage the hardware, software, and services necessary to maintain an Internet presence. This service is particularly attractive to information merchants who see the Internet as a suitable medium for selling their products, but who don't have the time, money, or expertise to set up their own Internet servers. It is also a great way for new information merchants to test the waters of Internet commerce on a shoestring.

Why the InfoHaus?

Opening a store in the real world is a complex and expensive task. Even the nine-year-old child selling lemonade on the corner needs to make a relatively significant investment in basics: pitcher and glasses, countertop, signs, and a cash box are the minimum operating equipment. An operating permit, as well as a corner to operate out of, are also necessary — and all this is before considering cost of products sold.

The Internet merchant also needs some minimum basic equipment, in addition to a product, to sell online. You can choose to set up your own Internet server, which means the following investments:

- A computer to act as the Internet server.
- An Internet connection for the server, preferably a high-speed link (this may mean purchasing an Internet router as well as other equipment). This will require some startup costs, as well as ongoing monthly charges for connectivity.

- Internet software for the server, including software capable of doing TCP/IP networking as well as appropriate Internet services — most likely a World Wide Web server program.

In addition to these outlays, you'll need to spend some time to get everything installed and configured. If you have a lot of time on your hands and have a reasonable understanding of how TCP/IP works, this may not take too long. However, you'll also have to allocate a portion of your working day to monitor your Internet connection, do system management tasks on your server, and make sure everything is running smoothly and securely.

The costs of setting up your Internet store this way can be compared to the costs of setting up your own real-world storefront. You can go for the lowest-cost options all the way, similar to leasing and operating a "push-cart" mini-store in a shopping mall, or you can go first class all the way, similar to building your own stand-alone retail operation. You can cut costs to the bone by using freeware, shareware, or low-cost commercial software on an inexpensive personal computer; sufficient Internet services (24-hour a day service) are still likely to cost at least $100 a month.

InfoHaus offers an attractive alternative to the entry-level Internet merchant. If you are selling information products and if you have set up as a First Virtual seller, you can upload your products to the InfoHaus Internet server and set up your storefront for a minimal storage charge (based on the amount of information stored on the server). You pay nothing else until you make a sale, at which point you are assessed an 8% charge to pay for the InfoHaus service, in addition to other First Virtual charges.

How It Works

The InfoHaus is a Web server that customers can browse through, and that merchants can load with their store information and information products over the Internet. You set up and stock your InfoHaus storefront using Internet applications such as telnet, ftp, and e-mail. Potential customers can see what you have to offer by browsing the InfoHaus Web site at:

```
http://www.infohaus.com
```

This site is also accessible through the First Virtual Web site.

At a minimum, InfoHaus merchants need only be able to send and receive Internet e-mail, but if you have the ability to connect to the InfoHaus systems directly with telnet and ftp, setting up and managing your storefront will be much easier. It is possible to do all InfoHaus functions by e-mail, but opening your shop, checking in products for sale, and uploading your information products will be much easier with direct Internet access. Step-by-step instructions explaining how to set up and stock the storefront are provided later in this chapter.

It's Not Just for the World Wide Web

The World Wide Web is the easiest way to access InfoHaus storefronts, but it isn't the only way. Not everyone has Web access; some have access to ftp, while others only have e-mail. These are an added pool of potential customers that InfoHaus merchants can reach: the InfoHaus creates an ftp directory automatically when a storefront is created, and users with only e-mail access to the Internet can also browse InfoHaus

using e-mail. For more details on buying through the InfoHaus by ftp or by e-mail, see Chapter 7.

What It Costs

The only extra charges for selling on the InfoHaus are a monthly charge of $1.50 per megabyte of data stored on the InfoHaus server, and an 8% "commission" on approved purchases. These charges are in addition to the standard First Virtual charges of $0.29 per transaction and 2% of gross sales.

Merchant offerings include 4.8 Mb of assorted text and graphics files.

During the course of a single month, the merchant makes 100 sales of $10 each, for gross sales of $1,000.

First Virtual Fees:	
Transaction fees (100 @ $0.29)	$ 29.00
2% on gross sales	20.00
InfoHaus Fees:	
Storage fee ($1.50/Mb)	$ 7.50
8% on gross sales	80.00
Total Charges:	$136.50

FIGURE 8-1 *A sample of how InfoHaus charges are determined. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

An example of how this works is shown in Figure 8-1. In practice, the "$1.50" monthly charge is actually prorated by the day, and by the amount of storage you actually use. The daily charge per megabyte of data is $18 (twelve times $1.50) divided by 365 (the number of days in the year) — or about a nickel per megabyte per day.

The merchant's storage fee is determined by the size of the files on disk at the InfoHaus, rounded up to the next highest

megabyte, measured once a day. For example, if you start out by storing only a single file of 20,000 bytes, you would still be subject to the minimum charge of about $0.05 a day. On the other hand, if you decided to upload the contents of a CD-ROM (about 600 MB) for sale on the InfoHaus, your daily storage charge would be almost $30.

This example also does not include the $1.00 First Virtual charge for a funds deposit to the merchant's account, because that charge may be incurred more or less than once in a month.

SETTING UP YOUR STOREFRONT

Once you've set up your First Virtual account (see Chapter 6 for more details), you can set up your InfoHaus storefront — you don't even have to wait for your account to be enabled for selling. Any sales you make from the InfoHaus before your account is sales-enabled will be held for you and forwarded appropriately when your check is received.

Opening your storefront on the InfoHaus can be done by e-mail, but the preferred method is to log onto the InfoHaus Telnet server and work through the process interactively.

Opening Your InfoHaus Storefront

When you are ready to open your storefront, you'll need to get certain information to the InfoHaus server. You can do this by putting the information into an e-mail message, or you can have the InfoHaus telnet server do this for you automatically

after you enter the necessary information interactively. This information includes the following:

- Your First Virtual account ID (VirtualPIN).
- Your e-mail address.
- Preferred currency — the default, and only currently supported currency, is USD for U.S. dollars.
- Preferred language — the default, and only currently supported language, is EN for English.
- A "doing business as" (DBA) name for your InfoHaus storefront.
- A brief description of your business.

Using e-mail may be convenient, but it requires that all information be formatted in precise conformance to the guidelines set by the InfoHaus specifications. The telnet option is simpler, since it walks you through the process and lets you edit your responses if necessary.

SETTING UP A STOREFRONT USING TELNET

The first step is to log onto the InfoHaus telnet server with your telnet client. The host name you need to connect to is:

```
infohaus.telnet.com
```

The opening screen will look something like that shown in Figure 8-2. To login, enter the user ID "ih" and press the return key; no password is necessary.

The login process is similar to that described in Chapter 6 for setting up a new First Virtual account; as shown in Figure 8-3, you will be asked if you are using X11 windows, followed by a

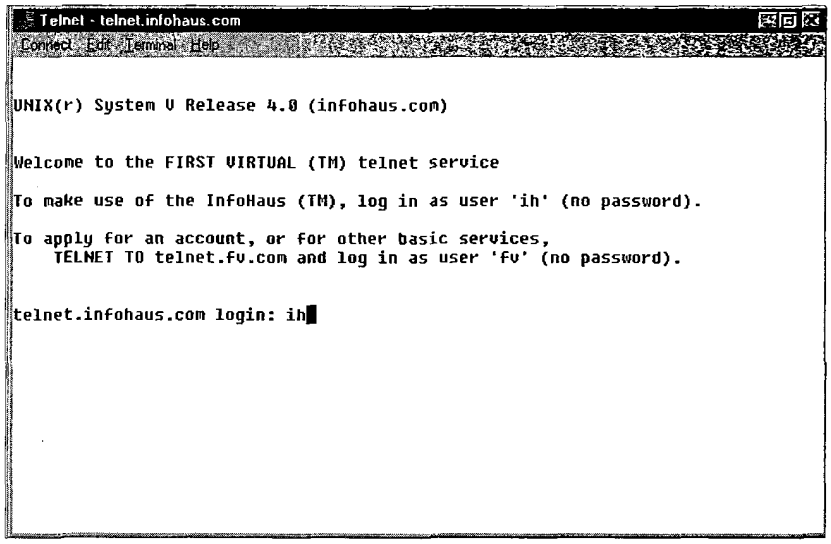


FIGURE 8-2 *Logging into the InfoHaus telnet server. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

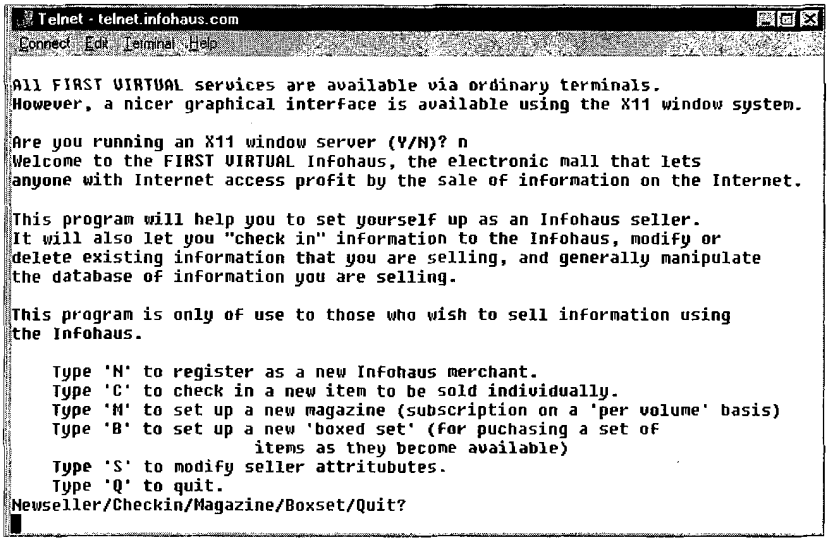


FIGURE 8-3 *InfoHaus telnet server welcome and options menu. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

brief explanation of what your options are along with a menu of choices. Options include registering as a new InfoHaus merchant, checking in new items for sale, setting up subscriptions and sets of items for sale, and modifying seller attributes.

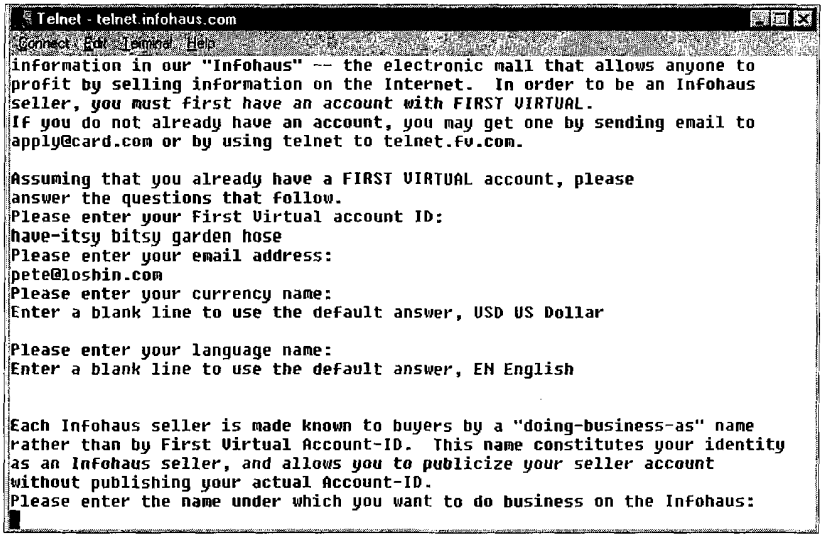


FIGURE 8-4 *Entering InfoHaus merchant registration information. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

By entering the letter "N" (for "new merchant") at the prompt, you will be further prompted through the registration process. Figure 8-4 shows the question/answer process, with prompts for First Virtual account ID, e-mail address, preferred currency and language, and "doing-business-as" name.

The next prompt (Figure 8-5) allows you to keep your InfoHaus store invisible until you finish stocking it with products (if you choose to do so, you will have to turn it to visible later, when you finish stocking it). The next prompts are for a brief (60 character maximum) description of your business, which is displayed when people browse through listings of InfoHaus sellers, and a prompt for a more complete description to be displayed after potential customers select your store. This can be much longer. You enter text in the exact form you want it to appear, and you can press the return key to force a line break in your storefront. To indicate that you have finished, you must enter a period (".") on

a line all by itself, to distinguish it from a blank line and to signal the InfoHaus telnet server that you are ready to move on to the next prompt (see Figure 8-6).

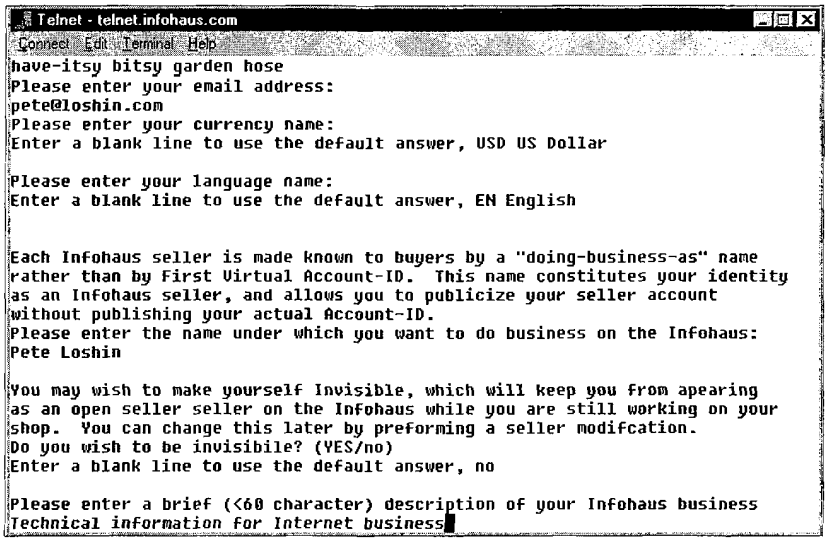


FIGURE 8-5 *More prompts for InfoHaus storefront information. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

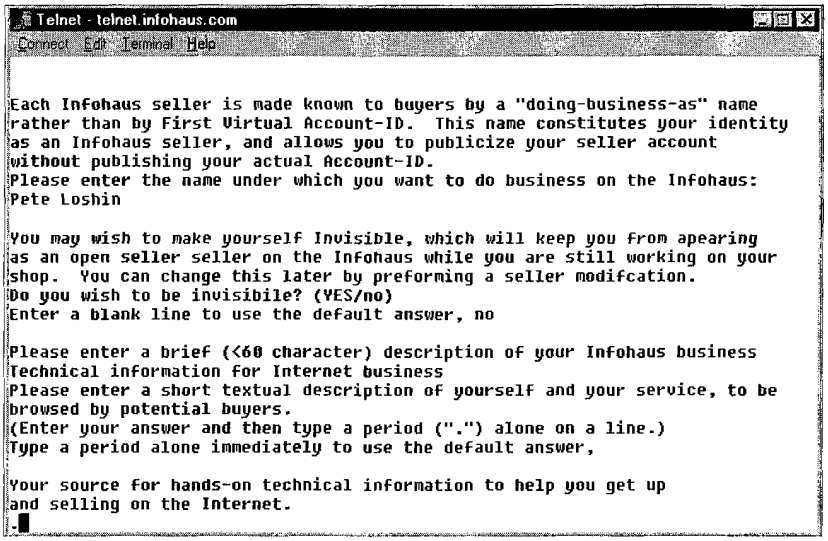


FIGURE 8-6 *Completing your storefront information. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

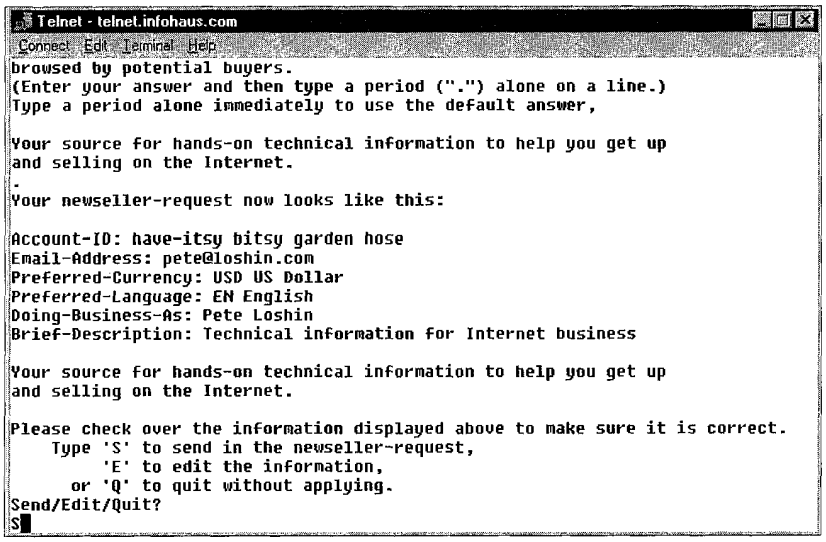


FIGURE 8-7 *Checking your InfoHaus storefront information. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The next step is to check what you have already entered. You may make errors of entry when you go through this process, although you can usually use the backspace key to back up through an entry. However, if you hit the enter key too quickly, you don't have to restart the process — just continue following the prompts, and when you are finished you will have the choice of editing your information by entered, as shown in Figure 8-7. Should you want to make a change, enter the letter "E" (for "edit"), and the server will give you the opportunity to change any or all of your answers. When editing is complete, you will see this display again.

At this point, if everything checks out correctly, you can send in your new InfoHaus seller request by entering the letter "S" (for "send"). If you decide you don't actually want to submit your request (you can't decide on a doing-business-as name, or you can't remember your VirtualPIN), you can enter the letter "Q" (for "quit") to quit without sending in your application.

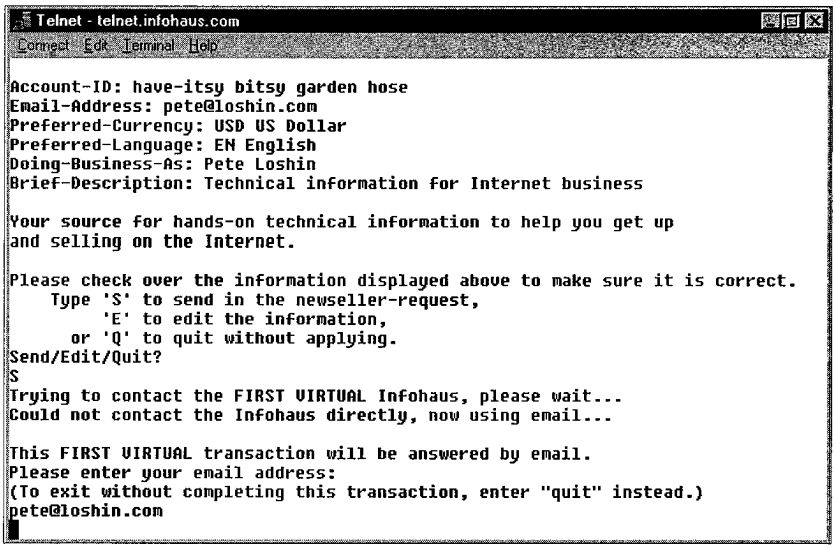


FIGURE 8-8 *Submitting your storefront information. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

When you send your request, you may get an immediate response from the InfoHaus telnet server; otherwise, you will receive an e-mail message indicating the result. (See Figure 8-8.) The text of such a message is reproduced in Figure 8-9.

From: InfoHaus Server[SMTP:infohaus-processing@infohaus.com]
Sent: Monday, February 19, 1996 10:45 AM
To: pete@loshin.com
Subject: Re: Newseller request

Welcome to First Virtual's Infohaus!

Your request to become a new seller has been accepted.
Your official identification is "Internet Commerce Technical Journal".
You may post new information at any time now, using
this identifier and your First Virtual Account ID.
Your information will be billed in USD US Dollar.

Buyers may access your information in several ways, including email,
ftp to ftp.infohaus.com under /infohaus/by-
seller/Internet_Commerce_Tech_Jrnl
and http://www.infohaus.com/access/by-
seller/Internet_Commerce_Tech_Jrnl

```
For the purposes of QuickBuy, your seller number is "1256",
meaning your QuickBuy numbers will be of the form "1256-9999".

For information about subscribing to the InfoHaus News, send the
following email message:
                To: retrieval@infohaus.com

                Seller: Darren New
                Info-Name: InfoHaus News
                Part: Free

Additional technical information of interest to InfoHaus sellers
is available under by browsing
http://www.infohaus.com/access/by-seller/InfoHaus_HelpMeister

Please ignore anything that appears after this line.

Doing-Business-As: Internet Commerce Technical Journal
Access-URLs:       mimeserver@infohaus.com
                   ftp://ftp.infohaus.com/infohaus/by-seller/
                         Internet_Commerce_Technical_Journal
                   http://www.infohaus.com/access/by-seller/
                         Internet_Commerce_Technical_Journal
Seller-Number: 1256
```

FIGURE 8-9 *A message sent by the InfoHaus server confirming a new storefront. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

As you can see, this message is simply a confirmation of the information you provided during the new seller registration process. Note also that your "doing-business-as" name is used to create methods of reaching your product by World Wide Web as well as by ftp, and the URLs are provided. Another important item is your seller number, which you can use to create "QuickBuy" numbers for individual products, which are discussed later in this chapter.

SETTING UP A STOREFRONT USING E-MAIL

One of the attractive features of the First Virtual system, as well as the InfoHaus Internet mall, is that you don't need to have a direct connection to the Internet with full graphics capabilities to use it — either as a buyer or a seller. Some users may

even prefer to use e-mail to manage their InfoHaus storefront, particularly if they are expert at e-mail but less sure of themselves when using Internet applications such as ftp or telnet.

```
Content-type: application/fv-infohaus;
              transaction=newseller-request

Doing-Business-As: Pete Loshin
Preferred-Currency: USD
Account-ID: pork-eenee meenie miny mo
EMail-Address: pete@loshin.com

If you need help getting up and running as an Internet merchant, look
no further. The hands-on, technical help you need is right here.
```

FIGURE 8-10 *This is the format to use when sending in your new seller information to the InfoHaus by e-mail. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The downside of managing your store by e-mail is that you don't always get instant gratification, and you'll need to follow directions exactly. Figure 8-10 shows the body of a newseller request message you would send to this address:

```
mimeserver@infohaus.com
```

Note the format used: each line contains an attribute defined in the InfoHaus specifications separated from its value by a colon and a space. The example in Figure 8-10 shows the minimum required attributes, with descriptive material added after the attributes. Each attribute gets its own line, and attributes that require more than one line to enter completely can be split as long as the continuing lines begin with a space.

There are other attributes that may be used, and can be added to the newseller-request e-mail message:

- Bill-to-ID. This is the First Virtual account to be used to pay for storage and transaction fees; this account has to be

enabled for purchases and must use U.S. dollars. This option is available for users who wish to bill these charges to a separate account other than that used to receive payments.

- Brief-Description. This is the 60-character maximum description that appears in the World Wide Web directories.
- Topic. This is a list of topic names separated by spaces used to indicate topics covered by the store.
- Contract-ID. This indicates a special type of program to be used to control how your store is managed. This attribute is not currently important to most merchants.
- Security-Requirements. This attribute is not currently implemented for InfoHaus merchants, but is relevant to hard goods sales, as discussed elsewhere in this book (see Chapter 4).
- Preferred-Language. The default (and only currently implemented language) is English.
- Send-Transfer-Requests. This is a "yes" or "no" option. If "yes" is indicated, edited versions of transfer-requests are sent to the InfoHaus merchant e-mail as they are processed. Otherwise, the seller receives only the transfer results.

When the InfoHaus server receives your new-seller request, it processes it and returns you e-mail indicating either that the request was processed or that the request was denied. If the latter, it will give a reason why the request was denied (for example, an error in transcribing your VirtualPIN would result in a message indicating that the account ID you provided was invalid).

Stocking Your Store

Once you've got your storefront set up, you still must stock it with items for sale. This is a two-part process: you must

check products in to the InfoHaus by providing basic information about them, including product name and price, and you must also upload the actual product data file to the InfoHaus. Checking in a product requires providing the following information:

- Your "doing business as" name.
- Your VirtualPIN.
- The name of the product.
- A price for the product.

Checking in products can be done by e-mail or by telnet; uploading products can be done by e-mail or by ftp. It is also possible to type your information product directly through a telnet session, but this is possible only when the product itself can be typed. You cannot type in binary data files, and it is impractical to enter lengthy text files this way. This method may be practical for entering small text products such as jokes, limericks, or (very) short stories.

PREPARING YOUR INFORMATION PRODUCTS

Anything that you can reduce to a computer file can be sold on the InfoHaus. That includes files containing the following:

- Text, which can include valuable information (instructions, recipes, contact lists, money-making opportunities, etc.) or interesting information (jokes, poems, fiction, travelogues, etc.)
- Graphics, including digitized photographs, paintings, or computer graphics.
- Computer software — any type of program to perform any type of function on a computer.

- Audio, video, or other types of multimedia files. These could record speeches, music, or anything else that can be recorded.

You can use your imagination: anything that you can express as a data file can be sold.

Before you can start selling the product, you must do three things:

- **Step 1:** Get the information product files ready. This means you must get the information into a suitable form for sale. This means selecting the correct format for the product. For example, a document could be sold in various formats. You could sell it as a word processing document, which retains formatting, but which makes it inaccessible to anyone who does not use that word processor or who cannot convert that format into a useable format. A more universal solution is to put the document into a straight ASCII text format, which makes it accessible to any computer user.

  Graphics files should be saved in a standard format (such as GIF or JPEG) rather than proprietary formats; the same goes for other types of multimedia files.

  The form in which software programs are sold will depend on the platforms they are written for. Personal computer programs will probably be sold in compiled form, while UNIX software may be sold as source code.

  If your information product is very large, you may want to use a standard compression program to produce an archive or self-extracting archive file. This reduces the cost of storage on the InfoHaus server, and reduces the time required to download the file. However, not all potential consumers will be able to extract files from a tar

(UNIX tape archive format) file; many won't even be able to handle zip files.

However you decide to package your product, you should collect the product together and make a note of the filenames for the next step.

- **Step 2:** Give your product a name. Product names appear on the InfoHaus as filenames under ftp, or as links on the InfoHaus Web pages. These names are case-sensitive, and may be made up of letters or numbers (A–Z, a–z, 0–9). The only valid punctuation marks are periods (".") and underscores ("_"). Underscores can be used to separate words in a product name for clarity.

  Periods can be used to separate hierarchical parts of the product name. For example, Table 8-1 shows a set of product names that might be used by a merchant selling three types of items ("Software," "Graphics," and "Documentation"). These product names are sorted alphabetically by within each hierarchical level, and make it easier for consumers to find what they are looking for.

TABLE 8-1 *Sample hierarchical InfoHaus product names.*

```
Documentation.Corporate.Mac_Spreadsheet
Documentation.Corporate.PC_Spreadsheet
Documentation.Personal.PC_Spreadsheet
Documentation.Personal.PC_Spreadsheet
Software.Corporate.PC_Spreadsheet_Program
Software.Corporate.Mac_Spreadsheet_Program
Software.Personal.Mac_Spreadsheet_Program
Software.Personal.PC_Spreadsheet_Program
Graphics.Animals.Chipmunk
Graphics.Animals.Deer
Graphics.Animals.Squirrel
Graphics.Animals.Zebra
Graphics.Trees.Ash
Graphics.Trees.Beech
Graphics.Trees.Oak
Graphics.Trees.Walnut
```

The product names don't have to be the same as the names of the files containing the products, but you will need to associate filenames with product names later. Also note that you need to consolidate each separate product into a single file. Keep this in mind when packaging products that consist of more than a single file (as with software products that use several different program files) since you'll probably have to create an archive or zip file for distribution purposes.

- **Step 3:** Set a price for your products. The prices you set is entirely dependent on what you think the product is worth. However, keep the following in mind when setting your prices:
  - Make sure it is possible to make money on the transaction. Remember that the First Virtual transaction charge on all transactions is $0.29, and other transaction fees (2% for First Virtual and 8% for InfoHaus) are levied on the gross amount of the sale. This means that if your product costs $0.33, you only make $0.01 after fees are deducted. If you price your product at $10, you net $8.71 ($0.20 to First Virtual plus the $0.29 transaction fee; $0.80 to the InfoHaus).
  - Be reasonable in pricing. If your product is priced too high, no one will buy it, particularly if similar products are priced more competitively. Don't expect someone to pay you $25 for your novel if similar reading material is available in paperback form for $7.
  - Don't forget about your storage costs, particularly if your products are very large. Keep your products as small as possible; remember that InfoHaus fees for storing the amount of data contained on a CD-ROM would be close to $30 *a day* — the monthly storage bill would be in the neighborhood of *$900*.

