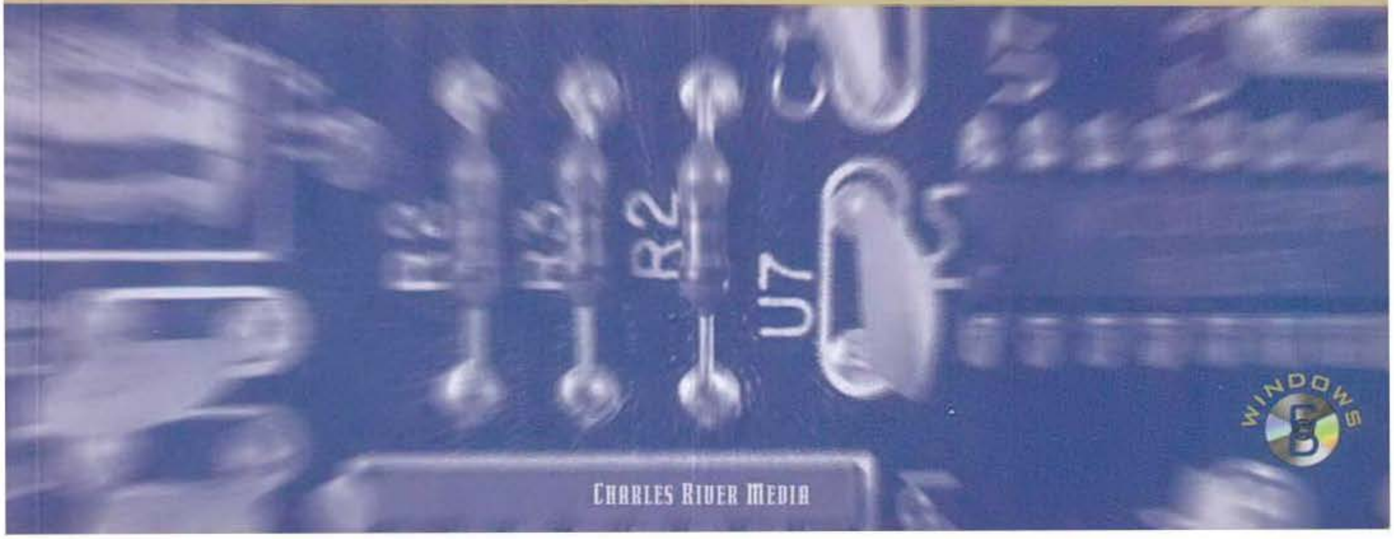
THE INTERNET MERCHANT MASTER SERIES

SELLING ONLINE WITH...

FIRST VIRTUAL

PETE LOSHIN

FOREWORD BY NATHANIEL BORENSTEIN



CHARLES RIVER MEDIA

WINDOWS

FIRST VIRTUAL

LOSHIN

CHARLES
RIVER
MEDIA

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

PETE LOSHIN

CHARLES RIVER MEDIA, INC.
ROCKLAND, MASSACHUSETTS

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

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

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

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 participation 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 transmits 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

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.

Contents

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 coworkers 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

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.

Contents

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 cryptographic 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 individuals 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

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.