- **Step 4:** Create a "free" portion for the product. This is a file that describes the product being sold. It may simply be a short textual description of the product, but it does not have to be text. For instance, if the product is a graphics image, the free part of the product might be a much smaller, "thumbnail" version of the image. Whatever you choose to incorporate into this part of your product, it will be displayed beneath the product name on the InfoHaus Web pages.

UPLOADING PRODUCTS BY FTP

Depending on the implementation you use, ftp can be almost as simple and intuitive a method of transferring files as any other type of file manager (e.g., Windows File Manager). You can get a version of ftp for your personal computer as part of a TCP/IP network software suite (such as those sold by FTP Software and other software vendors), or you may prefer to use a freeware or shareware version downloaded from the Internet. In either case, you should check with the software publisher for complete instructions in using ftp to transfer files (for more general information about using ftp, there are many books you should consider, including *TCP/IP for Everyone* by Pete Loshin, AP Professional, 1995).

To upload your products to the InfoHaus, connect to the host:

```
ftp.infohaus.com
```

Login with the user name "ftp" and enter your e-mail address as the password. If you use a GUI version of ftp, you then select the files you want to transfer and upload them to this directory on the InfoHaus ftp server:

```
/infohaus/incoming
```

Then, transfer your product files to this directory. Don't be surprised if your ftp client shows this directory to be empty, even after you've uploaded your files. Remote users are given only minimal privileges on this system (or any other First Virtual system connected to the Internet), so you won't be able to delete your files from the incoming directory — and no one else can. No one else can read your files (which would mean being able to access your products without paying), either.

Be sure to keep notes on what files have been uploaded, and what product names you plan to give those files. You can also upload files to serve as the free portion of your products at the same time. As always, keep track of what files are intended to be free so you can later refer to them when checking in your products.

UPLOADING PRODUCTS BY E-MAIL

If your product can be expressed as text and included in the body of an e-mail message, you can upload it at the same time you register the product, all in a single (possibly large) e-mail message. However, if your product is a binary file of some sort, such as a graphics image, a compiled program, or some other type of non-text file, you will have to use ftp to upload it to the InfoHaus server. Full instructions for registering and uploading products by e-mail are provided later in this chapter.

CHECKING IN PRODUCTS BY TELNET

Follow the instructions for connecting to the InfoHaus telnet server provided earlier in this chapter, and instead of selecting "N" to generate a newseller-request, enter the letter "C" to "check-in" a new product (see Figures 8-1 and 8-2). You will be prompted for the following information, in turn:

- Your business name (the "doing-business-as" name selected when you registered your storefront).
- The VirtualPIN associated with the seller's account.
- Product name. This is the complete hierarchical name, as demonstrated in Table 8-1.
- Product price, in the default currency. For example to price a product at US$9.95, enter "9.95" and the system assigns the correct currency value to it.

You will next be prompted for the free portion of the product, followed by prompts for the data portion of the product. The process of identifying both these parts is the same. In either case you have the option of typing in some text to describe the product, or of entering the name of a file you have already uploaded. If you did not upload a file, you can just press the Enter key and type your description.

If you did upload a file, you must enter its name exactly as you uploaded it. You will then have to answer two multiple choice questions about the file contents. The first question is shown in Figure 8-11. It asks for information about what type of data is contained in the file.

```
==== MULTIPLE CHOICE QUESTION ====
What kind of data is in the file fvhint.txt?
                1  - text
                2  - image
                3  - audio
                4  - video
                5  - MIME
                6  - other
Please enter your choice as a number from 1 to 6.
Enter a blank line to use the default answer, 1
```

FIGURE 8-11 *Describing product files to the InfoHaus server. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The file types should be largely self-explanatory. However, wherever possible you should try to determine the appropriate type if the product file is not one of these. If you choose "other" here, you will be prompted as shown in Figure 8-12.

```
==== MULTIPLE CHOICE QUESTION ====
What kind of data is in the file fvhint.txt?
                1  - application/postscript
                2  - application/safe-tcl
                3  - other
                4  - unknown
Please enter your choice as a number from 1 to 4.
Enter a blank line to use the default answer, 1
```

FIGURE 8-12 *Describing "other" product file types to the InfoHaus server. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

In general, the InfoHaus server will do "the right thing" with your files even if you are not sure exactly what type they are.

INSTALLING PRODUCTS BY E-MAIL

As mentioned previously, you can use e-mail to register and upload your products at the same time. However, this will work only if you can include your product as text within the body of the message. Registering by e-mail is recommended only for those merchants who absolutely have no access to direct Internet connections and ftp and telnet client software — or those with sufficient expertise in converting binary files into a suitable format for inclusion in e-mail.

To register your product by e-mail, you need to start by addressing a message to this address (the subject line does not matter):

```
mimeserver@infohaus.com
```

The first line of the message body should look something like this, and should be followed by a blank line:

```
Content-Type: multipart/FV-infohaus;
                boundary=abcdefg1234567
```

This defines the content-type of the message. In this case ("multipart/FV-infohaus"), it is a message containing more than one type of information as defined for the InfoHaus. The boundary parameter defines a set of characters to be considered as the boundary between the parts of the message. In this case, when the characters "abcdefg1234567" appear in the message it means that a new section is beginning.

If you break this data into more than one line (as shown here), the extra lines have to begin with a space. This holds for other parameters to be included in this message.

This defines the top of the product registration message; as mentioned, you must leave a blank space after the content-type information and type the boundary characters on the next line, preceded by two hyphens, as shown here:

```
-- abcdefg1234567
```

This indicates the start of another "part" of the message. The next line tells the server what kind of content is in this part:

```
Content-Type: application/FV-infohaus;
                transaction=addition-request
```

This indicates that this part is an "addition-request transaction," or a request to add new product. This should be followed by a blank line, with each of the following data items required for adding a new product on its own line:

```
Doing-Business-As: <name of your business>
Account-ID: <your seller VirtualPIN>
Info-Name: <product name>
Price: <product price>

 -- abcdefg1234567
```

This block of information is also set off by a space, followed by another boundary marker. The next section is devoted to the free part of the product, and can be nothing more than plain text describing the product. To be more formal, or to include content beyond plain text (HTML-tagged text, for instance), you would also define this section's content-type. Again, you would leave a space after the content-type definition, followed by the content itself, followed by:

```
Content-Type: text/plain

<Descriptive matter explaining what the product is, to be displayed
for free. This may be a simple text file, or some other type of file
(in the latter case, a different content-type would be in order).>

 -- abcdefg1234567
```

The last part of the message contains the paid portion of the product; it uses the same type of format as the free part. Since it is the last part of the message, it includes a termination boundary that is preceded and followed by two hyphens. The rest of the message might look something like this:

```
Content-Type: text/plain

<The contents of the product being sold. This may be a simple text
file, or some other type of file (in the latter case, a different
content-type would be in order).>

 -- abcdefg1234567 --
```

Figure 8-13 shows what an actual e-mail request to add a product might look like.

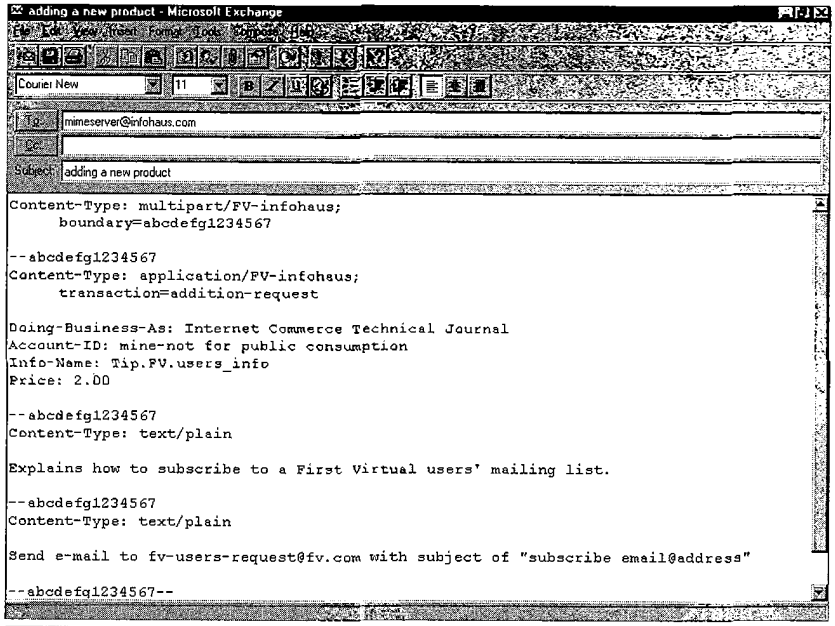


FIGURE 8-13 *An e-mail request to add a product to the InfoHaus. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

ADDING HTML TO YOUR INFOHAUS STOREFRONT

You don't have to settle for simple text descriptions of your products and store on the InfoHaus. However, if you want your shop description to use special formatting, such as bullet lists, or if you want to include hypertext links to other Web sites, you can do so by sending e-mail to:

```
mimeserver@infohaus.com
```

and specifying a content type of "multipart/fv-infohaus"; a sample message with HTML tags is shown in Figure 8-14.

The example in Figure 8-14 will work as a newseller-request, while you can also change the description of an existing shop

by sending the same message but using a transaction attribute of "seller-modification-request" instead of "newseller-request" as shown in the example.

```
Content-Type: multipart/fv-infohaus;
boundary="0987654321ZYX"

 - 0987654321ZYX
Content-Type: application/fv-infohaus;
                transaction=newseller-request

Doing-business-as: Wiggly Worm Weekly
Account-ID: buzz-eensy beensy spider
 - 0987654321ZYX
Content-type: text/html

<p>This is a paragraph.</p>
<ul>
<li>List item number one.
<li>List item number two.
</ul>
<p>Link to <A HREF="www.loshin.com">author's Web page</A></p>
 - 0987654321ZYX -
```

FIGURE *The format to use when adding an HTML-tagged InfoHaus shop description in an e-mail message (the To:, From:, and Subject: headers are not shown here). Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

Please note that you should *not* create your HTML-tagged description as a complete HTML document, as it will be inserted into more complete documents — the InfoHaus shopping pages. Thus, you should not use header tags such as <HTML>, <BODY>, or <TITLE>.

If you do add HTML tags to your shop description, be sure to visit your store as soon as possible to do some quality control. Improperly coded tags can cause problems for the display of your own storefront as well as those of other InfoHaus merchants.

INFOHAUS PERIODICALS

Many information products will take the form of periodicals: items that, individually, are not of sufficient value to pay very much for, but for which payment can be aggregated and delivery taken over a period of time. In other words, a subscription service. InfoHaus periodicals can be e-mail versions of traditional-style magazines or newsletters, or can be any other type of product for which customers will pay in advance for a series — like "joke of the day" or "picture of the day" products.

The InfoHaus allows two types of periodicals. The first is called a "boxset" and the second is called "volume" or "magazine." A boxset consists of all available pieces of the periodical, plus any additional pieces that may become available later. For example, you might sell a novel as a boxset, making the first few chapters (the ones you've already finished) available immediately and the right to see all the future chapters as they are completed.

The volumed periodical, or magazine, functions much like a real magazine. Customers can subscribe for a set period of time, paying a flat rate for each "volume" and starting delivery with the current issue of the current volume. When the subscription is up, the subscriber gets another transfer-request to continue the subscription. If the request is approved, the subscriber won't miss any issues of the periodical. Back issues may be available, but are not included as part of the paid subscription.

The big difference between boxsets and volumed periodicals is that the boxset includes all the members of the set, whether they have been issued or not; the volumed periodical includes

the current issue and one volume's worth (it may be a single year) of future issues.

When creating a periodical, a "magic e-mail address" is also created. The merchant sends e-mail messages to this address to create new issues of the periodical.

Subscribing to a Periodical

Customers can subscribe to a periodical in much the same way they make other First Virtual purchases. However, they also need to include an e-mail address to send periodical issues. Subscriptions can be submitted by e-mail to the address:

```
subscription@infohaus.fv.com
```

or through fill-in forms available on the InfoHaus Web pages. The subscriber must provide the following information:

- Seller: The merchant's DBA name.
- Buyer: VirtualPIN to be billed.
- Info-name: Name of the periodical.
- Email-address: E-mail address to which to deliver periodical issues.

Creating Periodicals

Periodicals are created in essentially the same way as any other InfoHaus product, except that there are some additional attributes required to describe how subscriptions are to be done.

"Periodical-volume" indicates the periodical is either volumed or a boxset. Values allowed for this attribute when creating a new periodical are either "newvolumed" or "newboxset."

"Periodical-subscription-price" is the price for subscriptions and renewals. This may be changed at a later date relatively easily, at the start of a new volume or even between issues of the same volume.

Other attributes relating to periodicals include "periodical-paid-part-only"; "periodical-send-addition-results"; and "periodical-payment-optional." These are usually not set by the merchant, but may be if some value other than the default is desired.

Adding Issues to a Periodical

New issues are added to periodicals using the same info-name as the original periodical by setting the "periodical-volume" attribute either to "nextissue" or "nextvolume." "Nextissue" causes all subscribers to receive a copy of the information item; "nextvolume" (which is valid only for volumed periodicals) will create a free item to start a new volume of the periodical.

As mentioned above, you can also send an issue to the "magic e-mail address" that you receive when you create a new periodical. If you indicate a Subject: line of "nextvolume," the message becomes a free item describing the next volume of the periodical; otherwise, it is treated as a new issue. These items are automatically delivered to all periodical subscribers.

CHAPTER NINE

SELLING FROM YOUR WEB SERVER

Contents

WHAT YOU NEED TO GO ONLINE 245
Hardware, Software, Services 246
Hardware 246
Software 247
Services 247
If You Outsource Your Web Site 248

FIRST VIRTUAL RESOURCES 249
Using First Virtual Programs and Templates 250
Using the First Virtual Web Site 251
Scripts, Templates, and More 253

THE SELLING PROCESS 254
Initiating a Transaction 254
Using E-mail 255
Using telnet 256
Using the Simple Green Commerce Protocol 257
Making Sales off the Internet 257
Verifying a Buyer's VirtualPIN 258
Finger 258
Telnet 259
E-mail 260
Using the FV-API 260

INFOHAUS HTML FORMS 261
Emailform 261
Emailpayform 263

CGI SELLING TOOLS 265
Member 265
Installing and Running Member 266
Websale 268
Using Tcl 269
Installing Websale 269

THE FIRST VIRTUAL API 269
Getting and Installing the First Virtual API 271
FV-API Operations 271
Autosell URLs 271
Manusell URLs 272
Formsell URLs 272

Summary If you can run CGI scripts on the Web server you use to publish your information, you can use First Virtual to collect payment for your products, both information goods and hard goods. This chapter explains how to use sample CGI and HTML forms to sell your goods from your own Web site.

First Virtual offers a complete solution for Internet commerce for the shoestring startup operation: digital transactions plus Internet service through the InfoHaus add up to a simple, low-cost Internet storefront. However, that answer is not for everyone. For example, you would probably want to First Virtual–enable your own Internet servers if any of these is true:

- You need to sell hard goods on the Internet.
- You are able to manage your own Internet server, and already have one up and running.
- You started out with the InfoHaus, and the 8% commission you pay for the service is higher than what you would pay to maintain your own Internet servers.

Determining when to move up to your own server from the InfoHaus depends entirely on your own situation. At one end of the spectrum is the individual with minimal computer experience, minimal computer equipment, and no employees, friends, relatives, or co-workers with Internet expertise. This person would need to make a large investment of money (to buy an Internet server, software, and Internet connection) and time (to learn how to install, configure, maintain, and administer the server; to create the Internet storefront — and to enable the server to accept First Virtual payments).

At the other end of the spectrum, you may already have access to an existing Internet server — for example, "rental" space on an Internet presence provider's system, or space available through some other type of affiliation. You may also have access to Internet and systems expertise through your own experience or through that of a friend, relative, employee, or colleague. If this is the case, then enabling your server to accept First Virtual payments may be a good deal.

Merchants selling hard goods, however, cannot take advantage of the InfoHaus; they must provide their own server. Also, as of early 1996, as a result of the passage of the Communications Decency Act, First Virtual merchants offering "adult" products (most often, images or other depictions of nudity or sexuality) are not permitted to use the InfoHaus and must make other arrangements. At this time, First Virtual is expected to allow third-party vendors license the InfoHaus software so that adult product sellers can continue to use the First Virtual system without having to set up their own servers.

WHAT YOU NEED TO GO ONLINE

It seems that everyone, from the largest corporations to school children, has a World Wide Web page now. If you decide to put up your own page to sell your product, consider that some of the corporate sites are estimated to cost as much as a million dollars or more to create, and many thousands of dollars to maintain every month. Even if you decide to have your Web site hosted by an Internet presence provider to save the costs of buying and maintaining the hardware and software, you still need to design and produce your site "content." Depending on your provider, you may be able to enable your site to accept First Virtual payments yourself, or they may be able to do it for you.

This section should help you determine whether you want to set up your own server, as well as help you decide on an Internet presence provider — knowing what's involved in putting an Internet server up will help you ask providers the right questions before you sign up.

Hardware, Software, Services

If you decide to go it on your own, you'll need to invest in computer hardware and software, as well as arrange Internet connection services. The biggest expense is likely to be your time, particularly if you don't already have experience in setting up Internet servers. I have omitted pricing information on these items, since you can pay almost anything you want for any of them. For example, suitable used computers may be available for well under $1,000 each; there are free or inexpensive versions of operating systems, TCP/IP stacks, and Web servers; and Internet service providers usually price their services very competitively.

HARDWARE

The Internet protocols defining applications such as the World Wide Web are designed to be portable across virtually any type of computer that can be connected to a network. As long as someone has written the appropriate software to run TCP/IP network applications on a platform, you could use that platform to be your Internet server. This presumes, of course, that you can connect the platform to the Internet through an appropriate network device (modem, ISDN adapter, Ethernet or other type of network card).

In practice, however, you will need a computer capable of multitasking with sufficient horsepower to handle peak period demands. While the software and network connections are available to turn Macintosh or Windows/Intel personal computers into Internet servers, the preferred platform for Internet servers is still a UNIX computer. Ultimately, however, the platform you choose will depend on the amount of traffic you expect to handle.

Very popular Web sites may have to deal with hundreds of thousands of "hits," or requests for data from clients, daily. However, unless your Web site offers something important to a very wide audience (such as indexing services to the World Wide Web), or to a narrower audience on a regular basis (such as stock quotes or daily news items), your Web site will not require a huge investment in hardware. It is entirely possible for a 486-based personal computer running Windows NT to support a modest Web site.

SOFTWARE

You'll need appropriate operating system software: this could mean Windows NT, some flavor of UNIX, or some other operating system. Some operating systems include TCP/IP, while for others it must be added on; in either case, you must have it. You'll also need a Web server package, so you can publish your information on your server. There are other tools you may want to add, even though they are not required: Web server auditing software to track your customers' visits; Web editor and management software to make it easier to create your content; "shopping cart" software to allow your customers to mark items they want to buy before making payment.

SERVICES

If you do it all yourself, you'll also need to get your Web server connected to the Internet. At the low end of the scale, you can get a personal Internet account through your local Internet service provider, set up a dedicated telephone line for your Internet connection, and just dial in. However, to keep your customers happy with better performance, you would more likely contract with your Internet service provider to set up some kind of a dedicated communications link in conjunction with your local telephone company (which is usually

billed through the telephone company). This link is for handling your Internet service (carrying all your Internet traffic), which is usually billed through your Internet service provider.

There are other services you might be interested in considering. For example, there are consultants who will register your Web site with search engines. This may be a worthwhile deal, as long as you know what you are getting. Check references, and also be sure you understand what you're getting. While this task can be time-consuming, some merchants may prefer to do it themselves.

As with any other medium of communication, there are a multitude of specialists who can help you create your content, design your Web pages, place ads, and provide marketing and management consulting. Quality and experience vary widely, so be careful before making any commitments.

Managing an Internet site can be a full-time job in itself, requiring constant monitoring of the site, the systems involved, and the content. Internet systems administrators need to understand the Internet, TCP/IP networking, system and network security, and more.

If You Outsource Your Web Site...

You may not want to go to all the trouble of building your Web site from scratch, but you may also want more options and control over your content than the InfoHaus can offer. There are many organizations offering Web services through their own Web servers. These companies maintain Web servers and allow subscribers to load their own HTML documents on the server. However, to accept First Virtual payments through these servers, you'll need to be able to load

CGI scripts — something that not all Internet presence providers are willing to allow. Discuss this issue with your provider before you make any commitments, and they may be eager to accommodate your desires (particularly because the scripts can be used by any other subscriber who wishes to become a First Virtual seller).

Another alternative is to continue to use the InfoHaus to handle your transactions, but to use some other Web site to publish your products. This option is discussed in the section of Chapter 10 that discusses adding forms to your InfoHaus storefront.

FIRST VIRTUAL RESOURCES

It is in First Virtual's best interest to make it as simple as possible for new merchants to become enabled to accept First Virtual payments. However, commerce-enabling a Web page can require a higher level of expertise (as well as customization) than setting up a customer's new account. As a result, it is recommended that merchants wishing to First Virtual–enable their servers should have some experience working with CGI and HTML, as well as with their operating system.

First Virtual has made various resources available to merchants at no charge — but also with no guarantees or support. If you are thinking about configuring your server to accept First Virtual payments, there are excellent resources available directly through First Virtual. Published on the First Virtual Web pages are many documents, sample HTML and CGI code, and other software to run on servers to enable them to accept First Virtual payments. Most of the software is designed and tested on UNIX systems, although the HTML and CGI scripts are very likely to be portable to other operating systems. In all

cases, however, First Virtual provides this software freely, with no guarantees and with no formal support.

While many of the same scripts, templates, and software available on the First Virtual Web site have been reproduced on this book's companion CD-ROM, you are urged to check the First Virtual Web site periodically for new offerings, changes, and additional support materials.

The First Virtual users' mailing list is another resource that may be of value to merchants. It is discussed in Chapter 5. It puts you in touch with other First Virtual customers and lets you ask and answer questions about using the First Virtual system.

Using First Virtual Programs and Templates

The various programs and templates that First Virtual provides through its Internet server are offered to users strictly as a convenience. First Virtual makes these works available freely, though not as public domain works, and makes very clear that they are offered for use "as-is" and with no warranties. You may choose to use them, but you should not expect any technical support from First Virtual if you do. Be sure to read First Virtual's disclaimers before using any of the software tools they provide.

Most of the programs and templates discussed in this chapter are available from the First Virtual Web site, as well as on the companion CD-ROM. If you choose to use these programs and templates, you should have at least some expertise in system administration, HTML and CGI programming, use of C compilers, shell programs, and other systems tools.

If you don't have these skills, you may want to consider using a consultant to set up your server to accept First Virtual pay-

ment. Another option is to use third-party software, as discussed in Chapter 10.

Using the First Virtual Web Site

Figure 9-1 shows a map of the First Virtual Web site, as of early 1996. This page is reached through the First Virtual help page, and it points you to different pages dealing with different First Virtual topics, but does not show all pages on the site. For more detailed guidance, you can click on a link on this page (not shown in the figure) to go to a comprehensive text hierarchical listing that shows all pages. This hierarchical list may be most useful when you are looking for specific technical information, software, scripts, or templates.

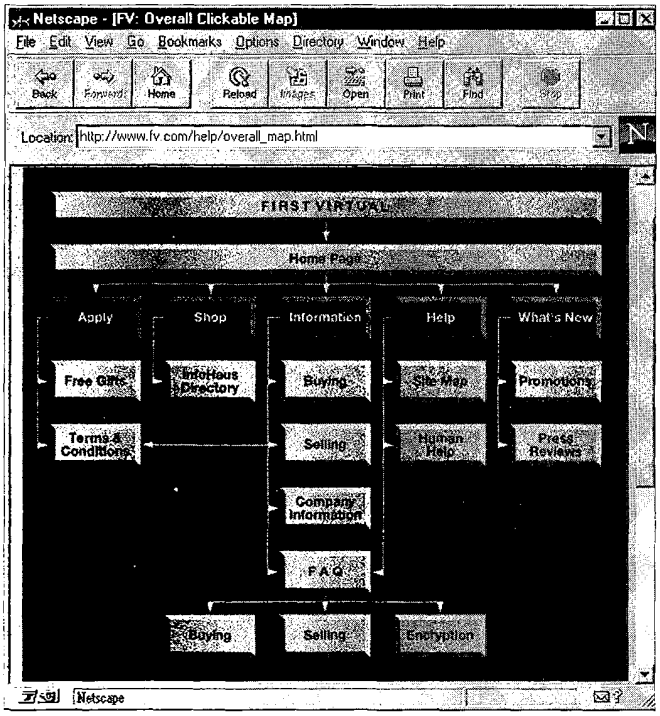


FIGURE 9-1 *A graphical mapping of categories on the First Virtual Web site. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The Help button, available on most pages, will reach another useful page for getting oriented within the First Virtual Web site. As shown in Figure 9-2, this page points you to the most important parts of the First Virtual Web site. It links you to more information resources such as the site map and the text hierarchy, as well as help in reaching a human at First Virtual, a Frequently Asked Questions list, and help on managing your account.

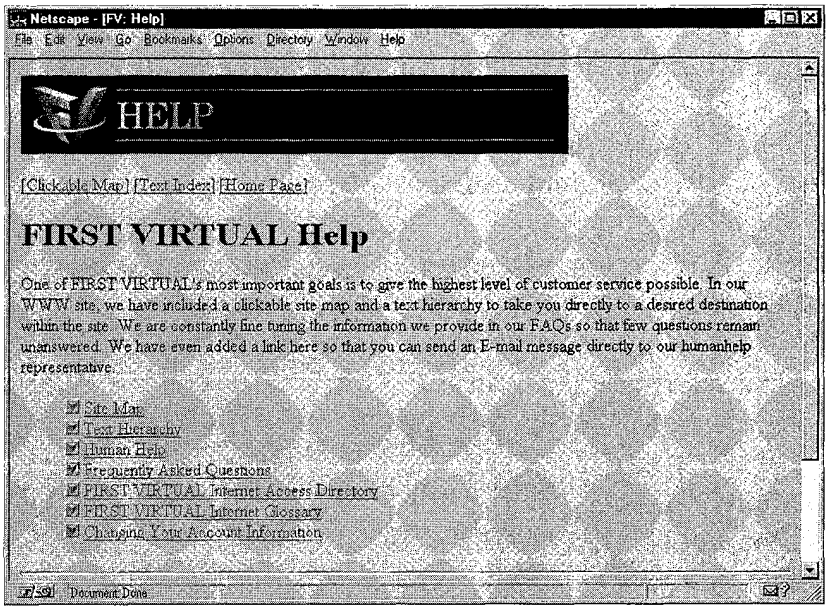


FIGURE 9-2 *The First Virtual Web site Help page. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

Another important page, shown in Figure 9-3, is the Information page. This page can be reached by clicking on the "Information" button at the bottom of most pages in the First Virtual Web site. It offers links to information specific to buyers and to sellers, as well general and technical information.

Not shown in Figure 9-3 are additional links on the Information page. These include more information, such as

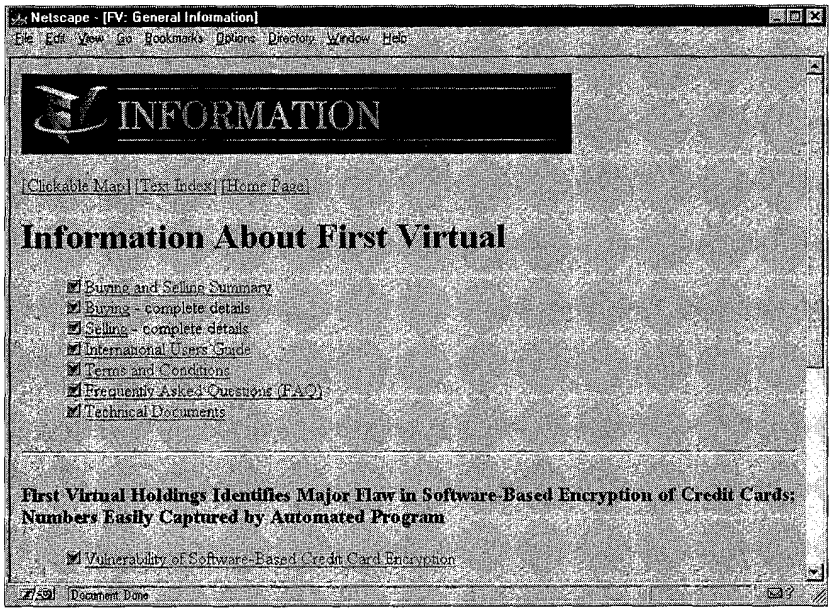


FIGURE 9-3 *The First Virtual Web site information page. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

pointers to articles mentioning First Virtual, company background, career opportunities at First Virtual, and various background papers about Internet commerce.