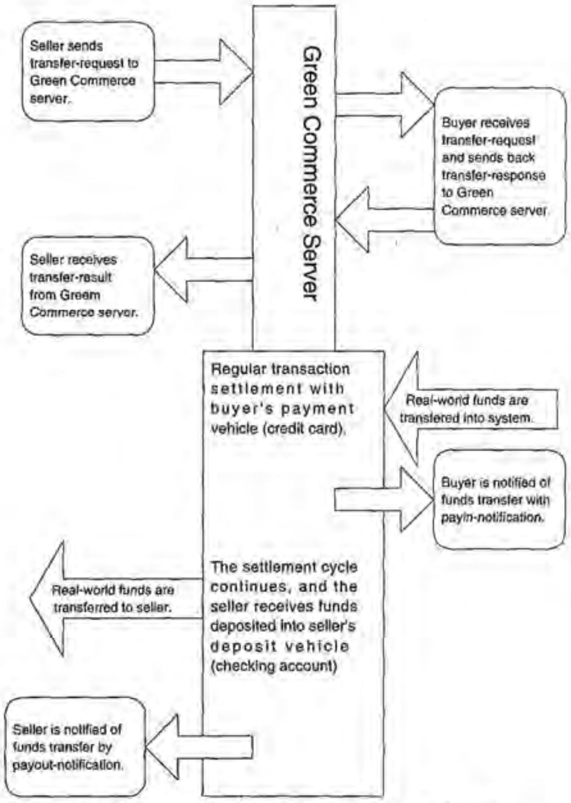

Seller sends transfer-request to Green Commerce server.
Green Commerce Server
Buyer receives transfer-request and sends back transfer-response to Green Commerce server.
Seller receives transfer-result from Greem Commerce server.
Regular transaction settlement with buyer's payment vehicle (credit card).
Real-world funds are transfered into system.
Buyer is notified of funds transfer with payin-notification.
The settlement cycle continues, and the seller receives funds deposited into seller's deposit vehicle (checking account)
Real-world funds are transferred to seller.
Seller is notified of funds transfer by payout-notification.

FIGURE 4-1 *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 cardnumber, 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 computers 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

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.

Contents

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

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).

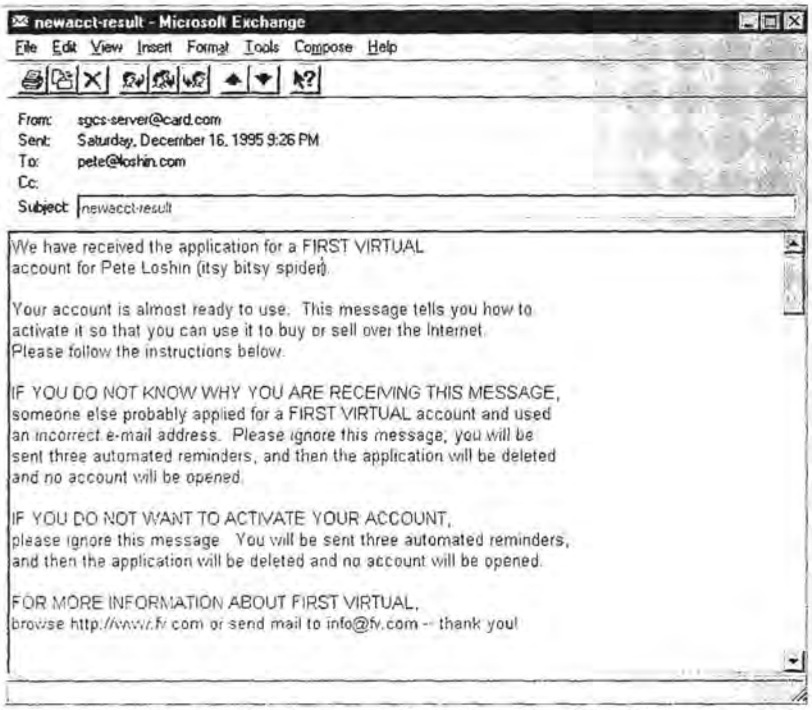
- **Address-Redistribution:**. On occasion, First Virtual customers may receive e-mail about products that seem to match the customer's interests, based on previous purchases. First Virtual does not sell customer records or e-mail addresses as mailing lists, but they may at some point do direct marketing 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


newacct-result - Microsoft Exchange
File Edit View Insert Format Tools Compose Help

From: sgcs-server@card.com
Sent: Saturday, December 16, 1995 9:26 PM
To: pete@loshin.com
Cc:
Subject: newacct-result

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 6-1 *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

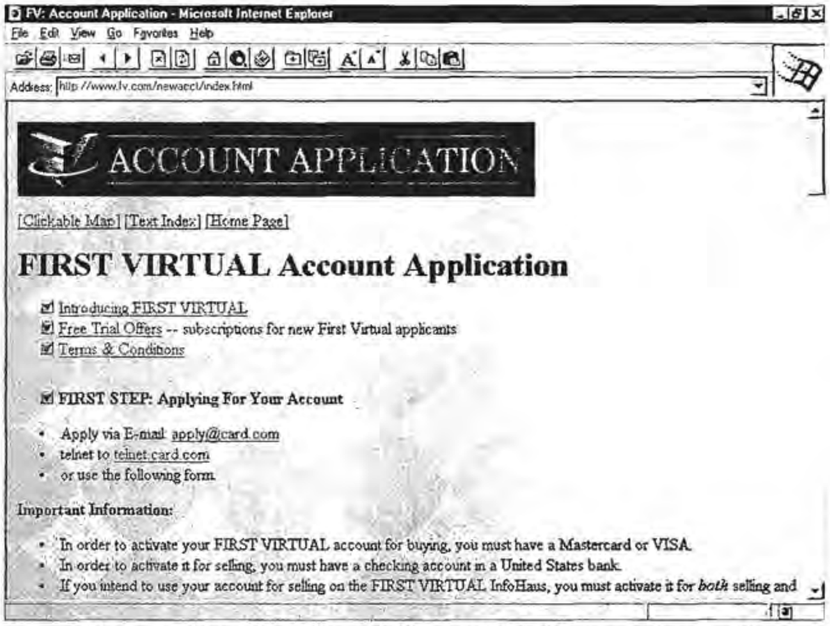
The First Virtual Web server address is:

```
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.


FV: Account Application - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address: http://www.fv.com/newacct/index.html

ACCOUNT APPLICATION

[Clickable Map] [Text Index] [Home Page]

FIRST VIRTUAL Account Application

☑ Introducing FIRST VIRTUAL
☑ Free Trial Offers -- subscriptions for new First Virtual applicants
☑ Terms & Conditions

☑ **FIRST STEP: Applying For Your Account**

- Apply via E-mail: apply@card.com
- telnet to telnet.card.com
- or use the following form.

Important Information:

- In order to activate your FIRST VIRTUAL account for buying, you must have a Mastercard or VISA.
- In order to activate it for selling, you must have a checking account in a United States bank.
- If you intend to use your account for selling on the FIRST VIRTUAL InfoHaus, you must activate it for *both* selling and

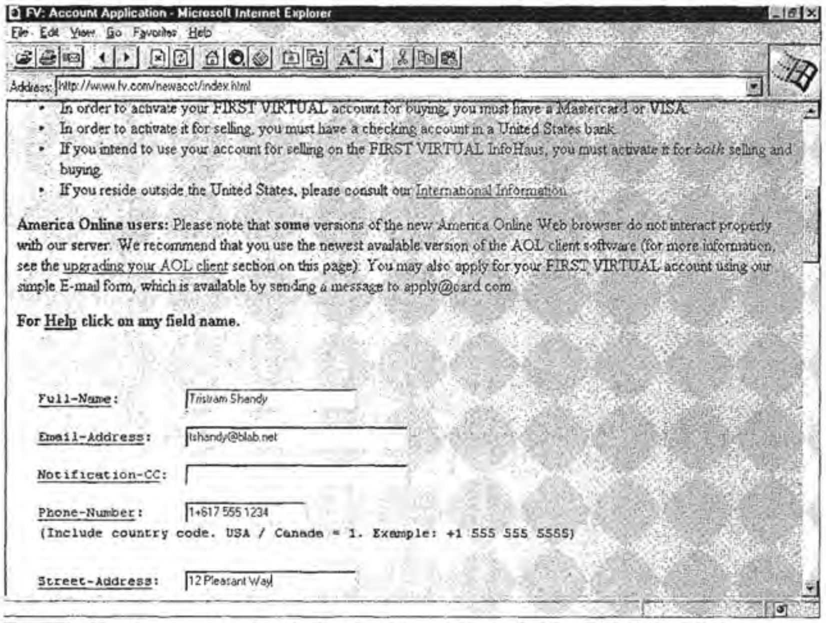
FIGURE 6-2 *The top of the First Virtual World Wide Web application form. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*

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.


FV: Account Application - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address: http://www.fv.com/newacct/index.html

- In order to activate your FIRST VIRTUAL account for buying, you must have a Mastercard or VISA.
- In order to activate it for selling, you must have a checking account in a United States bank.
- If you intend to use your account for selling on the FIRST VIRTUAL InfoHaus, you must activate it for *both* selling and buying.
- If you reside outside the United States, please consult our International Information.

America Online users: Please note that **some** versions of the new America Online Web browser do not interact properly with our server. We recommend that you use the newest available version of the AOL client software (for more information, see the upgrading your AOL client section on this page). You may also apply for your FIRST VIRTUAL account using our simple E-mail form, which is available by sending a message to apply@card.com.

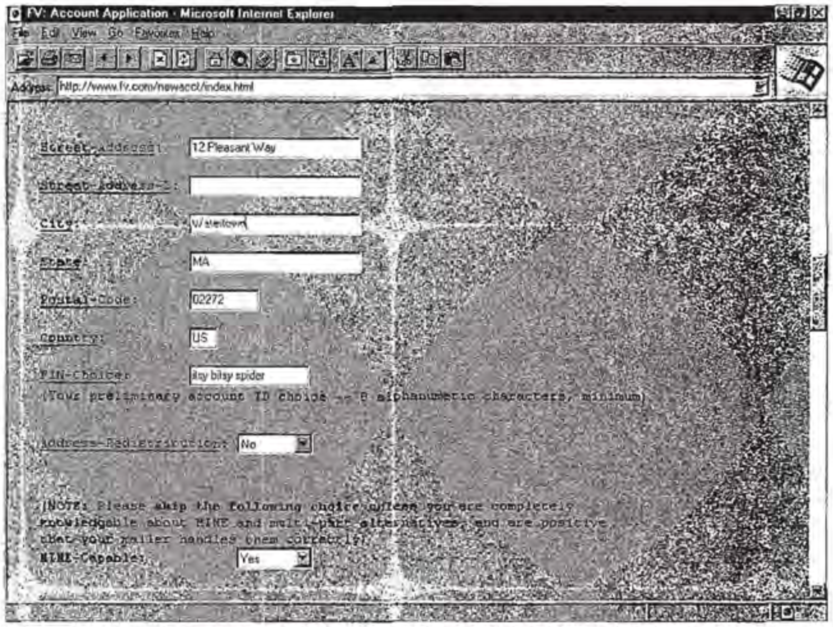
For Help click on any field name.