Scripts, Templates, and More

Available for download from the First Virtual Web site (as well as by anonymous ftp) are several different tools for making it easier to accept First Virtual payments. These include special HTML forms you can use to collect information and make sales through your InfoHaus storefront; CGI scripts called "MEMBER" and "WEBSALE" which can be used to set up forms on your own Web server; and the FV API (First Virtual Application Programming Interface) scripts, which you can use to customize your own programs to perform First Virtual functions automatically.

THE SELLING PROCESS

Selling through First Virtual is an orderly process that can be done manually or automatically, by computer or by hand. This section outlines the process itself, while later sections discuss how to use various tools to automate the process.

Initiating a Transaction

You can use several different Internet applications to initiate a First Virtual transaction. In all cases, however, you will need to provide at least the following information:

- The buyer's VirtualPIN.
- The seller's VirtualPIN.
- The sale amount.
- Currency (e.g., U.S. dollars, expressed as "USD").
- Transaction description (up to 40 characters).

The transaction itself can be carried over the Internet using several different methods:

- Manually entering a correctly formatted transfer-request in an e-mail message and sending it to First Virtual.
- Using a program or script that generates a correctly formatted transfer-request in an e-mail message, and then sends it to First Virtual.
- Manually entering a transfer-request through the First Virtual telnet server.
- Automating the process of putting together transfer-request information with software provided by First Virtual.
- Directly sending transfer-requests to First Virtual using software you write yourself (or have written for you) using the Simple Green Commerce Protocol specification.

- Directly sending transfer-requests to First Virtual using HTML forms that automatically send their contents to a special FIRST VIRTUAL address for processing.

USING E-MAIL

Transfer-requests can be submitted by e-mail to the address:

```
transfer@card.com
```

The information noted above as being required for transfer-requests must be included, as formatted in Figure 9-4. The subject line is not necessary and can be anything you like.

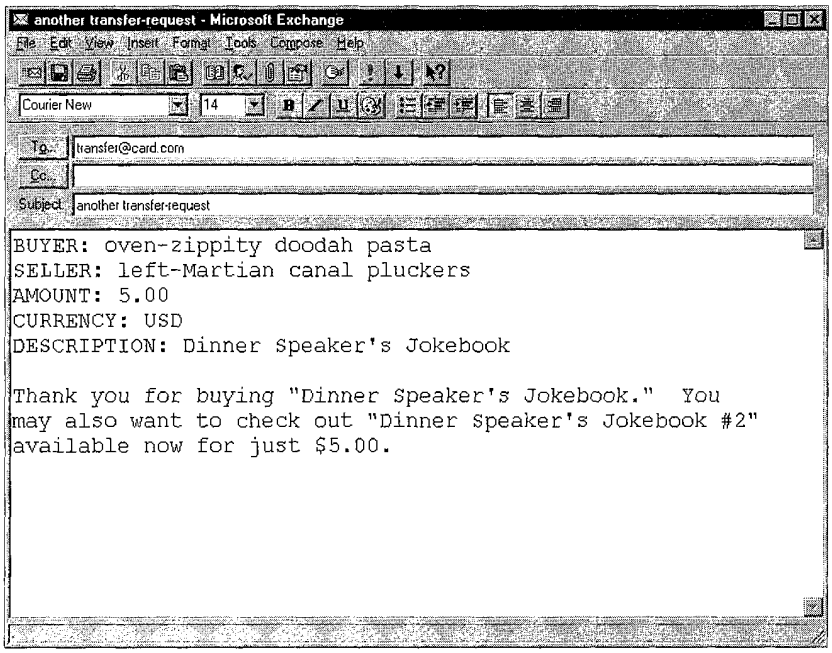


FIGURE 9-4 *Composing an e-mail message submitting a transfer-request. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

The example shows the minimum information that is required. Adding a description after a blank line after the last field will

cause that message to be delivered to the buyer. You can also add other optional items. For example, you can include other fields defined for First Virtual transactions:

- TRANSFER-TYPE: This defaults to "info-sale" but may also be "goods-sale" or "donation."
- TRANSFER-ID: This is a short string appearing between angle brackets to give the transaction your own ID number. It must include one "@" sign in it, like this: "<PQL-001@loshin.com>".
- SECURITY-REQUIREMENTS: If you are selling hard goods, you should set this to "x-pgp-transfer-notification" to receive digitally signed transfer notifications of sale authorizations.
- DELIVERY-STATUS: This field is ignored by First Virtual, but is passed along to the buyer if it is used. It can be either "pending" or "delivered."

When creating the message, you must keep in mind the following formatting requirements:

- Each field gets its own line, and the field name must start at the start of the line (no leading spaces).
- Each field name must be followed by a colon and one space, followed by the value for the field.
- The value for the AMOUNT field should be a number only — do not include any currency symbol with the value.
- The DESCRIPTION field can be up to 40 characters long, and should include the name of the product being purchased.

USING TELNET

To initiate a transaction via telnet, connect to the First Virtual telnet server:

```
telnet.card.com
```

Choose the "*funds transfer*" option from the menu after you log on, and respond to prompts for buyer and seller VirtualPINs as well as for sale amount, currency, and transaction description.

Telnet-initiated transactions don't permit the use of any optional fields, so if you are selling hard goods or wish to use any other of the optional fields, you will need to use e-mail or direct SGCP. There is also no way to enter a message from the seller by telnet.

USING THE SIMPLE GREEN COMMERCE PROTOCOL

Most users of First Virtual will rely on e-mail to deliver transfer-requests. Most of the free tools available at the First Virtual Web site use e-mail, even the relatively complex solutions described below. Rather than relying on entering transfer-requests through intermediary systems, that is, via e-mail or through a telnet server, you can submit them directly to First Virtual through applications using the SGCP protocol (see Chapter 4 for more details on the protocol itself).

Doing so requires the creation of special application software using the First Virtual API (application programming interface), which is a set of C language routines that can be adapted to your own programs. Programming techniques are beyond the scope of this book, but instructions for getting the FV API are included later in this chapter (the FV API and related documentation is included on the companion CD-ROM as well).

MAKING SALES OFF THE INTERNET

Because First Virtual relies on specific procedures rather than accessibility to systems or software, it is possible to make sales

through any medium. This means collecting transaction information from customers in person, over the telephone, or by postal mail, and then submitting transfer-requests to First Virtual through the Internet.

It is important, however, to remember that the merchant assumes the entire risk on nonpayment for all transactions. This means that merchants should use First Virtual for off-Internet sales only to the extent that the transactions are small enough that nonpayment is not likely to negatively affect their livelihood. Furthermore, wherever possible, merchants should attempt to use First Virtual for transactions that are unlikely to be declined by customers.

Verifying a Buyer's VirtualPIN

One important merchant function is the verification of the buyer's VirtualPIN. You may want to verify VirtualPINs before delivering information to a customer, or at least before submitting a transfer-request. Account verification can be done several different ways, using Internet applications.

FINGER

Finger is a standard Internet information utility. When a system connected to the Internet receives a finger request, it returns certain information about users of that system. Finger is most commonly found on UNIX systems, but there are versions available for virtually any computer.

To use finger to verify a VirtualPIN, use the VirtualPIN (without any spaces or punctuation) as an account at the system card.com. The VirtualPIN "fine-Perky, Pretty, and Pink!" would be entered as "finePerkyPrettyandPink". For example,

if you are running finger from a command line interface, you would execute the command:

```
finger finePerkyPrettyandPink@card.com
```

Sample finger results are shown in Figure 9-5. In the first instance, the VirtualPIN is not valid, and in the second instance it is. Note that when a valid VirtualPIN is indicated, the account holder's full name, preferred language, and currency are displayed — as well as the date and time of the last change made to the account.

```
unix% finger blah@card.com
[card.com]
Trying 199.100.120.2...
Content-Type: application/green-commerce; transaction=inquiry-result

Account-ID: blah
Account-Status: invalid

As of this writing, the account is invalid.

unix% finger someValidVirtualPIN@card.com
[card.com]
Trying 199.100.120.2...
Content-Type: application/green-commerce; transaction=inquiry-result

Account-ID: some-Valid VirtualPIN!
Account-Status: active
Full-Name: Pete Loshin
Preferred-Currency: usd us dollars
Preferred-Language: EN
Last-Change: Sun, 24 Dec 1995 02:28:01 +0000
Seller-Type: normal

As of this writing, the account is active.
```

FIGURE 9-5 *Running finger on a UNIX system to verify VirtualPINs. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

TELNET

If you use telnet to submit transfer-requests, you may get immediate feedback as to validity of the VirtualPINs used by

your customers. However, you may want to verify VirtualPINs prior to submitting a transfer-request. To do so, connect to the host:

```
telnet.card.com
```

and select "I" to inquire about an account. You will be prompted to enter a VirtualPIN as well as a preferred language; the response will indicate either that the account is active or inactive. If active, it will also indicate the default currency. Note that this technique yields less information than fingering the account, as described above.

E-MAIL

You can also verify VirtualPINs by e-mail. Send a message, with the VirtualPIN you want to verify as the subject line, to the address:

```
inquiry@card.com
```

You will receive in return a message containing the account holder's name, preferred language and currency, and the date of the last change made to the account.

USING THE FV-API

Included with the FV-API program "fv" is a routine called "checkat"; use this to verify a VirtualPIN directly. The syntax for the command is:

```
fv checkat card.com <VirtualPIN>
```

This will return the status of the account represented by the VirtualPIN direct to your application.

INFOHAUS HTML FORMS

Even if you do have your own Web site, you may have neither the experience nor the inclination to fully enable it for First Virtual transactions. However, you may want to have more complete control over how customers access your information, and how your products are presented. One option is to set up an InfoHaus storefront, but keep it hidden and use the InfoHaus only for processing transactions. First Virtual provides a couple of HTML forms that you can adapt to do this. However, if you use this option, you must abide by all InfoHaus rules, as well as pay InfoHaus fees.

The following HTML forms use CGI scripts stored on the InfoHaus server; you can add and adapt them to your own HTML pages. If you would like more information about HTML and CGI programming, consider one of the sources cited in Chapter 10.

Emailform

This form can be used to acquire information from your customers and potential customers. For example, you can have customers provide you with their names, addresses, and other contact information, or even solicit comments from them. The sample HTML form included on the companion CD-ROM, called "emailform.html," can be used to collect a customer's name, VirtualPIN, and telephone number; it will deliver that information by e-mail to an address you specify. This form is shown in Figure 9-6.

The HTML code of this template is shown in Figure 9-7.

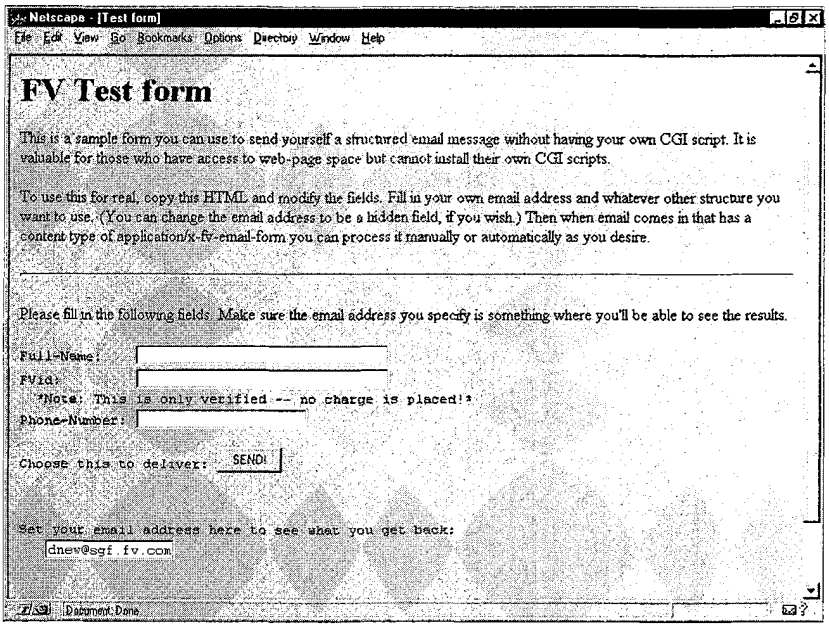


FIGURE 9-6 *Collecting information from customers through the InfoHaus, using the emailform.html template. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

```
<TITLE>Test form</TITLE>
<H1>FV Test form</H1>
<! - This goes in /h/httpd/htdocs/samp-cgi/emf.html>

This is a sample form you can use to send yourself a structured email
message without having your own CGI script. It is valuable for those
who have access to web-page space but cannot install their own CGI
scripts. <P>

To use this for real, copy this HTML and modify the fields. Fill in
your own email address and whatever other structure you want to use.
(You can change the email address to be a hidden field, if you wish.)
Then when email comes in that has a content type of application/x-fv-
email-form you can process it manually or automatically as you desire.
<p>

<hr>
<FORM ACTION="http://www.infohaus.com/fv/emailform" method=POST>
Please fill in the following fields. Make sure the email address you
specify is something where you'll be able to see the results.

<pre>
```

```
Full-Name: <INPUT type=text name=Full-Name maxlength=30 size=30>
FVid: <INPUT type=text name=FVid maxlength=30 size=30>
                *Note: This is only verified  - no charge is placed!*
Phone-Number: <input type=text name=phone-number>

Choose this to deliver: <input type=submit value="SEND!">



Set your email address here to see what you get back:
                <input type=text name=email-address
value="dnew@sgf.fv.com"
                maxlength=30 size=15><br>
</pre>
</FORM>
<hr>
Thank you for your interest in <IMG
SRC="http://www.fv.com/fvlogosmall.gif" ALT="First Virtual">!
```

FIGURE 9-7 *The emailform.html template code. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

This form uses the standard CGI post method of using forms and handling data collected through those forms. The FORM ACTION refers to the CGI script on the InfoHaus; input fields are defined using the <INPUT> tag.

There are some limitations on this form. You can add as many fields as you like to collect from the user, but you must include an e-mail address field (called "email-address") and a VirtualPIN field (called "FVid"). You do have the option of hiding these fields, by defining them as "type=hidden" in the <INPUT> tags.

Emailpayform

This form works very much like emailform.html, but has all the fields necessary to complete a sale. You can include this form in your InfoHaus storefront, or use it on your own Web server. Instead of just sending you e-mail with the customer's informa-

tion, it submits the transaction information to First Virtual. You will also receive an e-mail message with a MIME content type of application/x-fv-email-pay-form containing all the information gathered through this form, which you can use to take appropriate action. Part of this template is shown in Figure 9-8; the complete template is available on the companion CD-ROM.

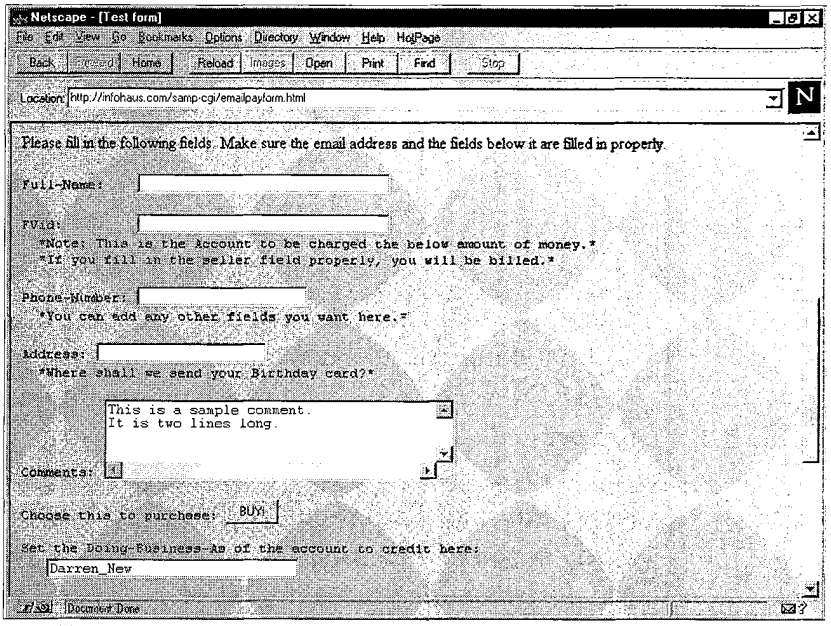


FIGURE 9-8 *Part of the emailpayform.html form, for making an InfoHaus sale through an HTML form. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

These HTML forms are useful for merchants who have their own Web pages but cannot put up their own CGI scripts. They use CGI scripts that reside on the InfoHaus server, and they require a valid VirtualPIN to be processed — and when the emailpayform.html form is used, they bill through the InfoHaus. This means that the InfoHaus fee (8% of the sale price) is incurred in addition to normal First Virtual transaction charges.

Also, when these form are submitted a First Virtual "thank you" response page is displayed. This may be inappropriate when the form is a request for information only.

CGI SELLING TOOLS

First Virtual provides two programs useful for merchants with some technical systems expertise. The first, called Member, is a CGI scripting mechanism that provides a convenient method for accepting membership fees. A second option is called Websale; although it is more complex, it is appropriate for merchants who wish to charge for retrieval of files from their Web server.

Both of these programs are included on the companion CD-ROM, as well as on the First Virtual Web site. Websale requires that Tcl, a script interpreter, be installed on the Web server as well. Tcl is available from First Virtual's Internet server.

Member

Member is useful for applications in which a customer makes a payment through First Virtual and there is no specific document immediately transferred from the merchant server. For example, Member is useful for collecting membership fees, contributions, or subscriptions.

Included with the distribution files are instructions (in the file called "README"), C program files, and other supporting files. Merchants wishing to use Member must have a C compiler and should be familiar with using it; also required are a Web server that supports CGI scripts, and access to certain

utilities on the server. While the code was written and tested on UNIX systems, you should be able to compile and install it under other operating systems. If you plan to install Member, you should either have sufficient system management skills or have a skilled system manager help you out.

Installing and Running Member

Member works like this: once it is installed and compiled, the merchant is prompted through an interactive process of creating a membership form. Member creates an executable program that you can install on your Web server, and which produces an HTML form for customers to fill out. Submitting the form submits a First Virtual transaction. All submissions must include fields called "FVid" and "price."

Member is distributed as a tar (tape archive format, a UNIX format) file, which includes all the necessary files. To install, unpack the files into an empty directory on your server and run the "make" program. This is the text of the questions you must answer:

- What is the name of your organization?
- Please enter a textual description of your organization. This text will be used as the initial text at the top of your WWW membership form. When you are finished, type control-D.
- Next, we need to know how much money you wish to charge people for membership. There are three basic options here. Either you can charge everyone the same amount, or you can have multiple membership categories (e.g., "normal," "student," etc.), or you can allow the user to fill in any amount he or she wants.

- If you wish to use a single price for everyone, please enter the price in U.S. dollars. If you wish to allow each user to enter the amount he or she wants to donate, type "any" (without the quotes) here. Otherwise just press RETURN now.
- Next, you will be asked to enter each of the different membership prices, and the descriptive name for each membership category (e.g. "student membership"). Please enter each membership category in turn, and then press RETURN alone on a line when you have entered them all.
- Enter a membership price, or press RETURN if done.
- Enter a description for the membership category (a description must be less than 40 characters).
- What description should be used for the charge?
- What is the e-mail address that should receive all e-mail regarding membership applications?
- What is your organization's First Virtual account-id, to which all money that is received should be credited?
- What is the name of the server this Web page will run on?
- Where is the "finger" program on this system?
- Where is the "sendmail" program on your system?

Fields for the user's name, company, address, city, state, zip code, phone, fax, e-mail, VirtualPIN, and comments are included by default in the resulting Web page, but the merchant can add more fields if they are desired by answering a prompt for them. These fields will be included in an e-mail message sent to the merchant, but won't be forwarded to First Virtual.

After compiling the results, you will have a program called "member" which should be copied into the cgi-bin directory. This program should be called as a URL from a browser using CGI, and should result in a usable form. If you want to modify the form, you can edit the HTML files in the Member

directory, remembering not to change any of the file headers or other structures. For instance, the "content-type" line, and the blank line following it, should not be altered. The "FVid" and "price" fields must not be altered, either.

If you want to add fields for customer information to be sent to you by e-mail, just add the fields using names starting with the string "QS_" in the file "membership.html," and run the "make" program again.

If you want to change the product price, address to send e-mail notification (and extra customer information) to the merchant, or product description, you can edit the file "config.h" to make the changes.

Websale

Whereas the Member program will walk you through the process of creating a membership form page for your Web server, the Websale program allows you to create Web pages that include links to special CGI scripts. These links allow you to offer files for sale directly through First Virtual by submitting transfer-requests by e-mail.

Websale requires system management skills, as well as the ability to run CGI and the Tcl interpreter on your Web server. Your programs must also have access to system programs "cat," "sendmail," and "date" so that e-mail messages, both to the merchant and to send transfer-requests to First Virtual, can be generated.

Websale is distributed in a tar file. It includes a Tcl program file as well as a document explaining how to install and con-

figure the program. The Websale distribution file is available on the companion CD-ROM, as is a version of Tcl.

USING TCL

Tcl is a text-based language designed to issue commands to command-line programs (such as UNIX shell programs). First Virtual distributes a version of Tcl, called safe-Tcl, which includes special extensions to make it easier to automate transactions through e-mail. The safe-Tcl tar distribution file is included on the companion CD-ROM and is also available directly through First Virtual's Internet servers.

INSTALLING WEBSALE

Websale is designed to run "out of the box" on UNIX systems. Included in the distribution file are instructions for installing it. However, unless you are familiar with UNIX system management and have full root access, you may not want to attempt installing Websale by yourself. Instructions are included in the file "websale.doc" included in the Websale tar distribution file.

THE FIRST VIRTUAL API

One way or another, the selling tools discussed so far in this chapter have interacted with First Virtual's system through e-mail. This is a perfectly acceptable method of interacting, but since Internet e-mail is a "store-and-forward" medium, it can be subject to delays, depending on the status of intermediary systems. These tools also offer relatively little in the way of customization and configurability, although they can be

adapted for use in many different situations — and they are relatively easy to use.

Merchants who require more immediacy, more sophisticated interaction between customer and merchant, or a higher degree of automation of the selling process can use the First Virtual API (application program interface) software to develop their own transaction-enabled applications. The FV-API is a set of C library routines that can be used to perform First Virtual merchant functions such as:

- Calculating the cost of a file to be purchased, based on its size or location.
- Submitting transfer-requests.
- Verifying VirtualPINs.
- Charging customers for access to a particular Web page.

These routines can be called from within UNIX shell scripts, CGI scripts, or C programs.

While some of the other software tools described here require some familiarity with systems management and networking, using the FV-API calls for real programming skills. As with the other software described here that First Virtual offers freely to their users, the FV-API includes a disclaimer:

> FIRST VIRTUAL MAKES NO REPRESENTATIONS ABOUT THE ACCURACY OR SUITABILITY OF THIS MATERIAL FOR ANY PURPOSE. IT IS PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES.

If you choose to use it, you should not expect any support from First Virtual. Before using it, you should be sure that there is not some other, simpler solution for your situation; if you do decide to pursue this course, you should be sure that

you have the proper skills to use the FV-API (or have hired a consultant with those skills).

Getting and Installing the First Virtual API

The First Virtual API is distributed as a tar file and can be retrieved from First Virtual's Internet server by anonymous ftp from the host "ftp.fv.com"; the URL is:

```
pub/code/fv-api/fv-api.tar
```

FV-API is also available on the companion CD-ROM. Also available is a document called "fv-api.txt" that describes how to install and use the FV-API utilities. Another document, "fv-api-spec.txt," describes how the FV-API utilities work, and how to use them with other programming tools.

FV-API Operations

There are three types of transactions that can be enabled using FV-API and CGI scripts also available from First Virtual (also available on the companion CD-ROM). These help make it easier to sell your products from your own server.

AUTOSELL URLS

An autosell URL is used to advertise a paid file for sale without also offering a free part of that file. This approach works well when you want to offer many different files for sale, without having to create description files for each paid one — very useful if you are selling files stored on an ftp server.

Autosell URLs can be set up to allow the customer to access the same file more than once over a predetermined time without having to pay again.

MANUSELL URLS

These function much like autosell URLs, except that instead of billing users depending on the content of the URL itself, charges are based on configuration information stored in the file the URL points to.

FORMSELL URLS

If your product consists of the contents of a database, you may prefer to sell the results of searches on that database rather than the database itself. Using a formsell URL, you can have the user fill in CGI forms to define a search and then charge the user depending on the results of that search. For example, you could charge customers $1 for each record retrieved from your database.

CHAPTER TEN

TIPS, TRICKS, AND POINTERS

Contents

TIPS FOR EVERYONE 274

TIPS FOR INFOHAUS MERCHANTS 275

GETTING YOUR STORE LISTED. 279

COMMERCIAL OPTIONS FOR MERCHANTS 280

MAKING TEST SALES THROUGH FIRST VIRTUAL. 281
InfoHaus "QuickBuy" Numbers 282

LEARNING MORE ABOUT HTML AND CGI. 284
Getting Help from the World Wide Web 284
Books about HTML and CGI. 285

Summary First Virtual is, by design, a relatively simply way to transact business over the Internet. That doesn't mean there aren't ways to make it easier. This chapter offers some special tips and tricks for the First Virtual merchant, as well as some pointers to more helpful resources and some vendors offering special products and services.

Whether you're looking for a way to make using First Virtual easier for you or for your customers, you'll find that your problem is very likely not a new or unique one. First Virtual consumers and merchants, as well as InfoHaus sellers, will find some useful tips here.

TIPS FOR EVERYONE

- When you create your VirtualPIN, you can use punctuation, spaces, and other symbols, but only characters and numbers are recognized — so you can save yourself some complexity by avoiding too many complicated characters.

- VirtualPINs are not meant to be shared publicly, but they do not have to be treated as securely as passwords or other sensitive information. Therefore, choose as your VirtualPIN a sequence of characters that is easy for you to remember, like a phrase. Unlike passwords, VirtualPINs can consist of recognizable names, words, or dates.

- You pay $2 to set up your First Virtual account, and pay nothing more as long as the underlying payment vehicle (usually credit card) is valid. If your credit card expires, or if you want to change the credit card to be used with First Virtual, you will have to pay another $2 fee. Thus, if you want to avoid extra fees over time, use a credit card with a distant expiration date; if you only want your First Virtual account to be valid a short time, use the credit card that expires soonest.

- If your primary e-mail address changes, you must notify First Virtual *before* you stop receiving mail there. This is to allow them to verify your new e-mail address by sending

you a confirmation of the change at your old address. If you aren't able to receive e-mail at your old address, you'll have to apply for a new VirtualPIN (and pay the $2 fee again).

- Customers can send e-mail to InfoHaus merchants, through the InfoHaus, by addressing their message to:

```
<Seller's DBA>@sellers.infohaus.com
```

replacing, of course, the seller's doing-business-as name. The message will be forwarded through the InfoHaus to the address the merchant gave when setting up the shop. This is useful for directing inquiries to merchants who haven't included their e-mail address in their InfoHaus shop information.

- Sellers (and buyers) can send e-mail to any owner of a VirtualPIN, as long as they know that VirtualPIN. This is done by using the VirtualPIN to create an e-mail address using the format:

```
VirtualPIN@relay.card.com
```

All spaces and punctuation must be removed from the VirtualPIN. First Virtual will revoke this privilege from users who abuse it by sending unsolicited e-mail.

TIPS FOR INFOHAUS MERCHANTS

- The InfoHaus HelpMeister is an excellent source of good ideas and helpful hints for InfoHaus merchants. Access it at the InfoHaus through the "by-seller" list of merchants, or directly by accessing this URL:

```
http://www.infohaus.com/access/by-seller/InfoHaus_HelpMeister
```

Although the HelpMeister is accessed through the InfoHaus, it is free — just link there for a list of helpful hints on using the InfoHaus.

- InfoHaus sellers can contact their paying customers by e-mail, even if the customers have not explicitly given the merchant their e-mail address. This is done by addressing the message to the customer using the Transfer-ID from the transfer-request. First Virtual will forward the message to the customer. You can find the Transfer-ID in the list of attributes in a transfer-result message from First Virtual. It consists of a random message number and looks something like this:

```
Transfer-ID: <12345678901@buyers.infohaus.com>
```

There is currently no charge for this service, but First Virtual may at some point impose a charge for each message forwarded.

IMPORTANT NOTE: This feature is not to be used to send "junk mail." It is intended to be used only in cases where the merchant needs to contact the buyer after a sale. For example, a merchant can use it to notify the customer that a bug fix for a program is necessary; another valid use is for contacting a customer who has not provided enough delivery information when purchasing hard goods. First Virtual does not explicitly define junk mail, but merchants who send junk mail can lose the privilege of sending e-mail and can even have their shops removed from the InfoHaus.