```
Full-Name:          Tristram Shandy

Email-Address:      tshandy@blab.net

Notification-CC:

Phone-Number:       1+617 555 1234
(Include country code. USA / Canada = 1. Example: +1 555 555 5555)

Street-Address:     12 Pleasant Way
```

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.


FV: Account Application - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address: http://www.fv.com/newacct/index.html

Street-Address: 12 Pleasant Way

Street-Address-2:

City: Watertown

State: MA

Postal-Code: 02272

Country: US

PIN-Choice: itsy bitsy spider
(Your preliminary account ID choice -- 8 alphanumeric characters, minimum)

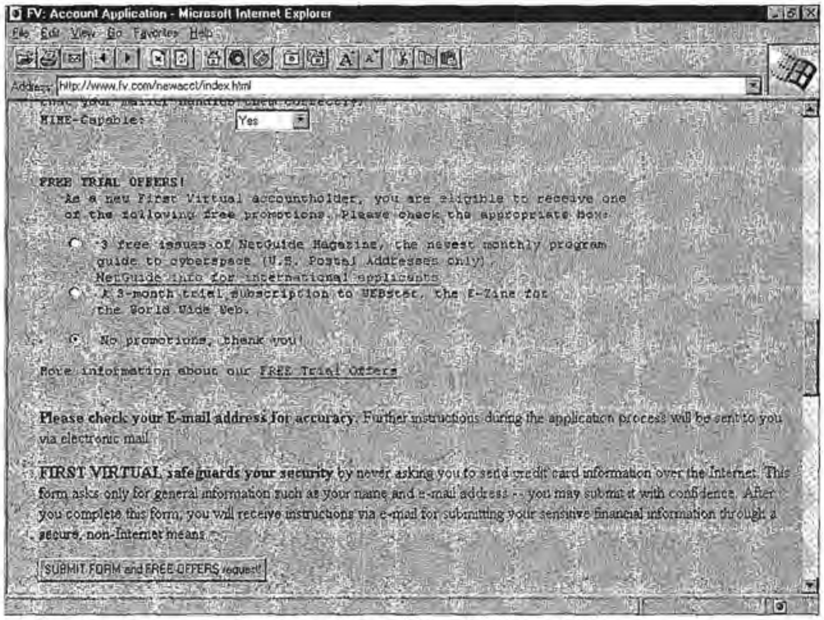
Address-Redistribution: No

[NOTE: Please skip the following choice unless you are completely knowledgeable about MIME and multi-part alternatives, and are positive that your mailer handles them correctly.]
MIME-Capable: Yes

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).


FV: Account Application - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address http://www.fv.com/newacct/index.html

MIME-Capable: Yes

FREE TRIAL OFFERS!
As a new First Virtual accountholder, you are eligible to receive one of the following free promotions. Please check the appropriate box:

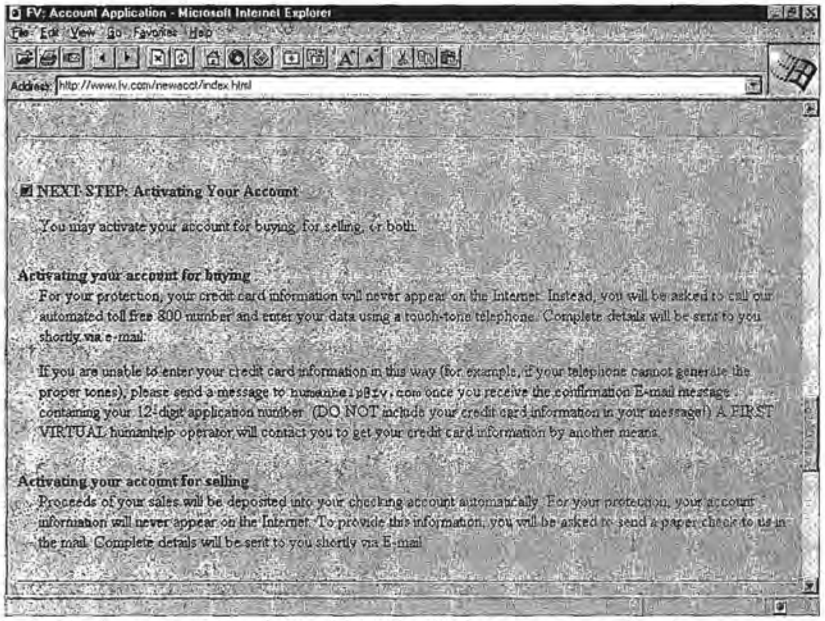
○ 3 free issues of NetGuide Magazine, the newest monthly program guide to cyberspace (U.S. Postal Addresses only).
NetGuide info for international applicants
○ A 3-month trial subscription to WEBster, the E-Zine for the World Wide Web.
● No promotions, thank you!

More information about our FREE Trial Offers

Please check your E-mail address for accuracy. Further instructions during the application process will be sent to you via electronic mail.

FIRST VIRTUAL safeguards your security by never asking you to send credit card information over the Internet. This form asks only for general information such as your name and e-mail address -- you may submit it with confidence. After you complete this form, you will receive instructions via e-mail for submitting your sensitive financial information through a secure, non-Internet means.

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


FV: Account Application - Microsoft Internet Explorer
File Edit View Go Favorites Help
Address http://www.fv.com/newacct/index.html

NEXT STEP: Activating Your Account

You may activate your account for buying, for selling, or both.

Activating your account for buying
For your protection, your credit card information will never appear on the Internet. Instead, you will be asked to call our automated toll free 800 number and enter your data using a touch-tone telephone. Complete details will be sent to you shortly via e-mail.

If you are unable to enter your credit card information in this way (for example, if your telephone cannot generate the proper tones), please send a message to humanhelp@fv.com once you receive the confirmation E-mail message containing your 12-digit application number. (DO NOT include your credit card information in your message!) A FIRST VIRTUAL humanhelp operator will contact you to get your credit card information by another means.

Activating your account for selling
Proceeds of your sales will be deposited into your checking account automatically. For your protection, your account information will never appear on the Internet. To provide this information, you will be asked to send a paper check to us in the mail. Complete details will be sent to you shortly via E-mail.

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

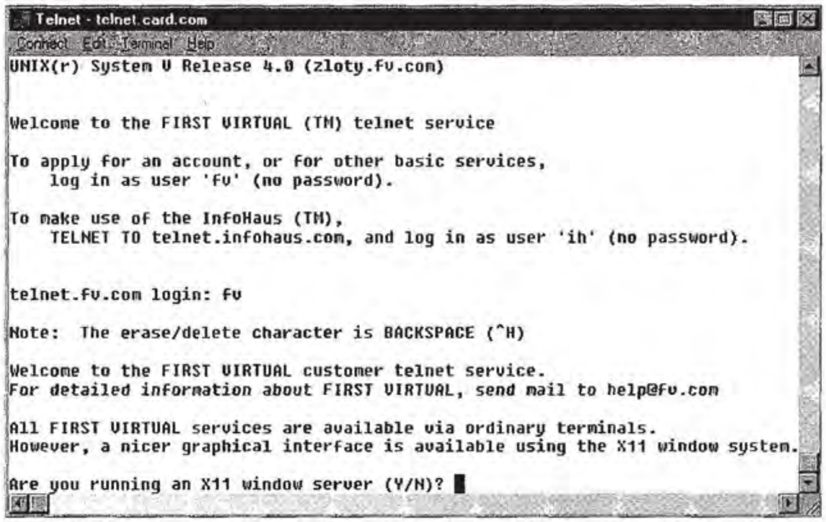
The first step is to initiate a telnet session with the First Virtual telnet server. The way this works depends on how your version of telnet works, but in any case you somehow enter the name of the remote host you want to start a session with:

```
telnet.card.com
```

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

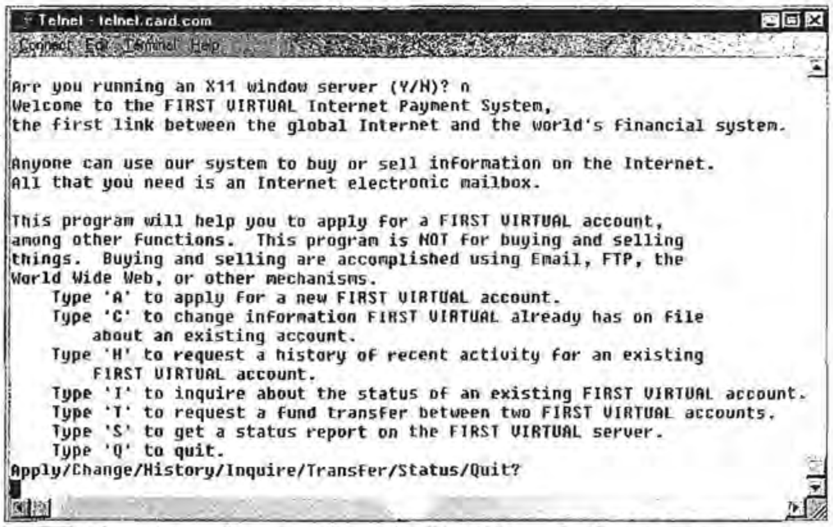
```
fv
```

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.



```
UNIX(r) System V Release 4.0 (zloty.fv.com)


Welcome to the FIRST VIRTUAL (TM) telnet service

To apply for an account, or for other basic services,
    log in as user 'fv' (no password).

To make use of the InfoHaus (TM),
    TELNET TO telnet.infohaus.com, and log in as user 'ih' (no password).


telnet.fv.com login: fv

Note:  The erase/delete character is BACKSPACE (^H)

Welcome to the FIRST VIRTUAL customer telnet service.
For detailed information about FIRST VIRTUAL, send mail to help@fv.com

All FIRST VIRTUAL services are available via ordinary terminals.
However, a nicer graphical interface is available using the X11 window system.

Are you running an X11 window server (Y/N)? █
```

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.*



```
Are you running an X11 window server (Y/N)? n
Welcome to the FIRST VIRTUAL Internet Payment System,
the first link between the global Internet and the world's financial system.

Anyone can use our system to buy or sell information on the Internet.
All that you need is an Internet electronic mailbox.