- You can make sure that your data files (both the paid and free parts of your products) are handled correctly by your customers' systems and receive the correct file-name

extensions by specifying a content-type for each file — the InfoHaus will automatically produce the correct file extension. You can specify content-type when checking files in through the InfoHaus telnet server. Indicate "other" both times when prompted for file type (see Figures 8-11 and 8-12), and enter one of the choices indicated in Table 10-1 at the next prompt.

Doing so will result in the file being given the appropriate extension.

TABLE 10-1 *Content-type options describing different types of file contents.*

Content-type	File Extension
image/gif	.gif
image/jpeg	.jpg
image/g3fax	.fax
image/tiff	.tif
audio/basic	.au
audio/x-aiff	.aif
audio/x-wav	.wav
audio/x-pn-realaudio	.ra
audio/midi	.mid
video/mpeg	.mpg
video/quicktime	.mov
application/postscript	.ps
application/zip	.zip
application/rtf	.rtf
application/pdf	.pdf
application/mac-binhex40	.hqx
application/x-msdos-exe	.exe
text/plain	.txt
text/html	.html

- Assign "QuickBuy" numbers to your products to make it even easier for your customers to purchase them by e-mail. See the section later in this chapter for full details on assigning QuickBuy numbers to your products.

- You can jump-start your subscription service by using trial subscriptions. Instead of billing subscribers immediately, you can give them an opportunity to try out your publication for a while before they are prompted to decide whether or not to pay for the subscription.

  Two optional attributes can be added to an e-mail transfer-request. The first is "FIRST-ISSUE," which refers to a first issue of your publication. If you use this attribute, your customer is treated as if he or she has already subscribed to your publication and will receive all issues from the one indicated in FIRST-ISSUE up to the current one, by e-mail — immediately followed by a renewal-request. This may be a bit intrusive, because it potentially floods the customer with back issues and then asks for money.

  An alternative is to use the attribute "REMAINING-ISSUES," which indicates a number of issues of your periodical to send before sending a billing request. For instance, you could offer customers one, or three, or six issues of your periodical before sending a billing request.

  If one of these attributes is used, the other cannot be; both are optional, and if neither is used the subscription will generate a renewal request at the end of the normal subscription cycle. A sample transfer-request is shown in Figure 10-1. Requests are sent to the address:

  ```
  mimeserver@infohaus.com
  ```

  and require the attributes shown in the figure.

```
Content-type: application/fv-infohaus;
                transaction=trial-subscription-request
Account-id: wolf-three little Pigsfeet
Doing-Business-As: Joyce's Worm Shop
Info-Name: The Wiggly Worm Weekly
Buyer: dang-eensy beensy spider
Email-address: eensy@beensy.com
Remaining-Issues: 4
```

FIGURE 10-1 *A trial-subscription request that will send four issues to the subscriber before sending a renewal request. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

GETTING YOUR STORE LISTED

- If you are accepting First Virtual for payment at your own Web site, you can request a link to your site from the First Virtual list of "Other places to shop." The best way to do this is to send an e-mail message to this address:

  `humanhelp@fv.com`

  Include in your message a description of your site and a link to it, in HTML, and indicate that you would like to have your shop listed.

- InfoHaus storefronts are accessible through the "By Keyword" or "By Topic" lists on the InfoHaus Web pages only if you specify keywords or topics for your products — you cannot specify a keyword or topic for your store. So, if you want customers to see your store in the list with the keyword "business," you will have to have at least one product with that as a keyword or topic.

  The only difference between keywords and topics is that there is a limited list of valid topics, while you can create your own keywords. First Virtual urges merchants to use existing topics and keywords, however, because it becomes

counterproductive to have too many keywords. You can see which keywords and topics are already in use by checking the bottom of the "By Topic" and "By Keyword" pages of the InfoHaus.

Topics and keywords can be assigned to your products either during the initial check-in (through the use of an "addition-request" e-mail message) or as a modification to an existing product (through the use of a "product-modification-request" message). For more details about checking in products to the InfoHaus, see Chapter 8. To include a topic with a product, add a line that looks like this to the message:

```
Topic: topic1 topic2
```

To include a keyword, add aline like this to the message:

```
Keyword: keyword1 keyword2
```

You can add more than one topic or keyword, but be sure to separate them with a space. As of early 1996, keyword and topic lists were recreated only about once every six hours, so if you don't see your store listed correctly, wait that long and check again before contacting First Virtual.

COMMERCIAL OPTIONS FOR MERCHANTS

If you are interested in setting up your own Web server to accept First Virtual payments, but don't want to have to deal with enabling it yourself, there are options. For example, HREF Tools Corporation offers a product called Cold Fusion for interactive Web development on Windows NT and Windows 95 without CGI programming. It allows you to create custom applications, including First Virtual applications, using Delphi (an object-oriented development system for client/server applications from Borland International, Inc.).

You can reach HREF Tools Corporation at:

HREF Tools Corp.
c/o Shine & Company
9 East 40th Street
New York, NY 10016
Phone: 800-365-9533 or 707-542-0844
Fax: 707-527-5373
HTTP://www.href.com/

Another company offering an easier path to a First Virtual-enabled Web server is StarNine Technologies, Inc. They offer a Macintosh Web server program called WebSTAR, with an optional Security Toolkit that includes support for First Virtual transactions. A 30-day trial version of the WebSTAR server is available from the StarNine Web site. You can reach StarNine at:

StarNine Technologies, Inc.
2550 Ninth Street, Suite 112
Berkeley, CA 94710
(510) 649 - 4949 (voice)
(800) 525 - 2580 (sales)
(510) 548 - 0393 (fax)
info@starnine.com
HTTP://www.starnine.com/

MAKING TEST SALES THROUGH FIRST VIRTUAL

It would be foolhardy to expect *anything* to work the first time out, and Internet commerce systems are no exception. One way to test your First Virtual implementation is to set up a separate buyer's account, create an inexpensive product, and use your buyer's account to purchase it.

First Virtual also provides a test payment server that works the same way their main transaction server does, except that no funds will be transferred as a result of any activity using it. The test server generates the same messages to buyer and seller as would be generated by actual transactions (such as transfer-requests and transfer-queries), so that you can verify that your systems are working as desired.

The test server is called "test.card.com" (the real First Virtual transaction server is called "card.com"), and it will work only with special test accounts. You'll need to set up at least two test accounts — one for buying, one for selling. To create a test account, you can fill out a form at this page on the First Virtual Web site:

```
http://www.fv.com/newacct/testsetup.html
```

You can also set up a test account by e-mail, using the same format as for initiating a real account, but instead of sending it to the address "newacct@card.com," you address it to

```
newacct@test.card.com
```

To run your tests, you will need to replace the First Virtual production server address, "card.com," with the test server address

```
test.card.com
```

Remember that this system will only recognize test accounts, and regular First Virtual accounts cannot be used.

InfoHaus "QuickBuy" Numbers

There is a "standard" method for buying InfoHaus products by e-mail: send a message to the address

```
buy@infohaus.com
```

with the buyer's VirtualPIN, seller's doing-business-as name, and Info-Name for the product being purchased. The body of a sample purchase e-mail message would include the following:

```
Buyer: like-Roly poly cupcakes
Seller: Wiggly Worm Weekly

Info-Name: Annual.sub
```

This can be a convenience to the merchant, as well as to the customer, but can also pose a challenge to all in getting the attributes exactly correct. If the customer makes a mistake in typing the seller's doing-business-as name or the product name, the transaction will not be completed. Using the QuickBuy option when setting up the information product, the merchant can assign a shorter, coded information product number to each product, to make it easier for customers to order.

Merchants add their own product numbers to their seller numbers (the seller number is assigned when the merchant first becomes a First Virtual seller), to create a set of unique identifiers for each information product. This is the QuickBuy number; when a customer wishes to order, he or she simply sends an e-mail message to the address:

```
quickbuy@infohaus.com
```

with the QuickBuy number and the customer's VirtualPIN in the body.

To add QuickBuy numbers to your products, you would add an attribute to the addition-request part of the e-mail message you send to set up the product. For example, the relevant part of the message might look something like this:

```
content-type: application/fv-infohaus;
transaction=addition-request

DOING-BUSINESS-AS: Wiggly Worm Weekly
ACCOUNT-ID: some-Itsy-bitsy spider
INFO-NAME: Annual Subscription
PRICE: 150.00
QUICKBUY-NUMBER: 666-1234
```

Customers can send e-mail messages with nothing more than their VirtualPINs and this QuickBuy number to purchase that product. This means merchants can promote their products more easily, and can even prepare special directories of products to send by e-mail upon request by new prospects.

LEARNING MORE ABOUT HTML AND CGI

One of the greatest benefits of selling through First Virtual is that you don't need to know C or Java or CGI programming, or how to write HTML documents. You don't even need your own Internet server. Even so, at some point most merchants will consider spicing up their InfoHaus storefront, or even setting up their own Web server. When that time comes, you will probably need some help learning how to use HTML and CGI to make your Internet store work.

Getting Help from the World Wide Web

If you are looking for up-to-date information about CGI, HTML, or any other Web/Internet publishing or programming tool, the Internet is a good place to go. Table 10-2 shows some good places to start looking; you can also do your own searches using your favorite Web search engine.

TABLE 10-2 *Some starting points for learning more about HTML and CGI.*

Site description	URL
NCSA offers a beginner's guide to HTML	`http://www.ncsa.uiuc.edu/General/Internet/WWW/HTMLPrimer.html`
NCSA offers a list of guides to writing HTML	`http://union.ncsa.uiuc.edu/HyperNews/get/www/html/guides.html`
An online index to HTML tags	`http://www.willcam.com/cmat/html/crossref.html`
A guide to using HTML and CGI scripts	`http://snowwhite.it.brighton.ac.uk/~mas/mas/courses/html/html.html`

Books about HTML and CGI

Publishers have been doing a great job of getting out handbooks for all types of Internet publishing tools. There are many to choose from, but here are three good ones to start with.

HTML TemplateMASTER CD
Erica Sadun/Christopher Watkins
CHARLES RIVER MEDIA, INC., 1995
$39.95

Foundations of World Wide Web Programming with HTML & CGI
Ed Tittel, Mark Gaither, Sebastian Hassinger, & Mike Erwin
IDG BOOKS WORLDWIDE, INC., 1995
$39.99

HTML Sourcebook
Ian S. Graham
JOHN WILEY & SONS, INC., 1995
$29.95

APPENDIX A

INTERNET COMMERCE GLOSSARY

Summary The Internet has spawned its own vocabulary, much of it acronyms. This glossary provides definitions of some of the more basic Internet and Internet commerce terms necessary to understanding commerce applications. The interested reader is directed to my book TCP/IP for Everyone (AP PROFESSIONAL, 1995), for more detailed information about the terms presented here, and for more information about other terms not included.

ACQUIRER

Entity that processes a credit card transaction for a merchant.

AGENT

A system acting on some other system or individual's behalf. Agents can be used to do comparison shopping, for example.

ANONYMOUS FTP

An implementation of the file transfer protocol software that allows users to access files without having accounts on the *ftp* server.

API

Application Programming Interface; a set of standard routines used to make standard functions available to custom-designed programs.

APPLICATION

A program providing some network function to end users or systems.

APPLICATION LAYER

The top layer in the standard Internet Protocol network architecture conceptual model. This is the level at which interaction takes place between the end user and the application.

ASCII

American Standard Code for Information Interchange; refers to the "standard" alphanumeric character set.

ASYMMETRIC CRYPTOGRAPHY

See **PUBLIC KEY CRYPTOGRAPHY.**

AUP

Acceptable use policy. Often refers to a policy of permitting only non-commercial uses for traffic carried by an Internet service provider subsidized by the U.S. government.

BACKBONE

A special type of internetwork intended specifically to connect other internetworks to the Internet, or used to connect internetworks across wide geographic areas.

BANDWIDTH

The amount of data that can be carried by a communications link in a given time. Usually measured in bits per second. A typical telephone link is capable of about 28.8 Kbps (thousands of bits per second).

BIT

The smallest unit of binary information, represented as either "1" or "0."

BRIDGE

A special-purpose computer that connects two networks of the same type. It reproduces transmissions from one and sends them to the other connected network.

BROWSER

Usually refers to a World Wide Web client program. Browsers are capable of requesting data from Web servers, and processing data received in response to these requests.

BYTE

A basic unit of data, consisting of 8 bits.

CARD-NOT-PRESENT TRANSACTION

A credit card transaction where the merchant receives the credit card number but cannot physically link the card to the purchaser. This includes telephone and mail orders, as well as online transactions.

CGI

Common Gateway Interface. A specification for creating programs that accept information acquired through World Wide Web pages and pass it on to other programs, or that take information from other programs and make it accessible through World Wide Web pages.

CIX

Commercial Internet Exchange. An industry organization for Internet service providers.

CLEARTEXT

Text that has not been encrypted.

CLIENT

A computer or system that makes requests for some kind of network service from another computer or system acting as a server.

CRACKER

An individual who uses computers for criminal pursuits. This term is not yet in general use, but is current among computer professionals and academicians. *See also* **HACKER**.

CRYPTANALYSIS

The study of cryptographic processes with the intention of finding weaknesses sufficient to defeat those processes.

CRYPTOGRAPHY

The study of mathematical processes useful for keeping data secret by encryption, guaranteeing its provenance, or guaranteeing that its content has been unchanged.

DAEMON

A program or process running on a server that listens to the network for requests for its service.

DATA LINK LAYER

The bottom layer in the standard Internet Protocol network architecture conceptual model. This is the level at which computers connected to the same physical wire (LAN) communicate with each other.

DATAGRAM

The basic unit of network transmissions under TCP/IP. A basic unit of network transmission in connectionless services.

DECRYPTION

The process of reversing encryption; application of a mathematical process to encrypted data to restore it to its cleartext version.

DES

Data Encryption Standard. A private key encryption standard approved by the United States government for the encryption of data when implemented in hardware. Uses 56-bit encryption and is generally accepted as sufficiently secure when correctly implemented.

DHCP

Dynamic Host Configuration Protocol. A protocol used to automatically configure Internet nodes when they initiate their network connection.

DIGITAL SIGNATURE

The result of the application of a cryptographic process to the digital document being signed. The signer uses his or her private key (of a public/private key pair) to come up with the signature, which is a sequence of characters. The document can be verified as coming from the signer by using the signer's public key to verify the document.

DNS

Domain Name System. A distributed database system implemented across the Internet for the purpose of linking Internet host names (used by people) with Internet Protocol addresses (used by computers).

E-MAIL

Electronic mail.

EBCDIC

Extended Binary Coded Decimal Interchange Code. This is the data representation standard used by IBM mainframe computers. Most other systems use ASCII representations.

EDI

Electronic Data Interchange. Refers to the exchange of business information, including purchase orders and invoices, between computers used by cooperating companies.

EFT

Electronic funds transfer.

ENCAPSULATION

The use of headers to "surround" network data for the purpose of handling its proper routing across a network or internetwork. The result is a network transmission unit directed to some destination host, with some unspecified content which will not be accessed until it arrives at its destination.

ENCRYPTION

A reversible process of modifying cleartext for the purpose of keeping it secret from anyone other than its intended recipient.

ETHERNET

A baseband networking medium, initially developed in the 1970s by Robert Metcalfe.

FAQ

A list of frequently asked questions (with answers) pertaining to a mailing list, Usenet newsgroup, product, or activity.

FDDI

Fiber Distributed Data Interface. A network standard for fiber optic media.

FILE SERVER

A computer connected to a network and capable of offering other users on that network access to its file system.

FINGER

A TCP/IP application used for retrieving a list of currently logged-in users on a specific system, or for getting information about some specific user of that system.

FIREWALL GATEWAY

A special construct used by an organizational internetwork to prevent attacks originating from the global Internet. The firewall may include one or more gateways or routers, and may include separate network segments, as well as software filtering and other mechanisms for protecting corporate network resources.

FTP

File Transfer Protocol. The set of specifications, or the program itself, for transferring files between two computers on the Internet.

GATEWAY

A special-purpose computer for internetwork connectivity. Often refers to a **ROUTER** (see entry). Often refers to a system mediating between protocols, as with e-mail gateways which accept e-mail from the Internet and translate it to the appropriate e-mail protocol on the internal LAN.

GIGABIT

1 billion bits.

GIGABYTE

1 billion bytes.

GOPHER

A character-based Internet information publishing application, developed at the University of Minnesota.

GREEN COMMERCE MODEL

Model for Internet commerce devised by founders of First Virtual. This model originally defined a method for selling information-only products, putting all risk of nonpayment on the vendor (whose loss was only theoretical, because the incremental cost of a digital product is close to zero).

HACKER

A term applied to individuals interested in computers and computing. This term is often used popularly to refer to individuals involved in criminal pursuits such as breaking into computers without proper authorization. Many purists prefer its original meaning, referring to individuals who have deep interest as well as understanding of computers. *See also* **CRACKER**.

HANDSHAKE

The process of negotiating a connection between two hosts. The initiating host waits for acknowledgment from the destination host, which in turn waits for acknowledgment of its own response.

HOME PAGE

The opening document of a World Wide Web site. It may also refer to the Web document that an individual user's Web browser points to on startup.

HOST

Any device connected to a network that can send or receive requests for network services.

HTML

Hypertext Markup Language. An Internet standard for creating World Wide Web documents, based on the Standard Generalized Markup Language (SGML). Markup languages create plain text files using tags to set off functional sections of the document, which are interpreted appropriately for display by the document viewing software.

HTTP

Hypertext Transfer Protocol. An Internet standard defining the interaction between World Wide Web clients and servers.

IAB

Internet Architecture Board. Part of the Internet Society, the IAB oversees the IESG and the IETF.

IANA

Internet Assigned Number Authority. A group organized through the Internet Society for maintaining assigned numbers relating to the Internet Protocol suite.

ICMP

Internet Control Message Protocol. A protocol used to exchange reachability and routing information between hosts and routers on the same LAN.

IESG

Internet Engineering Steering Group. A steering committee overseeing the activities of the Internet Engineering Task Force (IETF).

INFOHAUS

A World Wide Web storefront hosting service provided by First Virtual for sellers. In exchange for a commission on all sales, First Virtual provides server facilities for merchants selling information products.

INTERNET

See **INTERNETWORK.**

INTERNET

The network of networks connecting tens of millions of users around the world.

INTERNETWORK

Literally, a network of networks. Any network consisting of two or more discrete networks connected by routers and capable of supporting seamless interoperability between hosts connected to any part of the internetwork.

INTERNIC

The Internet Network Information Center. InterNIC administers and assigns Internet domains and network addresses.

INTEROPERABILITY

The ability of disparate computer systems to send and receive requests for network services across disparate networks, seamlessly and transparently to the end user.

IP

Internet Protocol. A protocol defining the interaction between hosts communicating across an internetwork.

IP ADDRESS

A numerical address assigned to a computer connected to an internetwork that uniquely identifies it on that internetwork.

IPNG

Internet Protocol, Next Generation. Another name for **IPv6**.

IPV6

Internet Protocol, version 6. The next revision of the Internet Protocol, to be implemented in the second half of the 1990s. In addition to various new features, IPv6 increases the size of Internet addresses from 32 bits to 128 bits, thus increasing the number of available network and host IP addresses. This is necessary to accommodate continued exponential growth in Internet connectivity.

IPX

Internetwork Packet eXchange. An internetwork protocol used by Novell NetWare and other LAN operating systems.

ISDN

Integrated Services Digital Network. A type of telephone service providing high speed (from 128 Kbps and up) and digital services (multiple phone lines on a single link, conferencing, and many others).

ISOC

The Internet Society. A professional organization supporting Internet standards processes as well as other activities.

KERBEROS

A method for securely authenticating users to networked hosts, developed at MIT. Kerberos uses special servers to maintain user passwords and mediate the exchange of session keys between users and hosts.

KEY

A quantity of data used in cryptographic procedures to encrypt, decrypt, or authenticate other data.

LAN

Local area network. A network connected computers in the same general area, on a single network cable (or a set of cables that emulate a single wire).

LATENCY

The delay between the transmission of a piece of data and its reception at its destination. Latency is one measure of network connection performance; **BANDWIDTH** is another. High-latency links will be very responsive and work well with interactive applications such as terminal emulation even if the transmission rate is low.

MAC

Message Authentication Code. A quantity of data based on the contents of a message, used to confirm that it has been received as transmitted.

MBONE

Multicast Backbone. A special network backbone used to transmit multicasts (including coverage of standards meetings and other content, in real time) over the Internet.

MIME

Multipurpose Internet Mail Extensions. A specification for the linking and transfer of nontext files with Internet e-mail and other IP applications (including Usenet news).

MULTICAST

Transmission of network traffic to some, but not all, hosts connected to the network or internetwork.

MULTIHOMED HOST

A system connected to an internetwork on two or more different individual networks. Routers and gateways are, by definition, multihomed hosts, since they link two or more separate networks.

NETWARE

A commercial network operating system available from Novell Inc. offering network resource services across the IPX network protocol.

NETWORK

Any system of interconnected systems. In particular, the system defined by computers connected to the same communications medium in such a way that each can communicate with the other connected computers.

NFS

Network File System. A TCP/IP network protocol developed by Sun MicroSystems, Inc., for sharing resources between connected workstations. Originally implemented mostly on UNIX systems, NFS implementations are now available for most platforms.

NIC

Network information center. An organizational resource devoted to providing information about a network.

NNTP

Network News Transfer Protocol. A TCP/IP protocol defining the exchange of Usenet news between servers and clients.

NOC

Network operations center. An organizational resource devoted to supporting the day-to-day operations of a network.

NODE

A device connected to a network; more specifically refers to the network interface itself, so a multihomed host may represent multiple nodes.

NONREPUDIATION

The ability of the recipient to prove who sent a message based on the contents of the message. The quality can derive from the use of a digital signature on the message, which links the sender to the message.

NOS

Network operating system. A software product that allows hosts on a LAN to share network resources including disk storage, programs, and peripherals connected to the LAN.

NSF

National Science Foundation. One of the most important organizations involved in development and research in TCP/IP internetworking, NSF funded NSFNET, which ultimately evolved into the Internet backbone.

OCTET

A term used to refer to an 8-bit byte of data, usually in the context of internetworking.

OUT OF BAND

Using a different medium of exchange than the primary medium of data exchange. Most commonly refers to the practice of exchanging keys or other sensitive information to be used for network communication by telephone, hard copy, or in person.

PACKET

A unit of network transmission. Specifically may refer to the unit of data transmitted across a packet switched network (such as the Internet).

PCT

Private Communication Technology. A protocol specification released by Microsoft in late September 1995, describing mechanisms for secure communication between individuals on the Internet, providing encryption and authentication.

PEM

Privacy Enhanced Mail. An Internet standard defining a protocol for the secure, authenticable, and nonrepudiable transmission of electronic mail.

PGP

Pretty Good Privacy. A freely distributed program implementing public key cryptography for e-mail. Also sometimes used for electronic commerce purposes.

PING

Packet Internet Groper. A simple TCP/IP network application in which the originating hosts sends a signal to a destination host to determine whether or not the destination host is reachable through the network.

PPP

Point-to-Point Protocol. A protocol defining the connection of a single host to another host over a bidirectional link (such as a telephone line), and connecting to network resources through that connection.

PRIVATE KEY

A key that is kept secret, specifically referring to the secret key of a public key pair, because it must be kept private by the owner.

PROTOCOL

A set of rules defining the behaviors of interacting systems, particularly when applied to rules for exchanging of information between networked systems.

PUBLIC KEY

Of the two keys used for public key cryptography, the one that can be made public, so that senders can encrypt messages.

PUBLIC KEY CRYPTOGRAPHY

The cryptographic system in which encryption is done with one key and decryption is done with another.

RFC

Request for Comments. The generic term for Internet standards documents. Originally, researchers and academicians working on specific

internetworking projects published their work as RFCs to solicit further comments from others working in the field, as well as to identify errors and problems.

ROUTER

A multihomed host (connected to at least two networks) that is able to forward network traffic from one connected network to another.

S-HTTP

Secure Hypertext Transfer Protocol. A protocol that defines security additions to the HTTP protocol, developed within the traditional Internet standards process. S-HTTP operates strictly at the application level, adding encryption and authentication to World Wide Web client/server communications.

SECRET KEY CRYPTOGRAPHY

The cryptographic system in which both encryption and decryption are done with the same key by both parties to the communication.

SECRET KEY

A key that must be kept secret, specifically referring to a shared secret key used for symmetric encryption by parties to both encrypt and decrypt messages.

SET

Secure Electronic Transaction standard. A standard for Internet transactions developed through the collaboration of Visa International, MasterCard International, IBM, Microsoft, CyberCash, Netscape, and other interested companies. This is likely to replace other specifications like **PCT** and **STT**.

SERVER

Any computer connected to a network that offers services to other connected systems on the network.

SGCP

Simple Green Commerce Protocol. This protocol requires SMXP to exchange the appropriate MIME entities to perform transactions as defined by the Green Commerce model.

SLIP

Serial Line Internet Protocol. A method of connecting a single computer to the Internet through a telephone link, SLIP is generally considered less desirable than PPP for this purpose.

SMXP

Simple MIME Exchange Protocol. This protocol defines the use of MIME entities for interactions that do not use e-mail; for example, to communicate transaction information using the Simple Green Commerce Protocol (SGCP).

SMTP

Simple Mail Transfer Protocol. The set of rules defining the transmission of electronic mail between users.

SNMP

Simple Network Management Protocol. This protocol defines functions used to monitor and manage network resources across internetworks.

SSL

Secure Sockets Layer. A protocol first developed by Netscape and subsequently provided to the rest of the Internet community to add encryption and authentication at the network layer just below the application level.

STT

Secure Transaction Technology. A protocol specification released by Microsoft and Visa International late in September 1995, intended to define the interchange of credit card payment information across public and private networks.

SYMMETRIC CRYPTOGRAPHY

See **SECRET KEY CRYPTOGRAPHY.**

TCL

"Tool command language," pronounced "tickle." Tcl is a simple, text-based, programmable language for issuing commands to interactive programs (for example, UNIX system shells).

TCP

Transmission Control Protocol. The protocol defining the way applications communicate with each other across the Internet. TCP is a reliable protocol, meaning that all transmissions between applications must be acknowledged by the recipient.

TCP/IP

Transmission Control Protocol/Internet Protocol. The description of any network using the Internet protocols, named from the two dominant protocols used on the Internet.

UDP

User Datagram Protocol. A protocol defining a connectionless, unreliable transport layer service between applications on the Internet.

URL

Uniform Resource Locator. A protocol for defining the exact location of a World Wide Web resource, identifying the method of access, the host on which it resides, and the path and filename of the resource.

VIRTUALPIN

A personal identification name (PIN) associated with a First Virtual account. The PIN can be up to 24 characters long, and includes a prefix assigned by First Virtual when the account is initiated.

WWW

World Wide Web.

APPENDIX B

ELECTRONIC COMMERCE ONLINE RESOURCES

The best resource for information about any aspect of the Internet is the Internet itself. Sometimes the Internet is too good a resource — there is such a wealth of material online with very little quality control. Thousands of organizations and individuals present themselves as "Internet experts," complete with Web pages full of their "articles" and extracts of talks, courses, and seminars. More useful, in general, are the Web sites maintained by mainstream vendors, financial institutions participating in the digital marketplace, and organizations devoted to supporting the Internet and electronic commerce, such as the Internet Society and CommerceNet.

The companion CD-ROM to this book includes URLs pointing to scores of different World Wide Web sites relating to electronic commerce. The reader is directed to these sites for the latest information about everything discussed in this book, as well as information that appeared too late to be included. The links in the CD-ROM are described here (as they are on the CD-ROM itself).

Other Internet resources include e-mail distribution lists and Usenet news groups. Some relevant ones are listed in the last section of this appendix.

While every effort is made to ensure accuracy and completeness, the state of the Internet is such that rapid change is inevitable. Neither this nor any other printed guide can hope to be up-to-date for very long. As a result, while most of these links should be accurate and useable, the reader may prefer to search for more up-to-date links directly on the Internet if one of the cited links does not connect to the expected resource.

WORLD WIDE WEB RESOURCES

There are hundreds of thousands of information sources of all types available online, many of them accessible through the World Wide Web. This section offers links and descriptions of some of those relating to electronic commerce, divided by categories.

Electronic Commerce Companies

These companies make information available online about their products and services, all of which are directly related to electronic commerce. Many of these companies work together in strategic partnerships, licensing arrangements, consortia, and other arrangements. Some of the listed organizations are in the process of acquiring others, while some may have been spun off from other companies. The point is that these URLs should be considered starting points for searches, rather than authoritative addresses.

BROADVISION, INC.

http://www.broadvision.com

Developing software to support foundations for electronic buying and selling.

CARDSERVICE INTERNATIONAL

http://www.cardsvc.com

Offers credit card services to Internet merchants.