This program will help you to apply for a FIRST VIRTUAL account,
among other functions.  This program is NOT for buying and selling
things.  Buying and selling are accomplished using Email, FTP, the
World Wide Web, or other mechanisms.
    Type 'A' to apply for a new FIRST VIRTUAL account.
    Type 'C' to change information FIRST VIRTUAL already has on file
        about an existing account.
    Type 'H' to request a history of recent activity for an existing
        FIRST VIRTUAL account.
    Type 'I' to inquire about the status of an existing FIRST VIRTUAL account.
    Type 'T' to request a fund transfer between two FIRST VIRTUAL accounts.
    Type 'S' to get a status report on the FIRST VIRTUAL server.
    Type 'Q' to quit.
Apply/Change/History/Inquire/Transfer/Status/Quit?
```

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

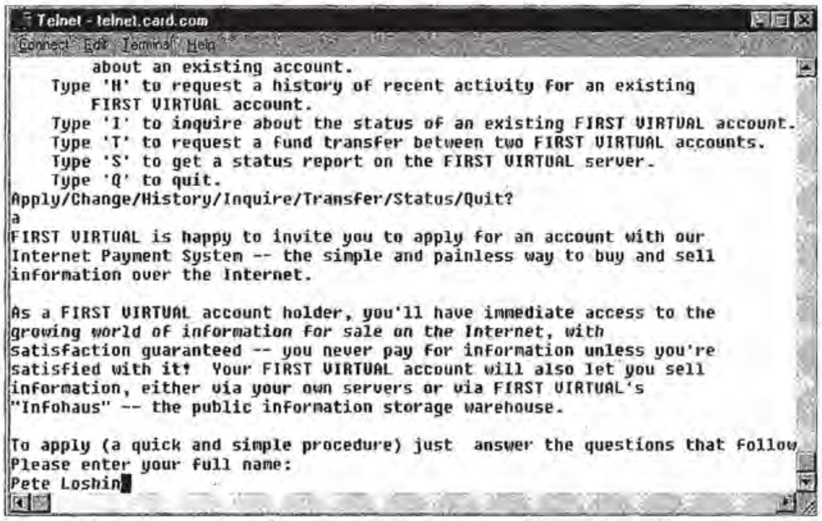
The telnet interface can be used for more than just applying for a new account, and details on the other options can be found in the last section of this chapter. These options are displayed in Figure 6-8 and include:

- 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

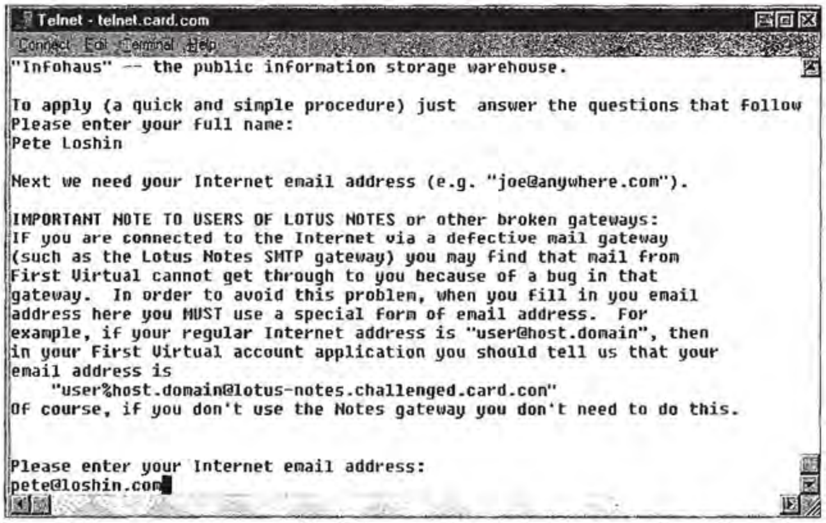
As with the other methods of applying for a First Virtual account, the telnet server provides explanatory material while requesting customer information. The same information listed in the first part of this chapter is collected interactively; for more details about each item, you are referred there (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.



```
        about an existing account.
    Type 'H' to request a history of recent activity for an existing
        FIRST VIRTUAL account.
    Type 'I' to inquire about the status of an existing FIRST VIRTUAL account.
    Type 'T' to request a fund transfer between two FIRST VIRTUAL accounts.
    Type 'S' to get a status report on the FIRST VIRTUAL server.
    Type 'Q' to quit.
Apply/Change/History/Inquire/Transfer/Status/Quit?
a
FIRST VIRTUAL is happy to invite you to apply for an account with our
Internet Payment System -- the simple and painless way to buy and sell
information over the Internet.

As a FIRST VIRTUAL account holder, you'll have immediate access to the
growing world of information for sale on the Internet, with
satisfaction guaranteed -- you never pay for information unless you're
satisfied with it!  Your FIRST VIRTUAL account will also let you sell
information, either via your own servers or via FIRST VIRTUAL's
"Infohaus" -- the public information storage warehouse.