CHECKFREE CORPORATION

http://www.checkfree.com/

Provides electronic payment services.

CLICKSHOP COM

http://clickshop.com/770/

Offers electronic shopping cart software called Shopping 770 to be added to electronic shop Web pages.

CYBERCASH, INC.

http://www.cybercash.com/

Provides payment services for the Internet.

CYLINK CORPORATION

http://www.cylink.com

A licenser of public key cryptography algorithms.

DIGICASH BV

http://www.digicash.com/

Developers of digital currency systems.

ENTERPRISE INTEGRATION TECHNOLOGIES

http://www.eit.com

Sells software and services in support of WWW commerce; was involved in the creation of CommerceNet, as well as the Secure HTTP specification.

FIRST VIRTUAL HOLDINGS INCORPORATED

http://www.fv.com/

An information-only Internet payment system.

INTERNET SHOPPING NETWORK

http://www.internet.net

Internet shopping services, offering computer-related products as well as online catalogs, floral arrangements, gifts, and more.

LION'S DEN LLC

http://www.globalone.net/lionsden/stydec

Offers an electronic shopping cart called Stydec to be added to electronic shop Web pages.

MARK TWAIN BANK

http://www.marktwain.com

First United States bank to offer DigiCash ecash.

MEGAWEB, INC.

http://www.megamart.com/forms/dwosfeatures.html

They offer the Dynamic Web Ordering System for setting up online storefronts.

MICROSOFT CORPORATION

http://www.microsoft.com

The software giant has big plans to get involved in electronic commerce. Released a specification for online transactions jointly with Visa International in September 1995, and cooperated on the SET industry standard released later.

MONDEX INTERNATIONAL

http://www.mondex.com/mondex/home.htm

U.K. provider of digital currency using smartcards.

NETCHEX

http://www.PrimeNet.Com/~rhm/

Online checking, including free client software.

NETMARKET

http://www.netmarket.com

Produces secure Web server package using PGP.

NETSCAPE COMMUNICATIONS INC.

http://home.netscape.com/

The latest information from the Web browser/server publisher.

PREMENOS

http://www.premenos.com

Pioneering EDI company, offering software for IBM multiuser systems.

RSA DATA SECURITY, INC.

http://www.rsa.com

A licenser of public key cryptography algorithms.

SUN MICROSYSTEMS

http://www.sun.com

Internet pioneer Sun offers network security solutions, among many other Internet products.

SURETY TECHNOLOGIES

http://www.surety.com

Offers "digital notary" services.

TERISA SYSTEMS

http://www.terisa.com

A joint venture of Enterprise Integration Technologies and RSADSI, Terisa was launched to market, license, and support technologies for secure Internet transactions.

THE INTERNET GROUP

http://www.tig.com

Provider of electronic commerce consulting and services.

THE NETCHECK COMMERCE BUREAU

http://www.mja.net/netcheck/

Providing reference services to companies doing business on the Internet.

VERIFONE

http://www.verifone.com

Leader in transaction automation industry; is acquiring EIT for its electronic commerce division.

VERISIGN, INC.

http://www.verisign.com

A spin-off from RSADSI, Verisign provides public key certificates to individuals and companies.

Financial Institutions

The number of banks offering some type of service over the Internet, from simple information services to actual banking services, is growing rapidly. These are just a few of the first to get online: there will certainly be more by the time you read this.

ASIAN DEVELOPMENT BANK

http://www.asiandevbank.org/

A development institution serving Asia and the Pacific.

BANK OF AMERICA

http://www.bofa.com/

Currently offering information services online.

BANK OF MONTREAL

http://www.bmo.com/

Canadian bank with WWW services.

BANKNET ELECTRONIC BANKING SERVICE

http://mkn.co.uk/bank

First bank to allow deposits online, in United Kingdom.

BARCLAYS BANK

http://www.barclays.co.uk/

Major U.K. bank offers information services online.

CITIBANK

http://www.tti.com/

Major bank offering global services; site provides information about services.

CYBERBANK

http://www.webshop.com/cbank/

A service for trading certificates of deposit online.

MARK TWAIN BANK

http://www.marktwain.com

First United States bank to offer DigiCash ecash.

MASTERCARD INTERNATIONAL

http://mastercard.com

International payment services organization, including credit and debit cards.

NATIONSBANK

http://www.nationsbank.com/

Major financial services and banking company.

NORWEST CORPORATION

http://www.norwest.com/

Major regional financial services institution serving U.S. Midwest.

VISA INTERNATIONAL

http://www.visa.com

International payment services organization, including credit and debit cards.

WELLS FARGO BANK

http://wellsfargo.com/index.html

Major bank, offering actual online services as well as information.

International Internet Commerce Sites

The Internet is truly a global phenomenon. Even though a great deal of activity and attention has centered on the United States, there is significant Internet commerce activity all over the world. In addition to the international banks mentioned elsewhere, as well as companies such as DigiCash and Mondex, international organizations are pivotal to influencing the future of Internet commerce. Here are just a few sites.

COMMERCE ALLEY

`http://www.calley.co.jp/`

About forty midsized Japanese businesses of all types working together on a "virtual shopping street."

EDI AWARE

`http://www.imaginet.co.uk/edi/ediaware.htm`

Newsletter about EDI from Wales.

EDI-TIE

`http://www.editie.nl/`

EDI products from the Netherlands.

ELECTRONIC MARKETS NEWSLETTER

`http://www-iwi.unisg.ch/iwi4/cc/em/emnewsl.html`

Newsletter covering electronic commerce, from Switzerland.

INTERNATIONAL COMMERCIAL CYBER CENTER

http://www.indra.com/jewels/cybercom/

A Web site in English and Spanish, from Spain, with multi-level marketing opportunities among other information.

INTERNET BUSINESS INFORMATION REGISTRY

http://quebec.ie.utoronto.ca/IBIR/ibir.html

A Canadian database of companies offering products for sale through the Internet.

KEWILL-XETAL SYSTEMS LIMITED

http://www.cityscape.co.uk/users/ew48/

United Kingdom provider of EDI systems and services.

NET COMMERCE INTERNATIONAL

http://www.lpac.ac.uk/Trel/NCI.html

A bimonthly newsletter on electronic commerce from the United Kingdom.

NIJENRODE BUSINESS WEBSERVER

http://www.nijenrode.nl/resources/bus/

Pointers to business resources on the Internet from the Netherlands.

ONLINE BEI INOVIS

http://www.inovis.de/

A German firm offering an online catalog and electronic commerce.

General Catalog and News Services

These general catalog services should be the first stop when tracking down new information sources. The interested reader will find some of them invaluable for tracking down the latest and most updated sites for electronic commerce, as well as other topics. Also included here are some sites that are neither comprehensive nor catalogs, but that are maintained (usually by individuals) to provide pointers specifically to topics related to online commerce.

ALL-INTERNET SHOPPING DIRECTORY

`http://www.webcom.com/~tbrown/`

A directory of sites offering items for sale over the Internet, including e-mail sales.

AT&T 800 NUMBER DIRECTORY

`http://www.tollfree.att.net/dir800/`

Access AT&T's directory for toll-free numbers.

COMMERCE

`http://gopher.econ.lsa.umich.edu/EconInternet/Commerce.html`

An interesting and fairly comprehensive collection of links to electronic commerce sites and other references.

COMMERCIAL SERVICES ON THE NET

`http://www.directory.net/`

A directory of sites with commercial orientation, maintained.

GALAXY

http://www.webcrawler.com/

An Internet catalog operated by TradeWave.

INFOSEEK

http://www.infoseek.com/

A for-pay Internet search service, covering more than just World Wide Web sites, including Usenet news searches as well as commercial/premium databases.

LYCOS

http://www.lycos.com/

One of the most comprehensive Internet catalog sites.

PATHFINDER (TIME/WARNER)

http://www.pathfinder.com/

Links and more, including a Catalog 1, for buying from your favorite mall stores and more — all online.

THE NANDO TIMES

http://www2.nando.net/nt/nando.cgi

An online, 24-hour Internet "newspaper."

WEBCRAWLER

http://www.webcrawler.com/

Another Internet catalog site, operated by America Online.

WWW Business Resources List

http://www.d.umn.edu/~rvaidyan/resource.html

A list of links to businesses, retailers, and other business resources on the World Wide Web. Maintained by a faculty member at the University of Minnesota, Duluth.

Yahoo

http://www.yahoo.com/

One of the most popular Internet catalog sites.

Yahoo/Electronic Commerce

http://www.yahoo.com/Business_and_Economy/Electronic_Commerce/

Links to hundreds of sites relating to electronic commerce, online sales, marketing, electronic currencies, and online transactions.

Online Commerce Organizations

Trade and industry groups are an important set of resources for any industry, but particularly for a new industry. Most prominent is CommerceNet (see the last section in this appendix), but there are other important groups.

CommerceNet

http://www.commerce.net

The trade association for online and Internet commerce.

DATA INTERCHANGE STANDARDS ASSOCIATION

http://www.disa.org

A standards body for Electronic Data Interchange (EDI).

ELECTRONIC COMMERCE ASSOCIATION

http://www.globalx.net/eca/

An organization based in Canada, dedicated to providing support to the electronic commerce industry and participants.

ELECTRONIC COMMERCE RESOURCE CENTER

http://www.ecrc.ctc.com/

A U.S. government–supported resource center for promoting use of electronic commerce technologies by industry.

FINANCIAL SERVICES TECHNOLOGY CONSORTIUM (FSTC)

http://www.llnl.gov/fstc/

A nonprofit consortium of financial services companies and academic and research organizations, working toward the goal of enhancing U.S. financial services industry competitiveness.

INTERNET SOCIETY

http://www.isoc.com

The professional organization for the global Internet. Supports wide range of standards and other activities relating to the Internet.

NAFTANET

http://www.nafta.net/

NAFTAnet, Inc., provides services relating to electronic commerce as it relates to international trade and NAFTA — the North American Free Trade Agreement.

THE EM-ELECTRONIC MARKETS NEWSLETTER

http://www-iwi.unisg.ch/iwi4/cc/em/emnews1.html

A quarterly technical journal published out of Switzerland covering the electronic commerce technologies.

WORLD WIDE WEB CONSORTIUM

http://www.w3.org/pub/WWW/Consortium/

Consortium dedicated to development of the World Wide Web.

Online Marketing, Buying, and Selling

There are literally hundreds of electronic malls on the Internet. This list is hardly comprehensive, but gives pointers to a few of the more interesting Web pages devoted to buying and selling, as well as some of the more typical digital malls.

For a more complete and current listing of digital malls, check one of the Internet directory services.

ANDERSEN CONSULTING (BARGAINFINDER)

http://bf.ac.cstar.com

The BargainFinder page is an example of an agent that can search online merchants for products and prices.

COMPUSERVE

http://www.compuserve.com

The online service's Internet site supports purchases with the CompuServe wallet (a relabeling of the CyberCash client software).

CYBERSOURCE CORP.

http://software.net

A product center for software vendors to market Windows 95 software products for online sales.

ELECTRONIC AUCTION

http://www.primenet.com/~auction/index.html

An electronic forum for buyers and sellers to buy and sell.

INDUSTRYNET ONLINE MARKETPLACE

http://www.industry.net/

A members-only service (but membership is free) providing information and links to products and information.

INTERNET SHOPPING NETWORK

http://www.internet.net

On-line shopping for electronics and other products.

NECX DIRECT

http://necxdirect.necx.com

An online computer products superstore.

NETCITY DEVELOPMENT CO.

`http://www.netcity.com`

Electronic mall.

YAHOO/SHOPPING CENTERS

`http://www.yahoo.com/Business_and_Economy/Companies/Shopping_Centers/`

Literally hundreds of pointers to Internet shopping centers.

MAILING LISTS

By limiting participation to subscribers, mailing lists can focus discussion within a group sharing interests. Subscribing is usually as simple as sending an e-mail message to the list server. Specific list rules and "administrivia" are almost always sent to new subscribers, describing how to unsubscribe from the list, how to submit messages to the list, and how to reach the list manager in an emergency.

These are a few lists dedicated to electronic commerce topics. While there is a wealth of information in these lists, it often flows too copiously for working people to keep up with. For example, the cypherpunks list may generate well over a hundred messages daily.

CYPHERPUNKS

Subscribers to this list discuss cryptography and its implementation in current software, as well as many other topics related to security and privacy issues. To subscribe, send e-mail to:

```
majordomo@toad.com
```

No subject is needed; put the following in the body:

```
subscribe cypherpunks your@email "Your Name"
```

You must substitute your own e-mail address where it says `your@email` and your own name where it says `Your Name`.

Before subscribing, remember that this is a very high-volume list. You may get well over 100 messages from the list daily, so if you can't handle that volume, you may prefer to subscribe to one of the cypherpunk digest services.

CYPHERPUNKS LITE

A moderated and edited version of the Cypherpunks list is available for $20 per year from COMSEC Partners. Only the more important, interesting, or relevant posts are forwarded to subscribers. You can look at previous selections by checking archived files at this site:

```
ftp://ftp.crl.com/users/co/comsec/cp-lite
```

Files at the site are compressed using gzip. To subscribe, send payment to COMSEC at:

COMSEC Partners
1275 Fourth Street, Suite 194
Santa Rosa, CA 95404 USA

Be sure to indicate your e-mail address, and whether you prefer the digest version (multiple postings are batched and sent together in a single message).

WWW-BUYINFO

The WWW-buyinfo list is for discussion of methods of using the World Wide Web to buy and sell products. To subscribe, send e-mail to:

```
www-buyinfo-request@allegra.att.com
```

The body of the message should include:

```
subscribe www-buyinfo
```

It is not necessary to include a subject for the message.

INTERNET MARKETING

The Internet Marketing list discussions are mostly about marketing activities using the Internet. To subscribe, send e-mail to:

```
im-sub@popco.com
```

It is not necessary to include a body or subject for this message. At this writing subscriptions are free but a voluntary contribution of $25 guarantees a lifetime subscription. Other subscription options may be introduced in the future.

EDI LIST

The EDI-L list is for discussions about Electronic Data Interchange issues of a general nature. To subscribe send mail to:

```
listserv@uccvma.ucop.edu
```

Include in the body:

```
subscribe edi-l Your Name
```

Substitute your own name where indicated; it is not necessary to include a subject for the message.

IETF-EDI

The IETF EDI working group works to produce specifications for the use of EDI standards over the Internet, with an initial focus on the transport of EDI via Internet e-mail.

To subscribe to this list, send email to:

```
listserv@byu.edu
```

Include in the body of the message:

```
sub ietf-edi Your Name
```

Substitute your own name where indicated; it is not necessary to include a subject for the message.

HTMARCOM

HTMARCOM stands for High Tech MARketing COMmunications. This list discusses that topic as it relates to Computer and Electronics products and services.

To subscribe to this list, send e-mail to:

```
listserv@rmii.com
```

Include this in the body of your email message:

```
SUBSCRIBE htmarcom you@domain.name
```

Substitute your own e-mail address where indicated; it is not necessary to include a subject for the message.

COMMERCENET

CommerceNet is a nonprofit organization created to help businesses and consumers use the Internet for buying and selling, with the specific purposes of improving efficiency of transactions, reducing costs of ordering and delivering goods and services, and speeding goods and services to market. Member organizations include networking service vendors, consultants, software publishers, hardware manufacturers, Internet service providers and consultants, and many other organizations with an interest in the development of electronic commerce over the Internet.

CommerceNet Charter

The CommerceNet charter includes the following goals:

- Operate of a World Wide Web server offering access to directories and other information useful to opening an electronic marketplace for business-to-business interaction.
- Increase the speed with which electronic commerce is implemented on the Internet through the use of pilot programs in areas including secure transactions, digital payment services, digital catalogs, EDI over the Internet, and others.
- Add electronic commerce features to existing Internet services and applications, and encourage development of new services.
- Encourage organizations of all sizes to participate in electronic commerce, and support programs to publicize CommerceNet facilities.
- Provide an information infrastructure for Northern California, and interface that resource with other national and international resources.

The entire enterprise is oriented toward the goal of making electronic commerce a superior alternative to paper-based commerce.

CommerceNet Participation

Large organizations can participate in CommerceNet as full corporate members; however, this option may cost $35,000 per year. Associate memberships are available for as little as $5,000 annually for smaller businesses (those with less than $10 million in annual revenue).

For those who do not need or wish to participate as members of the CommerceNet consortium, subscriptions are available for $400 annually, with a $250 initiation fee. Subscribers are entitled to inclusion in CommerceNet directories and Internet software and information packages, among other benefits. Subscribers may also purchase Internet host services from third-party Internet service providers at special rates.

What CommerceNet Offers

CommerceNet offers its members a forum for industry leaders to discuss issues, deploy pilot applications, and from these define standards and best business practices for using the Internet for electronic commerce. Through these efforts, CommerceNet will help this emerging industry evolve to common standards and practices so that users will see a seamless web of resources.

Participating companies get additional assistance from CommerceNet, including the following:

- Access to Internet connectivity through BBN.
- Directories to CommerceNet members and subscribers, as well as pointers to other electronic commerce organizations and activities are available online.
- Access to information provider and Internet presence software tools.
- Access to commerce security mechanisms supported within commerce applications (including authentication, encryption, digital signature, and public key certificates).
- Educational opportunities for small businesses to learn about publishing on the Internet.

APPENDIX C

FIRST VIRTUAL TERMS AND CONDITIONS DOCUMENTS

Legal documents detailing commercial agreements are often written in a foreign language (that of contract lawyers) and printed in small print barely legible to the naked eye. First Virtual's versions of these documents, their Terms and Conditions agreements, are different. These documents use an easy-to-understand question-and-answer format and hypothetical examples to explain your contractual obligations. This appendix includes the complete text of the most recent Terms and Conditions documents for First Virtual buyers, sellers, and users of the InfoHaus service (released December 16, 1995). Chapter 5 explains how to download the latest versions of these documents; this appendix contains the exact text of these documents, formatted for publication.

BUYER'S TERMS AND CONDITIONS

Buyer's Agreement with First Virtual Holdings Incorporated Effective December 16, 1995

The following questions and answers are called the First Virtual Buyer Terms and Conditions ("First Virtual Buyer TACs" or "Buyers TACs"). These First Virtual Buyer TACs are the only agreement between First Virtual Holdings Incorporated and you, the Buyer using the First Virtual Internet Payment System. When you become a First Virtual Buyer as provided in Q&A#3, we both agree to act according to these First Virtual Buyer TACs. We also agree that each numbered question and answer are to be read and applied together as the expression of one complete idea or "term" as it is called in the law. All the questions and answers are to be interpreted in a consistent manner as agreed in Q&A#14.2.

Q1. Who is First Virtual Holdings Incorporated?

ANSWER: First Virtual Holdings Incorporated, is a Wyoming corporation with its business office at 11975 El Camino Real, Suite 300, San Diego, CA 92130 and its Wyoming address is 1720 Carey Ave. or PO Box 1436, Cheyenne, Wyoming 82003-1436. Hereafter, we will call First Virtual Holdings Incorporated "First Virtual," or "FV." As used herein, the following are trademarks of First Virtual Holdings Incorporated: First Virtual Internet Payment System; VirtualPIN; InfoHaus.

Q1.1. How can I contact First Virtual?

ANSWER: It depends. If you want more information about First Virtual, send e-mail to "info@fv.com". This will give you general information on First Virtual and also tell you how to get FAQs (Frequently Asked Questions) on selected topics. For questions that are not answered by the First Virtual's FAQs, e-mail your question to "human-help@fv.com". Please remember that FAQs and e-mail from "human-help" are not a part of our agreement.

Q1.2. How do I know when these First Virtual Buyer TACs change?

ANSWER: First Virtual will e-mail you a message when a change is made to this agreement as it is published if you send e-mail to

"fineprint-changes-request@fv.com" and subscribe to the fineprint-changes mailing list in accordance with our instructions, after you sign up as a Buyer.

Q1.3. Are e-mail messages I send to First Virtual private?

ANSWER: No. It is possible that any message you send to First Virtual may be read by anyone or everyone at First Virtual. You must also assume that e-mail sent may be read by someone other than the intended recipient. Also, all messages sent to First Virtual are the property of First Virtual.

Q2. Who am I?

ANSWER: You are not a minor (younger than age 18) and you are applying to be a First Virtual Buyer. If you complete the application process according to Q&A#3, you are agreeing to the terms of this Agreement.

Q2.1. What does it mean to be"a First Virtual Buyer"?

ANSWER: It means that you completed the application process according to Q&A#3, First Virtual accepted your application, and you have used your VirtualPIN to buy something using the First Virtual Internet Payment System. It also means that you agree to follow the agreement as reflected in these Buyer TACs. It also means that, as a First Virtual Buyer, you can use the First Virtual Internet Payment System to buy information, goods and services. Hereafter, we will just call you the "Buyer" or "you," "me" or "I."

Q2.2. How does First Virtual contact me?

ANSWER: First Virtual contacts you through the e-mail address that you provide First Virtual during the application process. You agree that First Virtual sends all notices to this e-mail address. Just as an example, notices may include e-mail queries that are used in the First Virtual Internet Payment System (See Q&A#4 for further details), notice of a changed credit card, or any other notices required for any reason. First Virtual may get other addresses from you, such as postal addresses, but they are not used for purposes of providing any notice under this agreement.

Q2.3. What if my e-mail address changes or I no longer have an e-mail address?

ANSWER: If your e-mail address changes, you must inform First Virtual by e-mail from your old e-mail address. In other words, don't inform First Virtual from your new e-mail address that the old e-mail address is no longer valid. First Virtual does not consider this a valid e-mail address change. During the period you do not have an e-mail address, you cannot be a Buyer. The First Virtual Internet Payment System requires a current private (not shared with anyone else) e-mail address for the Buyer and Seller to buy and sell information. In the event you change e-mail addresses without properly notifying First Virtual you must reapply as a Buyer and pay any set up fees. First Virtual only delivers notices to your e-mail address as provided by you according to these Buyer TACs.

Q3. How do I enroll as a Buyer?

ANSWER: You enroll as a Buyer by applying through an application procedure offered by First Virtual. To apply, you will provide First Virtual with the information required in the First Virtual application form. By applying, you agree to follow this First Virtual Buyer TACs. For more information, First Virtual provides a "Signing Up" FAQ. Send an e-mail message to "signup@fv.com" if you want this FAQ.

Q4. What is the First Virtual Internet Payment System?

ANSWER: The First Virtual Internet Payment System is a method of communicating information between people using computers so that a person can sell ("Seller") and a person can buy ("Buyer") information, goods and services on the Internet. It has four components: a Buyer's account identification ("VirtualPIN"); e-mail queries to buy and sell information, goods and services on the Internet; the charging of a valid credit card for payment of information, goods and services bought using the Buyer's VirtualPIN; the payment of revenues to the seller after the deduction of First Virtual fees.

Q4.1. What is a VirtualPIN?

ANSWER: The Buyer's VirtualPIN is an unique set of letters and numbers. It is assigned to an applicant for buying something from a Seller.

To get a VirtualPIN, the applicant must present to First Virtual a valid credit card and a private (not shared with anyone else) e-mail address. The applicant for the VirtualPIN chooses the letters and numbers that make up part of his or her VirtualPIN. First Virtual then chooses a word prefix to make the VirtualPIN unique. By using his or her VirtualPIN to purchase, the Buyer agrees that First Virtual can charge his or her credit card for the purchase.

Q.4.1.1. Why is the Buyer's VirtualPIN important to me?

ANSWER: When you become a Buyer, you agree that your use of your VirtualPIN according to the Buyer's TACs is evidence that you agree to pay the Seller for anything purchased by you. You further agree that First Virtual can charge your credit card for what you purchase and pay the Seller according to the Seller TACs, First Virtual's agreement with the Seller.

Q4.2. What does First Virtual mean by "e-mail queries"?

ANSWER: After a Buyer presents a VirtualPIN to a Seller, the Seller can determine by several methods, including SGCP, "finger," or an e-mail query, whether the VirtualPIN is valid. After the Buyer purchases the information, goods or services from the Seller, the Seller sends, by e-mail to First Virtual, the VirtualPIN and the amount to be charged against the Buyer. Next, and before charging the Buyer, First Virtual sends an e-mail query to the Buyer asking whether the Buyer bought the information, goods or services from the Seller. The Buyer responds either with a "yes," which authorizes First Virtual to charge the Buyer with the purchase price; or "no," which tells First Virtual not to charge the Buyer; or "fraud," which tells First Virtual not to charge the Buyer and to cancel the Buyer's VirtualPIN. Buyers, please remember that the purchase is not complete until you respond with a "yes" answer to the e-mail query from First Virtual.

Q4.3. What does First Virtual do if the Buyer replies with a "no"?

ANSWER: First Virtual will e-mail the Seller, telling the Seller that the Buyer said "no," which means that First Virtual cannot charge the Buyer and thus the Seller cannot ask First Virtual to pay the Seller for what the Buyer purchased as there was no authorized purchase.

Q4.4. What does First Virtual do if the Buyer replies with "fraud"?

ANSWER: First Virtual will e-mail the Seller telling the Seller that the Buyer said "fraud," which means that First Virtual cannot charge the Buyer and thus, the Seller cannot ask First Virtual to pay the Seller for what the Buyer purchased as there was no authorized purchase. First Virtual also cancels the Buyer's VirtualPIN.

Q4.5. What does the Seller do if the Buyer replies with a "no" or "fraud" e-mail reply?

ANSWER: First, the Seller cannot ask First Virtual to pay the Seller any money for the sale. In case of a"no" e-mail reply, the Seller should decide whether to make any further sales to that Buyer. If the Seller believes that what was sold should have been paid for, then the Seller should contact the Buyer directly and attempt to resolve the dispute.

Q4.6. What will First Virtual do if I respond with a "no" answer even though I got what I purchased?

ANSWER: While First Virtual may not agree with you, First Virtual understands that you may not want to pay for what you purchased. You may or may not have a valid reason. You may e-mail the Seller, telling the Seller why you were not willing to pay for the purchase. The Seller should determine whether your reasons for not acknowledging your purchase are true or valid. On the other hand, First Virtual does not agree to a Buyer's abuse of this aspect of the First Virtual Internet Payment System. Therefore, if you make it a habit to respond "no" to e-mail purchase queries from First Virtual, First Virtual will cancel your VirtualPIN. First Virtual reserves the absolute right to determine, at its sole discretion, whether you are responding too often with a "no" answer to e-mail purchase queries. For example, responding once to an e-mail query with a "no" response, may be too often if the amount of the purchase is large.

Q4.7. What will First Virtual do if I respond with a "fraud" answer even though I got the information, goods or services?

ANSWER: The First Virtual Internet Payment System is designed to minimize the risk of fraud, but it is not foolproof. First Virtual understands that your VirtualPIN and e-mail address may be given to someone else and misused. Therefore First Virtual has no choice upon receiving a "fraud" reply to an e-mail purchase query but to cancel your VirtualPIN. There are no exceptions.

Q5. What can I buy?

ANSWER: Anything.

Q5.1. Say that again!

ANSWER: Yes, anything; information, goods and services. You can buy anything that a Seller agrees to sell using the First Virtual Internet Payment System, within the limits of your credit.

Q5.2. Can First Virtual give me an example?

ANSWER: Well, just as an example and nothing more, a Seller may offer to sell and a Buyer may buy: information such as software, text and pictures; goods such as hats, shirts and books; services such as consulting, advice and customization of software.

Q.6. What fees do I pay First Virtual?

ANSWER: The Buyer pays First Virtual a US$2 fee for setting up and maintaining the Buyer's enrollment. First Virtual charges no other fees to the Buyer. In the event you change your credit card associated with your VirtualPIN (even if only to change the expiration date), an additional US$2 maintenance fee will be charged.

Q6.1. How do I know when First Virtual charges my credit card?

ANSWER: First Virtual will e-mail you, telling you the date and amounts charged to your credit card when it is billed. On your credit card bill you will only see the notation "Internet 1st Virtual," the amount charged through the First Virtual Internet Payment System, and the date when the amount was charged to your credit card. The notation may change from time to time, but you will be notified by e-mail if the notation does change.

Q.7. What other promises do I make as a Buyer?

ANSWER: Several. Excuse us for yelling, but we will put these additional promises into caps so you can't say later that your eyes glazed over and you didn't read them:

FIRST, YOU PROMISE TO FOLLOW THE BUYER TACs;

SECOND, YOU PROMISE THAT:

* YOU ARE AUTHORIZED TO USE THE CREDIT CARD YOU PROVIDE FIRST VIRTUAL UPON APPLYING FOR YOUR VirtualPIN; * THAT THIS CREDIT CARD WILL REMAIN VALID AS LONG AS YOU USE YOUR FV BUYER'S VirtualPIN TO BUY ANYTHING USING THE FIRST VIRTUAL INTERNET PAYMENT SYSTEM ; * YOU WILL PAY ANY CHARGES POSTED TO YOUR CREDIT CARD BY FIRST VIRTUAL ACCORDING TO THE TERMS OF YOUR CREDIT CARD ACCOUNT.

THIRD, YOU UNDERSTAND THAT FV NEEDS TO USE YOUR E-MAIL MESSAGES AND, THEREFORE, YOU ALLOW FIRST VIRTUAL TO USE AND STORE THESE E- MAIL QUERIES IN ORDER TO KEEP RECORDS OF TRANSACTIONS BETWEEN YOU, FV AND A FV SELLER SO AS TO MAKE THE First Virtual Internet Payment System WORK.

Q7.1. What if I can't agree with all these Buyer TACs and "human-help" tells me that my concerns are valid; or, I send an e-mail message to First Virtual saying the I don't agree with certain Q&As, but will still become a Buyer? Does that mean this agreement has changed?

ANSWER: No (actually, h___ no!). When you become a Buyer, you are agreeing that these First Virtual Buyer TACs are our agreement. Only First Virtual can change our agreement. Your only choice is to not become a Buyer. If First Virtual changes these Buyer TACs and you don't agree to the change, you can stop buying as a First Virtual Buyer and thus end this agreement (see Q&A#1.2 as to how you can receive notices of any changes to this agreement).

Q8. What risks do I assume as a Buyer?

ANSWER: The biggest risk that you assume is that your VirtualPIN will be used fraudulently. A person could get your VirtualPIN and use it. This alone will not allow the person to charge a purchase to your VirtualPIN. But, if the person using your VirtualPIN also has access to your e-mail address (remember our agreement is that it is private — only accessible by you) so that he or she can respond "yes" to First Virtual's e-mail purchase query, First Virtual would charge your credit card. If you get a query from First Virtual asking whether you purchased something from a Seller and you know that you did not purchase it, you agree to reply "fraud." First Virtual will cancel your

VirtualPIN and you will have to reapply. You are also assuming the risk that a disaster of any kind (political, labor, natural) or an act of God may occur that terminates or suspends First Virtual's operation of the First Virtual Internet Payment System.

Q8.1. What does First Virtual mean by disaster or act of God?

ANSWER: Well, you need to be a little paranoid to understand what we are agreeing to here. There is the possibility that something can happen that First Virtual has no control over. It could be an earthquake, a flood, a break down of all electrical or communications facilities or an invasion from Mars. If something, anything, like this happens and First Virtual cannot operate the First Virtual Internet Payment System, then you can not buy anything on the Internet using the First Virtual Internet Payment System.

Q8.2. OK, I agree to that, but what if I suffer a loss because of the fault of First Virtual's people or because of a malfunction of First Virtual's software or machines?

ANSWER: Well, we can't imagine how such a situation would occur. But if it did occur, First Virtual is responsible. However since First Virtual does not charge you any fees other than the set up fee. In return for this low fee, you are agreeing that First Virtual's liability to you should be limited. Thus, you are agreeing that First Virtual's sole and exclusive obligation to you in this situation is to make a reasonable effort to correct any data that has been lost, corrupted or damaged by First Virtual's people, software or machines.

Q8.2.1. What if I lose money, or spend money I didn't plan on spending, or lose the opportunity to make or save money because of the fault of First Virtual's people or because of a malfunction of First Virtual's software or machines?

ANSWER: As stated in the ANSWER to Q&A#8.2, First Virtual will only make reasonable efforts to correct any damaged, corrupted or incorrect data. You cannot recover the amount of any loss or other damages you, the Buyer, incur even if you prove that the loss occurred because of the fault of First Virtual's people or because of a malfunction of First Virtual's software or machines or systems failure.

Q8.2.2. Can I sue someone else, like the First Virtual person who caused the problem, or a First Virtual supervisor, or the credit card company or anyone else who First Virtual contracts or works with to provide the First Virtual Internet Payment System?

ANSWER: No.

Q8.2.2.1. Why not?

ANSWER: For several reasons: First, First Virtual is a corporation and thus legally you can only sue First Virtual and not its employees, consultants, officers, directors and shareholders. By becoming a First Virtual Buyer, you agree to follow this legal principle by not suing First Virtual's employees, consultants, officers, directors and shareholders, no matter the reason. Next, First Virtual and others are spending much time and money to make the First Virtual Internet Payment System work. We do not want to be sued for every mistake, be it negligent or willful, which we and others who work with us make. First Virtual will treat you fairly. The bottom line is that when you become a Buyer you agree to give up your rights to sue us and others associated with First Virtual, whoever they may be. So, don't become a Buyer if you can't agree to this limitation on the liability of First Virtual and the people and other companies that contract or work with First Virtual in providing the First Virtual Internet Payment System.

Q9. What promises are First Virtual making to me in return for my agreeing to become a Buyer?

ANSWER: We thought you'd never ask! First Virtual agrees to follow these Buyer TACs. First Virtual is agreeing to nothing else. In fact, First Virtual DISCLAIMS ALL WARRANTIES WITH RESPECT TO THE SERVICES AND PRODUCTS PROVIDED UNDER THESE BUYER TACs. FIRST VIRTUAL IS NOT MAKING ANY IMPLIED OR LEGALLY REQUIRED PROMISE OR WARRANTY TO YOU, THE FIRST VIRTUAL BUYER, SUCH AS THE WARRANTY OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE.

Q9.1. Why is First Virtual yelling at me (putting the words in caps)?

ANSWER: The law of Wyoming, which governs this agreement, requires that we put in capital letters our disclaimers of certain warranties that are usually implied by the law. Sorry, but this is probably the first time you are reading them and the law requires that we yell.

Q10. What if I have a dispute with a Seller?

ANSWER: If you have any kind of dispute with a Seller, you are encouraged to negotiate with the Seller to resolve the dispute.

Q10.1. What if we can't agree on a solution?

ANSWER: First Virtual reserves the right, at First Virtual's sole discretion, to honor the Buyer's request for a refund and to deduct the amount of that refund from the amount due to the Seller.

Q10.2. What if I ask my credit card company to chargeback the purchase?

ANSWER: If First Virtual is told by the credit card company that there has been a Chargeback on a purchase by a Buyer, First Virtual will do two things. First, it will chargeback the purchase to the First Virtual Seller as outlined in the Seller Q&As. Next, it will cancel the Buyer's VirtualPIN and terminate its relationship with that Buyer.

Q11. What if I have a dispute with First Virtual?

ANSWER: If you have any kind of dispute with First Virtual over anything, First Virtual would ask you to e-mail us about your dispute at "humanhelp@fv.com" before you do anything. First Virtual wants to treat you fairly and will do everything it can to resolve disputes reasonably. But, if First Virtual and a Buyer cannot resolve a dispute, and the buyer decides to file a lawsuit, then the Buyer must sue First Virtual in the appropriate court in Cheyenne, Wyoming.

Q12. How do we end our agreement?

ANSWER: First, you can stop using the First Virtual Payment System. Next, either First Virtual or the Buyer can notify the other that this agreement has ended.

Q12.1. Can First Virtual end this agreement with me for any reason, or for no reason?

ANSWER: Yes, at any time and without any prior notice. First Virtual may tell you not to use the First Virtual Internet Payment System again.

Q12.2. Can I end this agreement with First Virtual for any reason, or for no reason?

ANSWER: Yes, at any time you choose by notice to First Virtual.

Q12.3. What obligations do we have to each other if we end this agreement?

ANSWER: Well, you still have the obligation to pay any amounts charged to your credit card for charges made using the First Virtual Internet Payment System.

Q13. Can First Virtual change these Buyer TACs?

ANSWER: Yes, First Virtual can change these Buyer TACs whenever it wants. First Virtual has no intention of changing these Buyer TACs often, but First Virtual will change these Buyer TACs whenever applicable law requires a change, or the credit card companies change their operating procedures, or whenever First Virtual introduces new protocols or other structural changes that require these Buyer TACs to change.

Q14. What if there are inconsistencies between these Buyer TACs, any FAQ or anything else published by First Virtual, like the Seller or InfoHaus TACs?

ANSWER: The first rule of interpretation is that these Buyer TACs govern our agreement. The FAQs affect our agreement and how we act towards each other as long as they is consistent with these Buyer TACs. If the FAQs are inconsistent with these Buyer TACs, these Buyer TACs govern our agreement.

Q14.1. What if a court decides that some part of this agreement is invalid, does that invalidate this whole agreement?

ANSWER: No. We agree that if a court tells us that a part of our agreement is invalid and thus not binding on us, we agree that the rest of our agreement is still valid and should be interpreted as we have agreed in Q&A#14.2.

Q14.2. I've never seen an agreement like this before, how is it to be interpreted?

ANSWER: Well, first remember that our agreement is being drafted this way because First Virtual thinks it will make it easier for First Virtual and you to understand our obligations to each other. We agree that each question and answer is to be read together. In other words, you don't take the words from a question and say "that's our agreement." Instead you read all the questions and the answers together when you try to determine what we have agreed. Finally, neither of us is perfect, so if we've left something out, or if something is not clear, then we agree that any court or person trying to interpret this agreement should apply it so that it limits First Virtual's liability to a Buyer or Buyers to (i) making reasonable efforts to correct data lost, corrupted or damaged, and, (ii) refunding any fees paid to First Virtual. We both realize that this is a significant limitation on your right to sue and recover money from First Virtual, but frankly it is the cost of having the opportunity to buy things on the Internet using the First Virtual Internet Payment System.

(Reprinted with permission from First Virtual Holdings Incorporated, 1996)

SELLER'S TERMS AND CONDITIONS

Seller's Agreement with First Virtual Holdings Incorporated Effective December 16, 1995

The following questions and answers are called the First Virtual Seller Terms and Conditions ("First Virtual Seller TACs" or "Seller TACs"). These First Virtual Seller TACs are the only agreement between First Virtual Holdings Incorporated and you, the Seller using the First Virtual Internet Payment System. When you become a First Virtual Seller as provided in Q&A#3, we both agree to act according to these First Virtual Seller TACs, our agreement. We also agree that each numbered question and answer are to be read and applied together as the expression of one complete idea or "term" as it is called in the law. All the questions and answers are to be interpreted in a consistent manner as agreed in Q&A#14.2.

Q1. Who is First Virtual Holdings Incorporated?

ANSWER: First Virtual Holdings Incorporated is a Wyoming corporation with its principal business office at 11975 El Camino Real, Suite 300, San Diego, CA 92130-5545 and its Wyoming address at 1720 Carey Avenue or PO Box 1436, Cheyenne, Wyoming 82003-1436. Hereafter, we will call First Virtual Holdings Incorporated "First Virtual," or "FV." As used herein, the following are trademarks of First Virtual Holdings Incorporated: First Virtual Internet Payment System; VirtualPIN; InfoHaus.

Q1.1. How can I contact First Virtual?

ANSWER: It depends. If you want more information about First Virtual, send e-mail to "info@fv.com". This will give you general information on First Virtual and also tell you how to get FAQs (Frequently Asked Questions) on selected topics. For questions that are not answered by the First Virtual's FAQs, e-mail your question to "human-help@fv.com". Please remember that FAQs and e-mail from "human-help" are not a part of our agreement.

Q1.2. How will I know when these First Virtual Seller TACs change?

ANSWER: First Virtual will e-mail you a message telling you when a change is made to this agreement as it is published if you send e- mail to "fineprint-changes-request@fv.com" and subscribe to the fineprint-changes mailing list in accordance with our instructions, after you sign up as a Seller.

Q1.3. Are the e-mail messages I send to First Virtual private?

ANSWER: No. It is possible that any message you send to First Virtual may be read by anyone or everyone at First Virtual. You must also assume that e-mail sent may be read by someone other than the intended recipient. Also, all messages sent to First Virtual are the property of First Virtual.

Q2. Who am I?

ANSWER: You are not a minor (younger than age 18) and you are applying to be a First Virtual Seller. If you complete the application

process according to Q&A#3, you are agreeing to the terms of this Agreement.

Q2.1. What does it mean to be "a First Virtual Seller"?

ANSWER: It means that you completed the application process according to Q&A#3, First Virtual accepted your application, and you have accepted at least one VirtualPIN for payment when selling something using the First Virtual Internet Payment System. This also means that you agree to follow the agreement as reflected in these Seller TACs. It also means that as a First Virtual Seller you can use the First Virtual Internet Payment System to sell information, goods and services. Hereafter, we will just call you the "Seller" or "you" or "I."

Q2.2. How does First Virtual contact me?

ANSWER: First Virtual contacts you through the e-mail address that you provide First Virtual during the application process. You agree that First Virtual sends all notices to this e-mail address. Just as an example, notices may include e-mail queries that are used in the First Virtual Internet Payment System (See Q&A#4 for further details), notices of payments made to your bank account, or any other notices required for any reason. First Virtual may get other addresses from you, such as postal addresses, but they are not used for purposes of providing any notice under this agreement.

Q2.3. What if my e-mail address changes or I no longer have an e-mail address?

ANSWER: If your e-mail address changes, you must inform First Virtual by e-mail from your old e-mail address. In other words, don't inform First Virtual from your new e-mail address that the old e-mail address is no longer valid. First Virtual does not consider this a valid e-mail address change. During the period you do not have an e-mail address, you cannot be a Seller. The First Virtual Internet Payment System requires a current private (not shared with anyone else) e-mail address for the Buyer and Seller to buy and sell information. In the event you change e-mail addresses without properly notifying First Virtual, you must reapply as a Seller and pay any set up fees. First Virtual only delivers notices to your e-mail address as provided by you according to these Seller TACs.

Q3. How do I become a Seller?

ANSWER: You become a Seller by applying through an application procedure offered by First Virtual. To apply, you will provide First Virtual with the information required in the First Virtual application form. By applying, you agree to follow these First Virtual Seller TACs. For more information, First Virtual provides a "Signing Up" FAQ. Send an e-mail message to "signup@fv.com" if you want this FAQ.

Q4. What is the First Virtual Internet Payment System?

ANSWER: The First Virtual Internet Payment System is a method of communicating information between people using computers so that a person can sell ("Seller") and a person can buy ("Buyer") information, goods and services on the Internet. It has four components: a Buyer's account identification ("VirtualPIN"); e-mail queries to buy and sell information, goods and services on the Internet; the charging of a valid credit card for payment of information, goods and services bought using the Buyer's VirtualPIN; the payment of revenues to the seller after the deduction of First Virtual fees.

Q4.1. What is a VirtualPIN?

ANSWER: The Buyer's VirtualPIN is an unique set of letters and numbers. It is assigned to an applicant for buying something from a Seller. To get a VirtualPIN, the applicant must present to First Virtual a valid credit card and a private (not shared with anyone else) e-mail address. The applicant for the VirtualPIN chooses the letters and numbers that make up part of his or her VirtualPIN. First Virtual then chooses a word prefix to make the VirtualPIN unique. By using his or her VirtualPIN to purchase, the Buyer agrees that First Virtual can charge his or her credit card for the purchase.

Q.4.1.1. Why is the Buyer's VirtualPIN important to me?

ANSWER: When you become a Seller, you agree that the Buyer's use of the VirtualPIN according to the Buyer's TACs is an acceptable form of payment for the information, goods and services you sell using the First Virtual Internet Payment System.

Q4.2. What does First Virtual mean by "e-mail queries"?

ANSWER: After a Buyer presents a VirtualPIN to a Seller, the Seller can determine by several methods, including SGCP, "finger," or an e-mail query, whether the Buyer's VirtualPIN is valid. After the Buyer purchases the information, goods or services from the Seller, the Seller sends by e-mail to First Virtual the Buyer's VirtualPIN and the amount to be charged against that account. Next, and before charging the Buyer's account, First Virtual sends an e-mail query to the Buyer asking whether the Buyer bought the information, goods or services from the Seller. The Buyer responds either with a "yes," which authorizes First Virtual to charge the Buyer for the purchase price; or "no," which tells First Virtual not to charge the Buyer; or "fraud," which tells First Virtual not to charge the Buyer and to cancel the Buyer's VirtualPIN.

Q4.3. What does First Virtual do if the Buyer replies with a "no"?

ANSWER: First Virtual will e-mail the Seller, telling the Seller that the Buyer said "no," which means that First Virtual cannot charge the Buyer and thus the Seller cannot ask First Virtual to pay the Seller since there was no authorized purchase.

Q4.4. What does First Virtual do if the Buyer replies with "fraud"?

ANSWER: First Virtual will e-mail the Seller telling the Seller that the Buyer said "fraud," which means that First Virtual cannot charge the Buyer and thus, the Seller cannot ask First Virtual to pay the Seller since there was no authorized purchase. First Virtual also cancels the Buyer's VirtualPIN.

Q4.5. What does the Seller do if the Buyer replies with a "no" or "fraud" e-mail reply?

ANSWER: First, the Seller cannot ask First Virtual to pay the Seller any money for the sale. In case of a "no" e-mail reply, the Seller should decide whether to make any further sales to that Buyer. If the Seller believes that the sale occurred and that the Buyer should pay the Seller, then the Seller should contact the Buyer directly and attempt to resolve the dispute.

Q4.6. What will First Virtual do to protect the Seller against a "no" answer?

ANSWER: First Virtual can do nothing to protect you against a "no" answer. It is the nature of any purchase that a Buyer can dispute a purchase after ordering the information, goods or services.

Q4.7. What will First Virtual do to protect the Seller against a "fraud" answer?

ANSWER: The First Virtual Internet Payment System is designed to minimize the risk of fraud, but it is not foolproof. First Virtual cannot promise you that you will not be defrauded. You can help First Virtual protect against fraud by sending a query to First Virtual about the validity of a Buyer's account before selling anything. (See Q&A#4.2) A reply from First Virtual that the VirtualPIN is active tells you that the applicant received that VirtualPIN, presented First Virtual with a valid credit card, agrees to follow the Buyer's agreement ("Buyer TACs") and has not replied with a "fraud" reply to a previous e-mail query. It does not, however, mean that the VirtualPIN is not being used fraudulently (by a different person than the applicant) at that time. It also does not mean that the Buyer's credit card company will pay First Virtual for the Buyer's purchase. According to Q&A#6.2, if the credit card company does not pay First Virtual for any reason, First Virtual will not pay the Seller.

Q5. What can I sell?

ANSWER: Anything.

Q5.1. Say that again!

ANSWER: Yes, anything; information, goods and services. You can sell anything that a Buyer agrees to buy using the First Virtual Internet Payment System.

Q5.2. Can First Virtual give me an example?

ANSWER: Well, just as an example and nothing more, a Seller may offer to sell and a Buyer may buy: information such as software, text

and pictures; goods such as hats, shirts and books; services such as consulting, advice and customization of software.

Q5.2.1 Are the sales of information, goods and services treated differently?

ANSWER: Unfortunately, yes. When you sell information, delivery, as you know will be at the same time as the e-mail queries confirming the transaction. But, when you sell goods or services, delivery may be at a later date. This delay in delivery can cause you, the Seller, a big problem. If you don't ship the goods purchased immediately or perform the services immediately, there is the possibility that the First Virtual Buyer will see the charge on his or her credit card prior to receipt of the goods or services. This will cause the Buyer to Chargeback (See Q&A#7.2.1) the purchase and you will not get paid for your goods or services. Therefore you must promise unconditionally that YOU, THE SELLER, WILL SHIP ALL GOODS SOLD USING THE First Virtual Internet Payment System WITHIN TWENTY-FOUR (24) HOURS OF RECEIVING CONFIRMATION FROM FIRST VIRTUAL THAT THE BUYER HAS SAID "YES." YOU MUST ALSO PROMISE THAT SERVICES HAVE BEEN PERFORMED PRIOR TO SENDING THE E-MAIL QUERY NOTIFYING FIRST VIRTUAL OF THE TRANSACTION. WE ARE YELLING BECAUSE THIS IS IMPORTANT. IF YOU DON'T WANT CHARGEBACKS YOU MUST SELL GOODS AND SERVICES THIS WAY.

Q5.3. What if I sell something illegal (like obscenity or pirated code or something stolen) or the way in which I sell it is illegal (like false advertising)?

ANSWER: Don't sell it! Really. First Virtual does not decide what is legal or illegal. First Virtual cooperates with any person (be it a government or private person) who tells First Virtual that you are selling illegally. Further as a First Virtual Seller you promise First Virtual that you will not use illegal methods nor sell anything illegal. You also promise to defend First Virtual and hold it harmless from any expense or other damage for any claim of illegality made against First Virtual because of your illegal methods or the sale of something illegal.

Q5.4. What does it mean that First Virtual will cooperate with any government or private person?

ANSWER: It means that First Virtual protects the Buyers and First Virtual. First Virtual will decide when and with whom it cooperates. First Virtual will follow the laws and requests of any government that First Virtual thinks has jurisdiction over First Virtual. This may mean that you will not get paid. If a private person has a subpoena or court order that First Virtual thinks is binding on First Virtual, First Virtual cooperates. If the private person does not have a subpoena or court order, First Virtual still acts to protect itself. First Virtual also reviews a Seller's account and acts appropriately to protect First Virtual if First Virtual gets any information about a Seller that suggests potential problems with the law. Remember, as we have agreed in Q&A#12.1, First Virtual can end this agreement for any reason or no reason.

Q5.5. So, why should I use the First Virtual Internet Payment System if First Virtual gives information about me to a government, or to a private person, with or without a proper subpoena or court order?

ANSWER: Well, first don't use the First Virtual Internet Payment System for illegal purposes! Next, you have no expectation of privacy in these e-mail queries or any other information you provide First Virtual. The only information First Virtual can give is information you have given First Virtual through your use of the First Virtual Internet Payment System. For example, First Virtual has information you provided when you set up your account, such as your e-mail address, the name you use to sell using the First Virtual Internet Payment System, and your bank account where we send payments to you. First Virtual also has a record of all Seller and Buyer queries that were processed through the First Virtual Internet Payment System. First Virtual may also have information about you as a Buyer, but that is only if you have enrolled as a Buyer. First Virtual will also make any other information about you in its paper or data files available.

Q5.6. Will First Virtual tell me if someone reports that I am selling something illegally?

ANSWER: Yes. First Virtual cannot promise to tell you in every instance, but will attempt to do so by e-mail. If the person requesting the information has the authority (and if First Virtual agrees that they have the authority) to tell First Virtual not to tell you, First Virtual will not tell you.

Q.6. What fees do I pay First Virtual?

ANSWER: You will pay First Virtual a US$10 fee for enrolling as a Seller, and each time you change your checking account. Also, when a Seller makes a sale using the First Virtual Internet Payment System, the Seller pays First Virtual, for each sale, a fee of US$0.29 plus 2% of the amount of the transaction ("Transaction Fee"). First Virtual deducts this Transaction Fee at the time that First Virtual deposits all amounts due the Seller for sales made using the First Virtual Internet Payment System. The time that First Virtual deposits these amounts is called the "Settlement Date." At the Settlement Date, First Virtual will also deduct an additional charge of $1.00 for the cost of processing your payment and depositing the funds in your bank account. The $1.00 fee is called the Settlement Fee. The Net Sales Amount consists of all sales amounts due the Seller minus the sum of the Transaction Fee and the Settlement Fee. The Net Sales amount will be deposited to your bank account only when it has reached a minimum of US$10.00. There are no other fees charged to the Seller.

Q6.1. Can First Virtual give me an example?

ANSWER: Well, just as an example and nothing more, this means that: When you sell something for $1.00, First Virtual charges you a Transaction Fee of 2% (2 cents) plus 29 cents for a total of 31 cents ($0.31) and credits you with $0.69. When you sell something for $10.00, First Virtual charges you a Transaction Fee of 2% (20 cents) plus 29 cents for a total of 49 cents and credits you with $9.51. When you sell something for $100.00, First Virtual charges you a Transaction Fee of 2% ($2) plus 29 cents for a total of $2.29 and credits you with $97.71. If these three transactions were the only sales you made before your next Settlement Date, First Virtual would total your sales of $111, minus each Transaction Fee (totaling $3.09), deduct the $1.00 Settlement Fee for a total of $4.09, and remit the Net Sales Amount of $106.91 into your bank account.

Q6.2. When is the Settlement Date?

ANSWER: It depends. First, it will always depend upon how long it takes First Virtual to collect payment from the Buyer once the Buyer has agreed to pay with a "yes" e-mail reply. First Virtual will not pay you until it receives payment from the Buyer's credit card.

First Virtual also establishes internal procedures about when a Buyer's credit card will be charged. First Virtual agrees not to establish unreasonable procedures by choice in this regard.

After a Buyer's credit card is successfully charged, and if First Virtual gets paid, First Virtual will wait 91 days until paying you for the transaction (see Q.6. and Q6.1. for settlement details).

Q6.3. Why the 91-day wait and do I get interest on the Net Sales Amount during the holding period?

ANSWER: Credit card issuers allow Buyers, under certain circumstances, to dispute (chargeback) a charge. First Virtual will not pay you until First Virtual has been paid in full and there is a minimal probability of a chargeback. (See Q&A#7.2.2 about Chargeback Rules) Further, you will not receive interest on the Net Sales Amount during the waiting period.

Q6.4. What if the amount due the Seller is less than the US$1.00 Settlement Fee?

ANSWER: First Virtual does not deposit the amounts due the Seller until and unless they exceed the minimum Net Sales Amount of US$10.00.

Q6.5. What if the Net Sales Amount is a negative number because of the Chargeback Rules?

ANSWER: Please read Q&A#7.2.4 and 10.3.

Q6.6. How do I know when First Virtual deposits the Net Sales Amount into my bank account?

ANSWER: First Virtual will e-mail you, telling you the date and Net Sales Amount deposited into your bank account.

Q.7. What other promises do I make as a Seller?

ANSWER: Several. Excuse us for yelling, but we will put these additional promises into caps so you can't say later that your eyes glazed over and you didn't read them:

FIRST, YOU AGREE TO FOLLOW THE TERMS AND CONDITIONS OF THESE SELLER TACs.

SECOND, YOU AGREE TO FOLLOW THE PROCEDURES ESTABLISHED BY FV FROM TIME TO TIME.

THIRD, YOU AGREE NOT TO USE ILLEGAL METHODS TO SELL ANYTHING, NOR SELL ANYTHING ILLEGAL, AND YOU AGREE THAT NO SUCH SALE OR OFFER TO SELL WILL INFRINGE ANY PATENT, TRADEMARK OR COPYRIGHT OWNED BY OTHERS.

FOURTH, YOU AGREE TO KEEP RECORDS OF ALL SALES DATA FOR FIVE (5) YEARS FROM THE DATE OF ANY SALE AND AGREE TO PROVIDE FIRST VIRTUAL COPIES OF THE RECORDS WHEN REQUESTED.

FIFTH, YOU AGREE NOT TO COPY, DISTRIBUTE, RENT, LEASE OR SUB LICENSE ALL OR ANY PORTION OF ANY SOFTWARE CODE PROVIDED TO YOU BY FIRST VIRTUAL. YOU ALSO AGREE NOT TO MODIFY OR PREPARE DERIVATIVE WORKS OF THIS SOFTWARE CODE. YOU ALSO AGREE NOT TO REVERSE ENGINEER, DECOMPILE OR DISASSEMBLE ANY OF THIS SOFTWARE CODE.

SIXTH, YOU AGREE THAT IF YOU USE THE MARKS "FIRST VIRTUAL", "INFOHAUS" OR "First Virtual Internet Payment System" ANYWHERE, THAT YOU WILL PLACE THE SYMBOL "TM" NEXT TO IT AND INDICATE IN AT LEAST 8PT TYPE THAT THE MARK "FIRST VIRTUAL" IS A REGISTERED TRADEMARK OF FIRST VIRTUAL HOLDINGS INCORPORATED, AND ALL RIGHTS TO THIS MARK ARE OWNED BY FIRST VIRTUAL HOLDINGS INCORPORATED. YOU MAY USE FIRST VIRTUAL'S LOGOS TO PROMOTE YOUR BUSINESS AND THE USE OF FIRST VIRTUAL BY YOUR CUSTOMERS.

SEVENTH, YOU UNDERSTAND THAT FV NEEDS TO USE YOUR E-MAIL AND THEREFORE YOU ALLOW FIRST VIRTUAL TO USE AND STORE THESE E-MAIL QUERIES IN ORDER TO KEEP RECORDS OF TRANSACTIONS BETWEEN YOU, FV AND A FV BUYER SO AS TO MAKE THE FIRST VIRTUAL INTERNET PAYMENT SYSTEM WORK.

EIGHTH, YOU WILL AGREE THAT YOU ARE RESPONSIBLE FOR FILING ANY STATE SALES TAX RETURN THAT YOU MIGHT BE

LEGALLY REQUIRED TO FILE, AND TO PAY ANY TAX DUE. FIRST VIRTUAL IS NOT A SELLER, NOR WILL IT REPORT ANY TAXES DUE FROM YOU, NOR PAY ANY SUCH TAX.

FINALLY, YOU AGREE TO TAKE FULL RESPONSIBILITY FOR ANY STATE TRANSACTION TAX OR SIMILAR CHARGE IMPOSED ON YOUR SALE OF ANYTHING USING THE FIRST VIRTUAL INTERNET PAYMENT SYSTEM.

Q7.1. What if I can't agree with all these Seller TACs and "human-help" tells me that my concerns are valid; or, I send an e-mail message to First Virtual saying that I don't agree with certain Q&As, but will still become a Seller? Does that mean this agreement has changed?

ANSWER: No (actually, h___ no!). When you become a Seller, you are agreeing that these First Virtual Seller TACs are our agreement. Only First Virtual can change our agreement. Your only choice is to not become a Seller. If First Virtual changes these Seller TACs and you don't agree to the change, you can stop selling as a First Virtual Seller and thus end this agreement (see Q&A#1.2 as to how you can receive notices of any changes to this agreement).

Q7.2.1. What is the relationship between these Seller TACs and the "Seller FAQs"?

ANSWER: The "Seller FAQs" are operating rules that provide you, among other things, with guidance on when and how to charge a Buyer's account. They are based upon credit card company operating regulations, applicable law and First Virtual's belief that you must treat your Buyer fairly. They may change from time to time and you are agreeing to be bound by them by becoming a Seller. First Virtual agrees that these "Seller FAQs" will not be arbitrary, but we both know that we have to follow the rules and procedures of the credit card companies, the appropriate authorities, and First Virtual if we want to do business.

Q7.2.2. What are the Chargeback Rules?

ANSWER: The term "Chargeback" refers to the debiting from you or withholding from Net Sales Amounts all or part of the amount of a particular sale. As a Seller, you agree to honor Chargeback Rules as established by the Buyer's credit card company. As examples, but nothing more, chargebacks may occur for the following reasons:

The credit cardholder account number was listed in a restricted card list at the time of the sale or is otherwise invalid; The sale exceeds the floor limit and was not authorized or required authorization was not obtained; The sale was authorized but not for the exact amount or for the wrong transaction date; The cardholder never received the merchandise/services requested; The cardholder's credit was processed as a sale; The sales slip contains an error in arithmetic; The cardholder was charged incorrectly; The cardholder was never credited for returned merchandise or a canceled order; The card was expired, counterfeit, altered, or invalid at the time of the sale; The cardholder's sales slip was deposited more than once; The cardholder did not authorize the transaction; The authorization code is invalid; The sales slip was not signed by the cardholder unless it was mail order, telephone order or preauthorized order in compliance with the agreement and authorized by the cardholder and indicated as such on the sales slip; If a cardholder asserts any disputes, claim, counterclaim, defense or offset against the seller, whether or not the assertion is valid; The sales draft or sales data or any material information thereon is illegible, incomplete, inaccurate or unsigned, or is not delivered to the credit card company within the required time limits; The sales draft or sales data is fraudulent or does not represent a bona fide transaction in the ordinary course of the seller's business, or is subject to any claim of illegality, negligence, dishonesty or offset; The seller/merchant has failed to provide copies of sales drafts requested by the credit card company within the prescribed time period; Suspicious transactions and fraudulent transactions are also subject to chargebacks.

You also agree to honor any other credit card company operating rule or procedure. You also agree to honor the time limitations for a credit card customer (herein, the Buyer) charging back a charge to a credit card as required under the Federal Truth in Lending Act or Regulation E or Regulation Z of the Board of Governors of the Federal Reserve System or any applicable State law. No matter what, you agree to honor any Chargebacks made within one year of First Virtual's charge to the Buyer's credit card.

Q7.2.3. Is there anything else I should know about the Chargeback Rules?

ANSWER: Yes. These rules are designed to protect the credit card customer (herein, the Buyer) and there will be times when First Virtual needs your cooperation so as to provide information to the credit card

companies. If First Virtual requests additional information from you and you do not provide the information within ten (10) days of First Virtual's request, then you agree that the one year period within which the Buyer can make the chargeback request (as stated in the answer to Q#7.2.2) is extended to three years.

Q7.2.4. What does honoring the Chargeback Rules mean?

ANSWER: Among other things, it means that you agree that First Virtual can deduct from your Seller's Net Sales Amount any money that the credit card company charges back for your sales according to the Chargeback Rules.

Q7.2.5. What if I don't think the Chargeback is valid?

ANSWER: You cannot dispute First Virtual's deduction from your Seller's Net Sales Amount for a Chargeback done according to the Chargeback Rules.

Q8. What risks do I assume as a Seller?

ANSWER: You are assuming the risk that the Buyer may never pay First Virtual for various reasons (such as a claim of fraud, dissatisfaction with the thing sold, etc.) and thus you may never get paid. You are assuming the risk that a disaster of any kind (political, labor, natural) or an act of God may occur that stops First Virtual from paying you.

Q8.1. Is the money due me insured or otherwise protected?

ANSWER: No. The money due you is not insured or otherwise protected. First Virtual is not a bank.

Q8.2. What does First Virtual mean by disaster or act of God?

ANSWER: Well, you need to be a little paranoid to understand what we are agreeing to here. There is the possibility that something can happen that First Virtual has no control over. It could be an earthquake, a flood, a breakdown of electrical or communications facilities or an invasion from Mars. If something, anything, like this happens and First Virtual cannot pay you because of this happening, you assume the risk of not getting paid.

Q8.2.1. Lets get specific, can First Virtual give me an example?

ANSWER: Just as an example and nothing more, let's suppose that a natural catastrophe occurs, destroying the telephone or electrical lines that serve First Virtual's servers and several e-mail queries confirming sales are not processed or data is destroyed. Because of this occurrence, the Seller ships something and the Buyer later says he or she didn't buy it. What happens? Well, since the Buyer has not agreed to the sale, First Virtual cannot charge the Buyer and the Seller cannot get paid by First Virtual. The key fact here, is that First Virtual was not at fault. Now, if you think First Virtual was at fault, your only remedy is as we agree in Q&A#11.

Q8.2.2. OK, I agree to that, but what if I can prove that my loss was because of the fault of First Virtual's people or because of a malfunction of First Virtual's software or machines?

ANSWER: Well, then First Virtual is responsible. However the fees First Virtual charge Sellers are quite small, so in return for this lower fee, you agree that First Virtual's liability to you should be limited. Thus, you are agreeing that First Virtual's sole and exclusive obligation to you in this situation is to make reasonable efforts to correct any data that has been lost, corrupted or damaged by First Virtual's people, software or machines.

Q8.2.3. What if I lose money, or spend money I didn't plan on spending, or lose the opportunity to make or save money because of the fault of First Virtual's people or because of a malfunction of First Virtual's software or machines?

ANSWER: As stated in the ANSWER to Q&A#8.2.2, First Virtual will only make reasonable efforts to correct any damaged, corrupted or incorrect data or systems failure. You can only recover the amount that you paid First Virtual for Transaction or Settlement Fees on the transactions in which data was lost, corrupted or damaged and First Virtual was at fault and charged you. You cannot recover the amount of any loss or other damages you, the Seller, incur even if you prove that the loss occurred because of the fault of First Virtual's people or because of a malfunction of First Virtual's software or machines or systems failure.

Q8.2.4. Can I sue someone else, like the First Virtual person who caused the problem, or a First Virtual supervisor, or the credit card company or anyone else who First Virtual contracts or works with to provide the First Virtual Internet Payment System?

ANSWER: No.

Q8.2.5. Why not?

ANSWER: For several reasons: First, First Virtual is a corporation and thus legally you can only sue First Virtual and not its employees, consultants, officers, directors and shareholders. By becoming a First Virtual Seller, you agree to follow this legal principle by not suing First Virtual's employees, consultants, officers, directors and shareholders, no matter the reason. Next, First Virtual and others are spending much time and money to make the First Virtual Internet Payment System work. We do not want to be sued for every mistake, be it negligent or willful, which we and others who work with us make. First Virtual will treat you fairly. The bottom line is that when you become a Seller you agree to give up your rights to sue First Virtual and others associated with First Virtual, whoever they may be. So, don't become a Seller if you can't agree to this limitation on the liability of First Virtual and the people and other companies that contract or work with First Virtual in providing the First Virtual Internet Payment System.

Q9. What promises is First Virtual making to me in return for my agreeing to become a Seller?

ANSWER: We thought you'd never ask! First Virtual agrees to follow these Seller TACs. First Virtual is agreeing to nothing else. In fact, First Virtual DISCLAIMS ALL WARRANTIES WITH RESPECT TO THE SERVICES AND PRODUCTS PROVIDED UNDER THESE SELLER TACs. THIS IS OUR ONLY AGREEMENT. FIRST VIRTUAL IS NOT MAKING ANY IMPLIED OR LEGALLY REQUIRED PROMISE OR WARRANTY TO YOU, SUCH AS THE WARRANTY OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE.

Q9.1. Why is First Virtual yelling at me (putting the words in caps)?

ANSWER: The law of Wyoming, which governs this agreement, requires that we put in capital letters our disclaimers of certain warranties that are usually implied by the law. Sorry, but this is probably the first time you are reading them and the law requires that we yell.

Q10. What if I have a dispute with a Buyer?

ANSWER: If you have any kind of dispute with a Buyer, you are encouraged to negotiate with the Buyer to resolve the dispute. Remember, you have agreed to treat each Buyer fairly.

Q10.1. What if we can't agree on a solution?

ANSWER: First Virtual reserves the right, at First Virtual's sole discretion, to honor the Buyer's request for a refund and to deduct the amount of that refund from the amount due to you, the Seller.

Q10.2. What if the Buyer asks his or her credit card company to Chargeback the purchase?

ANSWER: If First Virtual is told by the credit card company that there has been a Chargeback on a purchase by a Buyer, First Virtual will do two things. First, First Virtual will Chargeback the purchase to the First Virtual Seller. Next, First Virtual will cancel the Buyer's VirtualPIN and terminate its relationship with that Buyer.

Q10.2.1. So is there a risk that the Seller won't get paid by the Buyer because of the Chargeback Rules?

ANSWER: Yes.

Q10.3. What if the Net Sales Amount due me, the Seller, is not enough for First Virtual to recover the amount I owe because of Chargeback(s)?

ANSWER: Then, you must deposit with First Virtual the amount you owe because of the Chargeback(s). If you don't do this within the amount of time First Virtual gives you to do it, First Virtual will end this agreement and cancel your enrollment as a First Virtual Seller.

Q10.4. What if I have a Buyer's VirtualPIN also?

ANSWER: First Virtual will not charge your Buyer's VirtualPIN, as that is not how the First Virtual Internet Payment System works. However, First Virtual may cancel your enrollment as a First Virtual Buyer.

Q10.5. OK, as a Seller, I agree to this process involving Chargebacks, but what if First Virtual or the credit card company does something wrong or makes a mistake?

ANSWER: Guess what? Remember Q&A#8 through 8.2.5 where you agreed that you could not and would not sue anyone associated with First Virtual? Well, if you want to be and remain a Seller, you have to agree to give up all your rights to sue First Virtual or the credit card company or anyone who works with either of them to implement the First Virtual Internet Payment System. Your sole remedy is to end this agreement and cancel your account as a Seller and never use the First Virtual Internet Payment System again. First Virtual will treat you fairly, but we both know that reasonable people can differ as to what is fair, so First Virtual fully expects that some Sellers will cancel their Seller accounts. First Virtual regrets this, but it will happen.

Q11. What if I have a dispute with First Virtual?

ANSWER: If you have any kind of dispute with First Virtual over anything, First Virtual would ask you to e-mail us about your dispute at "humanhelp@fv.com" before you do anything. First Virtual wants to treat you fairly and will do everything it can to resolve disputes reasonably. But, if First Virtual and the Seller cannot resolve a dispute and the Seller decides to file a lawsuit, then the Seller must sue First Virtual in the appropriate court in Cheyenne, Wyoming.

Q12. How do we end our agreement?

ANSWER: First, you can stop using the First Virtual Payment System. Next, either First Virtual or the Seller can notify the other that this agreement has ended.

Q12.1. Can First Virtual end this agreement with me for any reason, or for no reason?

ANSWER: Yes, and without any prior notice to you. First Virtual may tell you not to use the First Virtual Internet Payment System again.

Q12.2. Can I end this agreement with First Virtual for any reason, or for no reason?

ANSWER: Yes, at any time you choose by notice to First Virtual.

Q12.3. What obligations do we have to each other if we end this agreement?

ANSWER: Well, when this agreement ends, First Virtual may estimate the total amount of Chargebacks and any other obligations or liabilities you may have to First Virtual and deduct this amount from your Seller's account and any Net Sales Amount due you. First Virtual may hold this amount for no more than ten months and deduct any Chargebacks or other obligations or liabilities you may have to First Virtual. After no more than ten months, First Virtual will deposit the balance into your bank account. Remember that if you change e-mail addresses during this ten month period, you must follow the procedures in Q&A#2.3 and inform First Virtual of the address change. If you change bank accounts during this ten month period, you must inform First Virtual.

Q13. Can First Virtual change these Seller TACs?

ANSWER: Yes, First Virtual can change these Seller TACs whenever it wants. First Virtual has no intention of changing these Seller TACs often, but First Virtual will change these Seller TACs whenever applicable law requires a change, or the credit card companies change their operating procedures, or whenever First Virtual introduces new protocols or other structural changes that require these Seller TACs to change.

Q14. What if there are inconsistencies between these Seller TACs, any FAQ, or anything else published by First Virtual?

ANSWER: The first rule of interpretation is that these Seller TACs govern our agreement. The FAQs are nothing more than explanations to help you use the First Virtual Internet Payment System and they may change. Thus, we should not rely on them. The second rule of interpretation is that we agree to treat the "Seller FAQs" differently. The FAQs affect our agreement and how we act towards each other and the Buyer(s) as long as they are consistent with these Seller TACs. If they are inconsistent with these Seller TACs, these Seller TACs govern our agreement. If you are a Seller using First Virtual's InfoHaus and there is an inconsistency between these Seller TACs and the InfoHaus TACs, it will depend on the situation: if any matter involves the First Virtual Internet Payment System, these Seller TACs govern; if the matter involves what a Seller can or can't do with InfoHaus, then the InfoHaus TACs govern.

Q14.1. What if a court decides that some part of this agreement is invalid, does that invalidate this whole agreement?

ANSWER: No. We agree that if a court tells us that a part of our agreement is invalid and thus not binding on us, we agree that the rest of our agreement is still valid and should be interpreted as we have agreed in Q&A#14 through Q&A#14.2.

Q14.2. I've never seen an agreement like this before, how is it to be interpreted?

ANSWER: Well, first remember that our agreement is being drafted this way because First Virtual thinks it will make it easier for Sellers to understand their obligations to First Virtual and to Buyers. We agree that each question and answer is to be read together. In other words, you don't take the words from just one question and say "that's our agreement." Instead, you read all the questions and the answers together when you try to determine what we have agreed. Finally, neither of us is perfect, so if we've left something out, or if something is not clear, then we agree that any court or person trying to interpret this agreement should apply it so that first, it protects Buyers, and second, it limits First Virtual's liability to a Seller or Sellers to (i) making reasonable efforts to correct data lost, corrupted or damaged, and, (ii) refunding Transaction and Settlement Fees. We both realize that this is a significant limitation on your right to sue and recover money from First Virtual, but frankly it is the cost of doing business as a Seller using the First Virtual Internet Payment System.

(Reprinted with permission from First Virtual Holdings Incorporated, 1996)

INFOHAUS TERMS AND CONDITIONS

Agreement on the use of the First Virtual InfoHaus Effective December 16, 1995

The following questions and answers are called the First Virtual InfoHaus Terms and Conditions ("InfoHaus TACs"). These InfoHaus TACs are the only agreement between First Virtual Holdings Incorporated and you, the InfoHaus Merchant, regarding your use of

First Virtual's InfoHaus. When you open a First Virtual InfoHaus Merchant storefront as provided in Q&A#3, we both agree to act according to these InfoHaus TACs. We also agree that each numbered question and answer are to be read and applied together as the expression of one complete idea or "term" as it is called in the law. All the questions and answers are to be interpreted in a consistent manner as agreed in Q&A#12.2.

Q1. What is the InfoHaus?

ANSWER: The InfoHaus is a computer server connected to the Internet. First Virtual provides space on the InfoHaus computer for First Virtual Sellers to sell information to First Virtual Buyers. First Virtual Sellers are defined in the First Virtual Seller Terms and Conditions (Seller TACs), which we agree are a part of this agreement. First Virtual Buyers are defined in the First Virtual Buyer Terms and Conditions (Buyer TACs), which we agree are a part of this agreement. "InfoHaus" is a registered trademark of First Virtual Holdings Incorporated, a Wyoming corporation with its business office at 11975 El Camino Real, Suite 300, San Diego, CA 92130 and its Wyoming address at 1720 Carey Ave. or PO Box 1436, Cheyenne, Wyoming 82003-1436. Hereafter, we will call First Virtual Holdings Incorporated "First Virtual," or "FV."

Q1.1. How can I contact First Virtual?

ANSWER: If you want more information about First Virtual, send e-mail to "info@fv.com". This will give you general information on First Virtual and also tell you how to get FAQs (Frequently Asked Questions) on selected topics such as the First Virtual InfoHaus. For questions that are not answered by the First Virtual or InfoHaus FAQs, e-mail your question to "humanhelp@fv.com". Please remember that FAQs and e-mail from "humanhelp" are not a part of our agreement.

Q1.2. How will I know when these First Virtual Seller TACs change?

ANSWER: First Virtual will e-mail you a message telling you when a change is made to this agreement as it is published if you send e- mail to "fineprint-changes-request@fv.com" and subscribe to the fineprint-changes mailing list in accordance with our instructions, after you sign up as an InfoHaus Merchant.

Q2. Who am I?

ANSWER: You are not a minor (younger than age 18) and you are both a First Virtual Seller and a First Virtual Buyer who is applying to be an InfoHaus Merchant. If you complete the application process according to Q&A#3, you are applying to become an InfoHaus Merchant and you are agreeing to the terms of this Agreement. Hereafter, we will call you "I," "me," "you," or "InfoHaus Merchant."

Q2.1. What does it mean to be "an InfoHaus Merchant"?

ANSWER: It means that you completed the application process according to Q&A#3, First Virtual accepted your application, and you opened your InfoHaus site. This also means that you agree to follow the agreement as reflected in these InfoHaus TACs.

Q2.2. How does First Virtual contact me?

ANSWER: First Virtual contacts you through the e-mail address that you provide First Virtual during the First Virtual Seller application process. You agree that First Virtual sends all notices to this e-mail address. First Virtual may get other addresses from you, such as postal addresses, but they are not used for purposes of providing any notice under this agreement.

Q2.3. What if my e-mail address changes or I no longer have an e-mail address?

ANSWER: If your e-mail address changes, you must inform First Virtual by e-mail from your old e-mail address. In other words, don't inform First Virtual from your new e-mail address that the old e-mail address is no longer valid. First Virtual does not consider this a valid e-mail address change. During the period you do not have an e-mail address, you cannot be an InfoHaus Merchant.

Q3. How do I open an InfoHaus Merchant's Site or Storefront?

ANSWER: You open an InfoHaus Merchant's site by applying through an application procedure offered by First Virtual. To apply, you will provide First Virtual with the information required in the InfoHaus Merchant application form. By applying, you agree to follow these

InfoHaus Merchant TACs. For more information, First Virtual provides a "Signing Up" FAQ, which may change from time to time and thus is not part of these InfoHaus TACs. Send an e-mail message to "signup@fv.com" if you want this FAQ.

Q4. What can I sell on the InfoHaus?

ANSWER: Information.

Q4.1. What is "information"?

ANSWER: "Information," for purposes of this agreement, is being used in very broad sense to mean anything that can be stored on a computer and transferred to someone else's computer so they can read it, view it, listen to it, use it, or print it.

Q4.1.1. Can First Virtual give me an example?

ANSWER: Yes, but only as an example, information would include: articles, books, stories, poems, academic research, compiled data, and anything else that can be expressed in words or numbers; pictures, photos, drawings, maps, plans, blueprints, and anything else that can be put into a two-dimensional graphic image; video and audio clips, music, TV programming, sound recordings, animation, news footage, and anything else that can be recorded on magnetic media; computer software, GIF and other graphics files, and anything else that can be enclosed in a binary file. The information products you can sell using the InfoHaus is limited only by your imagination. The key distinction is not the substance or content, but the form in which it is kept and transmitted.

Q4.2. Can I sell goods or services?

ANSWER: No. You agree to sell only information on the InfoHaus.

Q4.2.1. What if I customize software, thus adding value to information by providing a service?

ANSWER: Remember the distinction pointed out in Q&A#4.1.1. Customizing software and pricing it so that the price reflects the added value does not breach this agreement as long as the information sold is information which can be transmitted from one computer to another

and the parties can use the First Virtual Internet Payment System to make the sale. Most compilations of information such as dictionaries, lists and such have added value as a result of the effort of the compilers or information gatherers. If you can find ways to add value to information and place it in your InfoHaus storefront and a Buyer agrees to buy it, with both of you using the First Virtual Internet Payment System, you can sell it.

Q.5. What fees do I pay First Virtual for selling information on the InfoHaus?

ANSWER: There are two fees that an InfoHaus Merchant pays First Virtual for operating an InfoHaus storefront. These two fees are in addition to the transaction fees agreed to in the First Virtual Seller TACs: * The first is a nominal storage fee of US $1.50 per month per megabyte of storage space you use with a minimum of $1.50 per month. * The second is a charge of 8% of the sale proceeds of each transaction we handle for you on the InfoHaus.

Q.5.1. How are these fees billed to me?

ANSWER: It is important to understand that your InfoHaus fees are billed to your Buyer's VirtualPIN. InfoHaus fees are NOT deducted from your sales revenue before it is deposited into your bank account.

Q.6. What other promises do I make as an InfoHaus Merchant?

ANSWER: Several. Excuse us for yelling, but we will put these additional promises into caps so you can't say later that your eyes glazed over and you didn't read them:

FIRST, YOU AGREE TO FOLLOW THESE InfoHaus TACs, OUR AGREEMENT.

SECOND, YOU AGREE TO FOLLOW THE PROCEDURES ESTABLISHED IN THE SELLER TACs AND BUYER TACs.

THIRD, YOU AGREE NOT TO SELL ANYTHING ILLEGAL OR USE ILLEGAL METHODS TO SELL, AND PROMISE THAT ANY SALE OR OFFER TO SELL WILL NOT VIOLATE ANY LAW, NOR WILL SUCH SALE OR OFFER TO SELL INFRINGE ANY PATENT, TRADEMARK OR COPYRIGHT OWNED BY OTHERS.

FOURTH, YOU AGREE TO KEEP A RECORD OF ALL SALES DATA FOR FIVE (5) YEARS FROM THE DATE OF ANY SALE AND AGREE TO PROVIDE FIRST VIRTUAL COPIES OF THE DATA WHEN REQUESTED.

FIFTH, YOU AGREE NOT TO COPY, DISTRIBUTE, RENT, LEASE OR SUBLICENSE ALL OR ANY PORTION OF ANY SOFTWARE CODE PROVIDED YOU BY FIRST VIRTUAL SO THAT YOU CAN USE THE FIRST VIRTUAL INTERNET PAYMENT SYSTEM. YOU ALSO AGREE NOT TO MODIFY OR PREPARE DERIVATIVE WORKS OF THIS SOFTWARE CODE. YOU ALSO AGREE NOT TO REVERSE ENGINEER, DECOMPILE OR DISASSEMBLE ANY OF THIS SOFTWARE CODE.

SIXTH, YOU AGREE THAT IF YOU USE THE MARKS "INFOHAUS" OR "FIRST VIRTUAL INTERNET PAYMENT SYSTEM" OR "FIRST VIRTUAL" ANYWHERE, THAT YOU WILL PLACE THE SYMBOL "TM" NEXT TO IT AND INDICATE IN AT LEAST 8PT TYPE THAT THESE MARKS ARE A REGISTERED TRADEMARK OF FIRST VIRTUAL HOLDINGS INCORPORATED, AND ALL RIGHTS TO THESE MARKS ARE OWNED BY FIRST VIRTUAL HOLDINGS INCORPORATED.

FINALLY, YOU AGREE TO TAKE FULL RESPONSIBILITY FOR ANY STATE OR OTHER SALES OR USE OR OTHER TRANSACTION TAX OR SIMILAR CHARGE IMPOSED ON YOUR SALE OR OFFER FOR SALE OF ANYTHING USING THE INFOHAUS AND YOU AGREE THAT FIRST VIRTUAL WILL NOT BE EXPECTED TO FILE ANY TAX RETURNS OR PAY ANY TAX ON YOUR BEHALF.

Q6.1. What if I can't agree with all these InfoHaus Merchant TACs and "humanhelp" tells me that my concerns are valid; or, I send an e-mail message to First Virtual saying the I don't agree with certain Q&As, but will still become a Seller? Does that mean this agreement has changed?

ANSWER: No (actually, h___ no!). When you become an InfoHaus Merchant, you are agreeing that these InfoHaus TACs are our agreement. Only First Virtual can change our agreement. Your only choice is to not become an InfoHaus Merchant. If First Virtual changes these InfoHaus Merchant TACs and you don't agree to the change, you can

stop selling anything as an InfoHaus Merchant and thus end this agreement (see Q&A#1.2 as to how you can receive notices of any changes to this agreement).

Q6.2. What is the relationship between these InfoHaus TACs and the Seller TACs and the Buyer TACs?

ANSWER: The "Seller TACs" are your agreement with First Virtual that governs your status as a First Virtual Seller using the First Virtual Internet Payment System. The "Buyer TACs" are your agreement with First Virtual that governs your status as a First Virtual Buyer using the First Virtual Internet Payment System. For purposes of this agreement, these InfoHaus TACs and the Buyer TACs govern how you, the InfoHaus Merchant pay for your storefront on the InfoHaus computer.

Q7. What risks do I assume as an InfoHaus Merchant?

ANSWER: Other than the risks you have already agreed to assume as outlined in the Seller TACs and the Buyer TACs, you are assuming the risk that a disaster of any kind (political, labor, natural) or an act of God may occur that stops you from using the InfoHaus to sell information.

Q7.1. What does First Virtual mean by disaster or act of God?

ANSWER: Well, you need to be a little paranoid to understand what we are agreeing to here. There is the possibility that something can happen that First Virtual has no control over. It could be an earthquake, a flood, a breakdown of all electrical or communications facilities or an invasion from Mars. If something, anything, like this happens and the InfoHaus cannot operate, you can't sell.

Q7.2. If the InfoHaus is not operating, do I have to pay the InfoHaus fees?

ANSWER: Yes; First Virtual will use reasonable efforts to have the InfoHaus operational at all times.

Q7.2.1. What if I lose money, or spend money I didn't plan on spending, or lose the opportunity to make or save money because of the fault

of First Virtual's people or because of a malfunction of First Virtual's software or machines as relates to the InfoHaus?

ANSWER: You cannot recover the amount of any loss or other damages you, the Seller, incur even if you prove that the loss occurred because of the fault of First Virtual's people or because of a malfunction of First Virtual's software or machines.

Q7.2.2. What if I lose information and cannot recover it?

ANSWER: Don't be so stupid as to place your only copy of the information on the InfoHaus computer! YOU AGREE TO KEEP ADDITIONAL COPIES OF ALL INFORMATION YOU UPLOAD TO THE InfoHaus!!!! No matter what happens or who is at fault, First Virtual will not reimburse you for the loss of such information. First Virtual will make reasonable efforts to retrieve and correct the information, but the only sure remedy is for you to keep a separate copy of the information.

Q7.2.3. Can I sue someone else, like the First Virtual person who caused the problem, or a First Virtual supervisor, or anyone else who First Virtual contracts or works with to provide the InfoHaus?

ANSWER: No.

Q7.2.4. Why not?

ANSWER: For several reasons: First, First Virtual is a corporation and thus legally you can only sue First Virtual and not its employees, consultants, officers, directors and shareholders. By becoming an InfoHaus Merchant, you agree to follow this legal principle by not suing First Virtual's employees, consultants, officers, directors and shareholders, no matter the reason. Next, First Virtual and others are spending much time and money to make the InfoHaus work. We do not want to be sued for every mistake, be it negligent or willful, which we and others who work with us make. First Virtual will treat you fairly. The bottom line is that when you become an InfoHaus Merchant you agree to give up your rights to sue us and others associated with First Virtual, whoever they may be. So don't become an InfoHaus Merchant if you can't agree to this limitation on the liability of First Virtual and the people and other companies that contract or work with First Virtual in providing the InfoHaus.

Q8. What promises is First Virtual making to me in return for my agreeing to become an InfoHaus Merchant?

ANSWER: First Virtual agrees to follow these InfoHaus TACs. First Virtual is agreeing to nothing else. In fact, First Virtual DISCLAIMS ALL WARRANTIES WITH RESPECT TO THE SERVICES AND PRODUCTS PROVIDED UNDER THESE InfoHaus TACs. THIS IS OUR ONLY AGREEMENT. FIRST VIRTUAL IS NOT MAKING ANY IMPLIED OR LEGALLY REQUIRED PROMISE OR WARRANTY TO YOU, THE FIRST VIRTUAL SELLER, SUCH AS THE WARRANTY OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE.

Q8.1. Why is First Virtual yelling at me (putting the words in caps)?

ANSWER: The law of Wyoming, which governs this agreement, requires that we put in capital letters our disclaimers of certain warranties that are usually implied by the law. Sorry, but this is the first time you probably read them and the law requires that we yell.

Q9. What if I have a dispute with First Virtual?

ANSWER: If you have any kind of dispute with First Virtual over anything, First Virtual would ask you to e-mail us about your dispute at "humanhelp@fv.com" before you do anything. First Virtual wants to treat you fairly and will do everything it can to resolve disputes reasonably. But, if First Virtual and an InfoHaus Merchant cannot resolve a dispute, and the InfoHaus Merchant decides to file a lawsuit, then the InfoHaus Merchant must sue First Virtual in the appropriate court in Cheyenne, Wyoming.

Q10. How do we end this agreement?

ANSWER: You can stop using the InfoHaus by removing all information from your storefront and notifying First Virtual by e- mail that you are ending this agreement.

Q10.1. Can First Virtual end this agreement with me for any reason, or for no reason?

ANSWER: Yes, at any time by notice to you.

Q10.2. Can I end this agreement with First Virtual for any reason, or for no reason?

ANSWER: Yes, at any time you choose by notice to First Virtual.

Q10.3. What obligations do we have to each other if we end this agreement?

ANSWER: Well, when this agreement ends, First Virtual will calculate the total amount you owe for using the InfoHaus and charge your credit card in accordance with the Buyer's TACs. If you leave any information on the InfoHaus computer after this agreement is ended, you take the risk that it will be deleted and thus lost.

Q11. Can First Virtual change these InfoHaus TACs?

ANSWER: Yes, First Virtual can change these InfoHaus TACs whenever it wants. First Virtual has no intention of changing these InfoHaus TACs often, but as you know First Virtual will change the InfoHaus TACs whenever applicable law requires a change, or whenever First Virtual introduces new protocols or other structural changes that require the InfoHaus TACs to change.

Q12. What if there are inconsistencies between these InfoHaus TACs, Seller TACs, Buyer TACs or any FAQ or anything else published by First Virtual?

ANSWER: The first rule of interpretation is that these InfoHaus TACs govern our agreement as to your use of the InfoHaus as an InfoHaus Merchant. The Seller TACs govern our agreement as to your use of the First Virtual Internet Payment System as a Seller, and the Buyer TACs govern our agreement as to your use of the First Virtual Internet Payment System as a Buyer. The FAQs are nothing more than explanations to help you use the First Virtual Internet Payment System or the InfoHaus and they change often. Thus, we should not rely on them.

Q12.1. What if a court decides that some part of this agreement is invalid, does that invalidate this whole agreement?

ANSWER: No. We agree that if a court tells us that a part of our agreement is invalid and thus not binding on us, we agree that the rest

of our agreement is still valid and should be interpreted as we have agreed in Q&A#12.

Q12.2. I've never seen an agreement like this before, how is it to be interpreted?

ANSWER: Well, first remember that our agreement is being drafted this way because First Virtual thinks it will make it easier for InfoHaus Merchants to understand their obligations to First Virtual about the use of the InfoHaus. We agree that each question and answer is to be read together. In other words, you don't take the words from a question and say "that's our agreement." Instead you read all the questions and the answers together when you try to determine what we have agreed. Finally, neither of us is perfect, so if we've left something out, or if something not clear, then we agree that any court or person trying to interpret this agreement should apply it so that first, it protects Buyers, and second it limits First Virtual's liability to InfoHaus Merchants so that there is no liability to the InfoHaus Merchant no matter what happens. We both realize that this is a significant limitation on your right to sue and recover money from First Virtual, but frankly it is the cost of doing business as an InfoHaus Merchant using the InfoHaus.

(Reprinted with permission from First Virtual Holdings Incorporated, 1996)

APPENDIX D

GUIDE TO THE CD-ROM

First Virtual offers a considerable body of documentation, scripts, templates, and code in support of their payment system. The companion CD-ROM contains many of these items. While the files included on the CD-ROM are up-to-date versions as of early 1996, the interested reader is strongly urged to check the First Virtual Web site for changes, additions, and updates.

INSTALLING THE CD-ROM

The companion CD-ROM should not require any special installation, as long as you are able to access the files on it through your own PC. The best way to view the included files is through the "First Virtual Companion CD-ROM Index" using your favorite Web browser.

Accessing the CD-ROM Index

Included on the CD-ROM are HTML-tagged documents that you can use to more easily access resources. You can use your favorite Web browser to view these pages. If you are using the Netscape Navigator, use the command "Open File" from the File pulldown menu; for Microsoft Explorer users, use the "Open" command from the File pulldown menu and choose "Open file" from the resulting dialog box.

The file to open is called "INDEX.HTM" and is in the root of the companion CD-ROM. So, if your CD-ROM is accessed through drive "D:" you would enter the following to open the file:

```
D:\index.htm
```

From there you will be able to connect directly to a list of pointers to electronic commerce firms as well as to the home pages for First Virtual, and the author and publisher of this book.

You can also access the various First Virtual distribution files through the main index. Copies of First Virtual documents as well as text-only files can be viewed directly through your Web browser. Included files include tape archive format (tar file) versions of some of the tools provided by First Virtual.

SUPPORT FOR SOFTWARE ON THE CD-ROM

First Virtual provides the various software tools, templates, and utilities "as is." In general, the following disclaimer should be considered to apply to software and tools that First Virtual freely provide to users:

FIRST VIRTUAL MAKES NO REPRESENTATIONS ABOUT THE ACCURACY OR SUITABILITY OF THIS MATERIAL FOR ANY PURPOSE. IT IS PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES.

In general, users should not assume that First Virtual will be able to offer any kind of support or help using these tools (although it is possible that they may be able to answer some questions, it should not be counted on).

Likewise, this material is reproduced in this book and CD-ROM as a service to readers. Neither the author nor the publisher can be counted upon for help in installing, using, or modifying any of these tools. Users should be familiar with the systems and tools described as prerequisites in Part 4 before attempting to use these tools.

CD-ROM CONTENTS

Each of the following sections refers to the contents of five different directories on the companion CD-ROM.

Structure of the CD-ROM

The CD-ROM includes some HTML files in the root directory, to be read with a Web browser. These include:

```
ECLINKS.HTM
INDEX.HTM
```

The five sub-directories are listed in Table D-1.

TABLE D-1 *Subdirectories on the companion CD-ROM.*

Directory	Contents
\SPECS	First Virtual specifications
\INFOHAUS	InfoHaus templates
\WWW-CGI	HTML and CGI scripts/templates
\FVAPI	First Virtual API software
\FTPD	Software for First Virtual-enabling an ftp server

First Virtual Specification Documents

First Virtual specification documents are stored in the directory on the CD-ROM called:

```
\SPECS
```

Included here are the Green Commerce model, the Application/Green Commerce MIME Content Type, the Simple Mail Exchange Protocol (SMXP), the InfoHaus technical specification, and the First Virtual API technical specification. The relevant file names are shown in Table D-2.

TABLE D-2 *First Virtual specification file names.*

Name	Contents
green.txt	Green Commerce model document
agc.txt	Application/Green Commerce MIME Content Type specification
smxp.txt	Simple Mail Exchange Protocol specification
infohaus.txt	InfoHaus technical specification document
fvapi.txt	First Virtual API specification

InfoHaus Templates

Two templates for use with the InfoHaus, EMAILFORM.HTML and EMAILPAYFORM.HTML, are included in the directory:

```
\INFOHAUS
```

These templates are stored in files with DOS format filenames, as shown in Table D-3.

TABLE D-3 *InfoHaus HTML templates.*

Name	Contents
mailform.htm	The EMAILFORM.HTML template described in Chapter 9
epayform.htm	The EMAILPAYFORM.HTML template described in Chapter 9

HTML Templates and CGI Scripts

HTML and CGI templates and scripts described in Chapter 9 include the Member and Websale packages. These files are available in the directory \WWW-CGI and its subdirectories:

```
\WWW-CGI\MEMBER
\WWW-CGI\WEBSALE
```

Member and Websale are included both as archived files (these require a program like WinZip on Windows or tar on Unix to decompress) and in uncompressed form in their respective subdirectories.

The First Virtual API

The First Virtual API is stored in the directory:

```
\FV-API
```

It is available both as an archived file and in uncompressed form in this directory. The archived file name is:

```
fv-api.tar
```

First Virtual Enabling Your ftp Server

Software for enabling your Unix ftp server to accept First Virtual payments is also included in the CD-ROM in the directory:

```
\FTPD
```

This software was not described in the text of this book. Using it requires relatively sophisticated programming skills; instructions and supporting files are included in the distribution file, called:

```
WUfvftpd.tar
```

ELECTRONIC COMMERCE LINKS

An Electronic Commerce links page is also included, pointing to the Web sites in Appendix B.

INDEX

A

acceptable use policies 20
account
  information 153
account application 103
  confirmation 187
account creation process 102
account ID 179
account identifiers 26, 93, 108
  First Virtual 29
account maintenance 190
account requirements 103, 130
account status 190
acquirer 68, 84, 85, 287
addition-request transaction 236
address-redistribution 156
agent 287
America Online 10
anonymous ftp 287
API 287
application 287
application form 102, 162, 174
application layer 41, 288
application-request 115
application-result 115
application/green-commerce 108
application/green-commerce MIME
  content-type 106, 111, 117
application/x-fv-email-pay-form 264
apply@card.com 174
ASCII 15, 288
asymmetric cryptography 288
asymmetric functions 56
asymmetric key 79
ATM card 96
audit trail 8
AUP 288
authentication 25
authorizations 70
automated telephone system 103
automation 125
autosell URL 271

B

backbone 288
bandwidth 288
bill-to-ID 226
bit 288
blinding 88
Borland International, Inc. 280
boundary parameter 236
boxset 240

bridge 288
Brief-Description 227
browsers 17
  secure 71
brute-force 80
brute-force attacks 51, 120
buyer's account 126
buyer's terms and conditions 129
buying
  by e-mail 209
  by ftp 208
byte 289

C

capabilities-request 115
card not present transactions 120, 289
cardholders 109
  account application 115
  numbers 108
  status 112
cardnumber 110
  inquiries 114
certification authorities 59
CGI 15, 249, 284, 289
  scripts 249, 253, 261
chargebacks 115, 127
check-in
  InfoHaus products 233
checkat 260
Checkfree Corporation 86
chgacct-query 116
chgacct-request 116
chgacct-result 116
ciphers 50
ciphertext 55
CIX 289
cleartext 289
client 289
code 50
cold fusion 280
commerce 6
  by e-mail 21
  Internet 22
commercial transaction 57
Common Gateway Interface 15
Communications Decency Act 245
CompuServe 10, 86
content 245
content-type
  multipart/FV-infohaus 236
contract-ID 227
cost of the goods sold 33
counterfeiting
  digital currency 90
cracker 290
credit card
  card numbers 71
  entering account number 187
  issuers 23
  sales 21
cryptanalysis 290
cryptography 46, 47, 290
customer support 132
CyberCash 71, 84
  digital wallet 27

D

daemon 290
data link layer 290
datagram 290
DBA name 219
decryption 290
DELIVERY-STATUS 256
Delphi 280
DES 290
DHCP 290
dial-up connection 44
digest function 61
DigiCash 71, 87
digital cash 69
digital check cashing 24
digital coins 87
digital commerce 5, 24
digital currency 24, 87
digital envelope 68, 71, 84
digital signatures 25, 37, 57, 61, 70, 87, 120, 291
digital wallet 68, 85

digitally signed confirmations 34
direct deposit 134
DNS 291
doing business as name 219

E

e-mail 291
  account application 174
  account setup 152
  address changes 274
  confirmation 182
  forgery 43
  protocols 43
  setting up InfoHaus storefront with 226
  to InfoHaus merchants 275
  to VirtualPIN holders 275
  transaction negotiations 20
  uploading products to InfoHaus by 233
  verification of VirtualPINs 260
EBCDIC 291
ecash 71, 87
EDI 291
EFT 9, 291
electronic commerce 5
electronic funds transfer 9
emailform.html 261
emailpayform 263
emissary 17
enabling accounts 135
encapsulation 291
encrypted channels 85
encrypted communication channel 84
encryption 37, 49, 56, 60, 67, 74, 93, 292
  consumer/merchant channel 67
  defeat 29
encryption technologies 28
Ethernet 292
Express Merchant 95, 188
  status 127
external channel 90, 91
failure notification messages 113
FAQ 292
FDDI 292
file server 292
file transfer protocol (ftp) 11, 41, 79, 292
  uploading products to InfoHaus by 232
  software 10
file transfer protocol servers
  First Virtual-enabled 209
file types
  InfoHaus products 235
findappl@card.com 190
fineprint 171, 181
  documents 164
finger 258, 267, 292
firewalls 38, 44, 73
  gateway 292
First USA Bank 189
First Virtual
  account activation 157
  account creation process 102
  account identifier 18
  account maintenance 190
  account requirements 103, 130
  account setup 152
  accounts 31
  birth of 100
  buyer's account 126
  changing account information 191
  confirming account for sales 187
  customer support 132
  e-mail addresses 141
  e-mail application 174
  enabling account 181
  enabling Internet servers 244
  Express Merchant status 188
  fees 27, 32
  ftp server 143
  holdback period 95, 136
  holding period 158
  key management 121
  list of merchants 279
  mailing list 144
  making a purchase with 194
  model of commerce 101
  organization 124
  payment system 92

payment system basis 108
procedures 101
product delivery 206
products and services 126
programs and templates 250
protocols 5, 95, 105
security 94
security measures 198
seller's account 126
selling 105
telephone confirmation 186
telnet application 164
telnet server 143
terms and conditions 127
test payment server 282
transaction 195
Web application 159
Web site 140, 251
First Virtual API 257, 269
getting and installing 271
First Virtual Application Programming Interface 253
forgery 43
formsell URL 272
fraud 20, 23, 94
Frequently Asked Questions list 252
funds transfer 257
FV API 253
FV-Users List 145
FVid 263

G
Gabriel, Peter 100
gateways 293
firewall 44
gigabit 293
gigabyte 293
goods-sale 207
Gopher 12, 293
Green Commerce
account maintenance 116
server 111
server capabilities 115
Green Commerce Model 106, 107, 293

H
hacker 293
handshake 293
hard goods 4, 34, 95, 207, 244
delivery 132
selling with First Virtual 119
hash function 57
HelpMeister 275
history-request 116
holdback period 95, 136
holding period 158
home page 294
host 294
HREF Tools Corporation 280
HTML 15, 138, 249, 284, 294
tags in InfoHaus storefronts 238
HTML forms 261
HTTP 14, 41, 77, 294
humanhelp 146
hypertext 79
Hypertext Markup Language 15, 138
Hypertext Transfer Protocol 14
Hypertext Transport Protocol 41, 77

I
IAB 294
IANA 294
ICMP 294
IESG 295
IETF 100
InfoHaus 103, 127, 137, 214, 295
charges 217
e-mail addresses 142
file types 235
forms 253
HelpMeister 275
information product preparation 228
keywords and topics 279
news list 194
periodicals 240
product check-in 234
product names 230
QuickBuy numbers 282
software license 245

terms and conditions 130
InfoHaus product
file extensions 277
InfoHaus storefront 218
creation 138
stocking 228
Information Society 101
initchg-request 116
initchg-result 116
Internet 9, 295
commercialization 18
layer 41
protocols 38, 40
router 44
security holes 43
security risks 42
server 246
service 248
transactions 95
Internet access providers 19
Internet commerce 5, 22, 77
companies 70
First Virtual's approach to 19
mechanisms 23
protocol 84
services 4
Internet Engineering Task Force 78, 100
Internet presence provider 244, 245
Internet servers 214
First Virtual-enabling 244
Internet Service Provider, the 10
internetworks 40, 295
InterNIC 295
interoperability 295
intruders 73, 75
IP 295
IP address 296
IPnG 296
IPv6 296
IPX 296
ISDN 296
ISOC 296
ISP 10

J
Java 16
joke of the day 100

K
Kerberos 296
key 55, 296
distribution 54
security 51
size 52
key certification 58
key distribution 56
key management 121
keywords 279

L
LAN 297
latency 297
liability 67
loss 33
Lynx 17

M
MAC 297
magazine 240
magic e-mail address 241
mail order 28
manusell URL 272
Mark Twain Bank 71, 87
MasterCard 71
MBONE 297
MEMBER 253, 265
message integrity 62
Microsoft 10, 73
MIME 106, 179, 297
MIME content-type 118
MIME enclosures 206
multicast 297
multihomed host 297
multimedia 15
multipart/FV-infohaus
MIME content-type 236
Multipurpose Internet Mail Extensions 106

N

Navigator 76
Netcruiser 17
Netscape 27, 71, 81, 84
  Commerce Server 78, 95
Netscape Navigator 17, 27, 29
NetWare 298
network 298
  integrity 44
network layer 41
newacct-request 115
newacct-result 115
newacct@card.com 180
newseller-request 233, 239
newsgroup 22
nextissue 242
nextvolume 242
NFS 298
NIC 298
NNTP 298
NOC 298
node 298
nonrepudiation 62, 298
NOS 299
notification message 181
notifications
  forged 120
Novell 10
NSF 299
nudity 245

O

octet 299
on-line payments 19
Open Market 27, 72
OS/2 Warp 17
out of band 299

P

packet 299
passwords 45, 75
pay-in method 109
pay-out method 109
payer anonymity 87
payin-chargeback-notification 115
payin-notification 199
payment authorization notifications
  digitally signed 19
payment information 84, 102
payout-chargeback-notification 115
PCT 299
PEM 299
periodical-paid-part-only 242
periodical-payment-optional 242
periodical-send-addition-results 242
periodical-subscription-price 242
periodical-volume 242
periodicals
  InfoHaus 240
PGP 120, 300
PIN 155, 156, 168, 179
ping 300
plaintext 55
plaintexts 49
PPP 44, 300
preferred-language 227
preparing infohaus products 228
pretty good privacy 120
private key 80, 300
private key encryption 55
process
  First Virtual purchase 35
Prodigy 10
product
  delivery 206
product registration message 236
protocol specifications 73
protocols 300
  Internet 38, 40
public key 56, 59, 79, 300
public key cryptography 37, 46, 56, 57, 60, 300
public key encryption 82
public key pairs 60
purchase
  credit card 8

Q

Quickbuy numbers 211, 278, 282

R

receipt 25
receipts 8
Regulation Z 137
reliability 41
retrieval@infohaus.com 211
RFC 300
ROT-13 77
router 44, 214, 301

S

S-HTTP 16, 77, 301
sales
  off Internet 257
sales commissions 26
scheme 79
search@infohaus.com 210
secret key 56, 301
secret key cryptography 301
secure channel 81, 84
secure Hypertext Transfer Protocol 16, 77
secure sockets layer 16, 77
security 23, 40
  through obscurity 66
security vulnerabilities 76
security-requirements 227, 256
  parameter 119
seller's account 126
seller-modification-request 239
sellers' terms and conditions 129
send-transfer-requests 227
sendmail 267
server 301
session key 80
SET 301
settlement queue 112
sexuality 245
SGCP 107, 118, 257, 302
shopping cart 247
Simple Green Commerce Protocol 106, 118, 257
Simple MIME eXchange Protocol 106, 118
SLIP 44, 302
SMTP 302
SMXP 106, 118, 302
sniffing 24
  network 34
SNMP 302
soft goods 4, 31
Spyglass Mosaic 17
SSL 16, 77, 302
StarNine Technologies, Inc. 281
Stefferud
  Einar 100
Stein
  Lee 100
storefront
  InfoHaus 218
STT 303
subscriptions 207
SunSoft 10
symmetric cryptography 51, 303
symmetric functions 55
symmetric key 80

T

tags 15
tar file 229
tax evasion 69
Tcl 265, 269, 303
TCP 118, 303
TCP/IP 9, 38, 78, 215, 232, 247, 303
telnet 11, 102
  account setup 153
  First Virtual application 164
  setting up InfoHaus storefront with 219
  verification of VirtualPINs 260
telnet.card.com 165
termination 132
terms
  negotiating 23

terms and conditions 103, 127, 164, 171, 181
test drives 33
test payment server 282
test.card.com 282
theft 23, 94
topics 279
traditional file transfer servers 14
transaction data
  authenticating 25
transaction fees 26
  First Virtual 30
transaction information
  transmission 70
transaction initiation 254
  by telnet 256
transaction security
  First Virtual approach 28
transactions 195
  authorizations 57
  charges 26
  fraudulent 29, 198
  Green Commerce model types 110
  notification 104
transfer inquiries 114
transfer query 199
transfer-ID 256
transfer-query 111
transfer-requests 111
  by e-mail 255
  off Internet 258
  subscription attributes 278
transfer-response 112
transfer-result 112, 199
  message 204
transfer-type 207, 256
transfers
  settlement 112
transport layer. 41
trial subscriptions 278
trust 8, 18

U

UDP 303
Uniform Resource Locator 15
URL 15, 303
  autoesell 271
  formsell 272
  manusell 272
Usenet 9, 22, 90

V

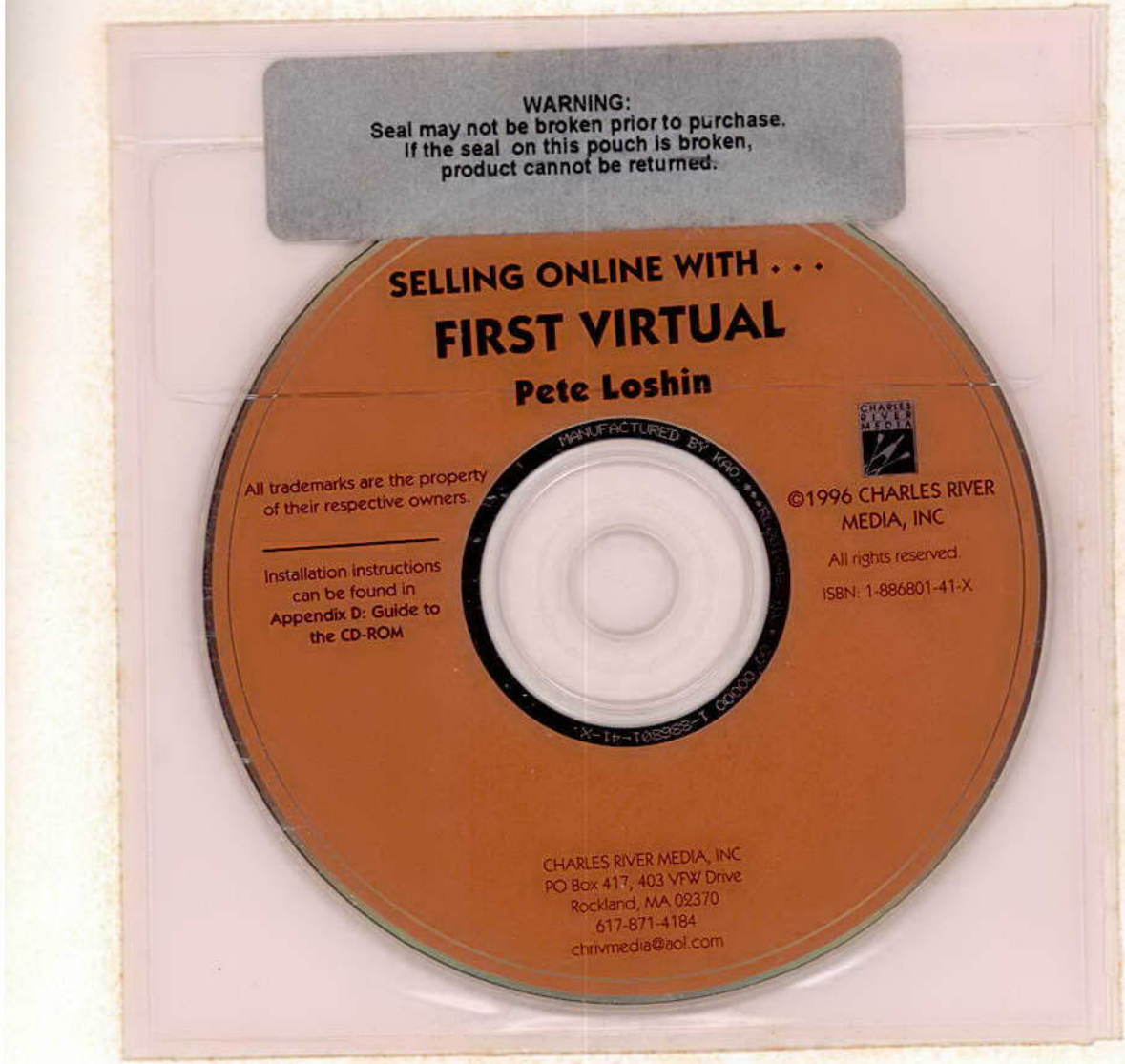
ViaCrypt 121
virtual organization 125
VirtualPIN 32, 104, 108, 135, 156, 188, 191, 194, 206, 227, 274, 303
  verifying buyer's 258
Visa 71
volume 240

W

waiver of holdback period 158
web of trust 59
Web pages
  commerce-enabling 249
  design 248
Web servers 248
  secure 71
Web storefront 8
Websale 253, 268
WebSTAR 281
World Wide Web (WWW) 9, 12, 18, 41, 303
  account setup 153
  browsers 14
  clients 16
  document development 14
  server software 17
  servers 15
  servers, secure 27
  sites 18

X

x-pgp-transfer-notification option 120


WARNING:
Seal may not be broken prior to purchase.
If the seal on this pouch is broken,
product cannot be returned.
SELLING ONLINE WITH . . .
FIRST VIRTUAL
Pete Loshin
All trademarks are the property of their respective owners.
Installation instructions can be found in Appendix D: Guide to the CD-ROM
©1996 CHARLES RIVER MEDIA, INC
All rights reserved.
ISBN: 1-886801-41-X
CHARLES RIVER MEDIA, INC
PO Box 417, 403 VFW Drive
Rockland, MA 02370
617-871-4184
chrivmedia@aol.com

Everything You'll Need To Transact Business On the World Wide Web!!!

SELLING ONLINE WITH... FIRST VIRTUAL

PETE LOSHIN

In the first book of an exciting new series, Pete Loshin provides step by step instructions for online buying and selling with one of the pioneers in the electronic commerce industry. First Virtual Holdings Inc. has quickly become one of the most popular vendors for doing business on the Internet. This is a hands-on, how-to guide, which includes everything from the electronic order forms to the electronic deposit.

FEATURES

- CD includes: HTML and CGI scripts and templates, InfoHaus templates, First Virtual specifications, software for First Virtual-enabling an ftp server, First Virtual API software, and electronic commerce links to other web sites;
- Includes everything needed to buy and sell over the Internet, as well as to maintain your account;
- Walks you through entire FV setup with step by step instructions and screenshots of what you'll see;
- Provides an overview of electronic commerce and the various issues and trends involving secure transfer of funds, protocols, encryption, etc.

FROM THE FOREWORD

"...It's a very practical, "how to" book, and by the time you're done reading it, you should be able to set up a whole new business in cyberspace starting with nothing but $10, an Internet connection, a good idea, and a willingness to work."

—Nathaniel Borenstein
Chief Scientist, First Virtual Holdings

ABOUT THE AUTHOR

Pete Loshin writes and consults about networking and the Internet. His articles have appeared in industry publications such as *PC Magazine*, *PC World*, *Communications Week*, and several others. He recently published *Electronic Commerce* (Charles River Media) and resides in Boston, MA.

SYSTEM REQUIREMENTS

IBM or compatible • CD drive • 38 .1 or higher • 4MB RAM • Web brows..

SHELVING

Internet, Networking, WWW, Gener..

401 0028182

DBS-BM
100000801658

CHARLES RIVER MEDIA, INC
PO Box 417 • Rockland, MA 02370 • http://www.algorithm.com/cm..
First Virtual logo used with permission
Cover design by Gary Ragaglia
Printed in the USA by InterCity Press, Rockland, MA

ISBN 1-886801-41-X
53295
9 781886 801417