To apply (a quick and simple procedure) just  answer the questions that follow
Please enter your full name:
Pete Loshin
```

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



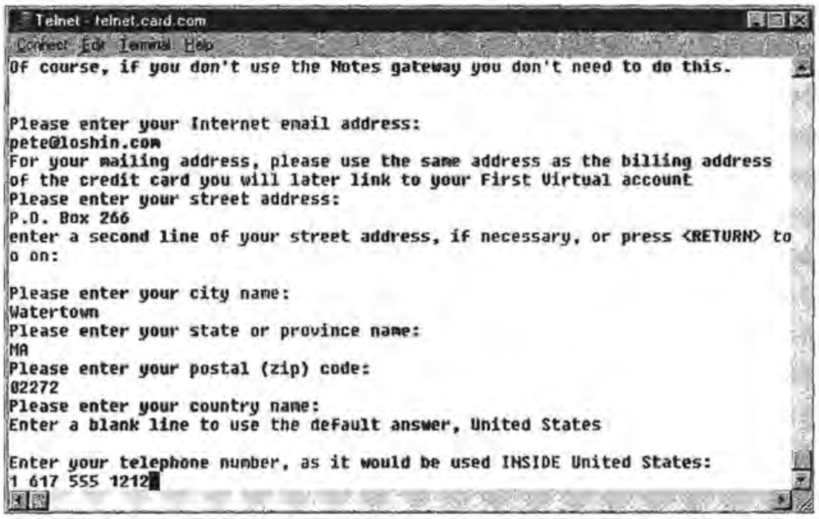
```
"Infohaus" -- the public information storage warehouse.

To apply (a quick and simple procedure) just  answer the questions that Follow
Please enter your full name:
Pete Loshin

Next we need your Internet email address (e.g. "joe@anywhere.com").

IMPORTANT NOTE TO USERS OF LOTUS NOTES or other broken gateways:
IF you are connected to the Internet via a defective mail gateway
(such as the Lotus Notes SMTP gateway) you may find that mail from
First Virtual cannot get through to you because of a bug in that
gateway.  In order to avoid this problem, when you fill in you email
address here you MUST use a special form of email address.  For
example, if your regular Internet address is "user@host.domain", then
in your First Virtual account application you should tell us that your
email address is
    "user%host.domain@lotus-notes.challenged.card.con"
Of course, if you don't use the Notes gateway you don't need to do this.


Please enter your Internet email address:
pete@loshin.com
```

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.

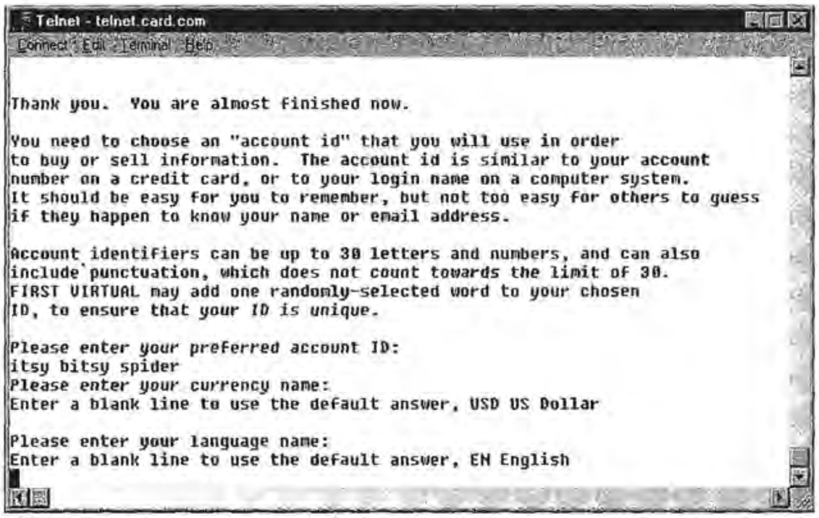
The next few prompts, as shown in Figure 6-11, are for your address and telephone number. These are self-explanatory, with only two things to watch out for: don't enter your country telephone code, and don't enter your city name on the second line of your street address.

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).



```
Of course, if you don't use the Notes gateway you don't need to do this.


Please enter your Internet email address:
pete@loshin.com
For your mailing address, please use the same address as the billing address
of the credit card you will later link to your First Virtual account
Please enter your street address:
P.O. Box 266
enter a second line of your street address, if necessary, or press <RETURN> to
o on:

Please enter your city name:
Watertown
Please enter your state or province name:
MA
Please enter your postal (zip) code:
02272
Please enter your country name:
Enter a blank line to use the default answer, United States

Enter your telephone number, as it would be used INSIDE United States:
1 617 555 1212
```

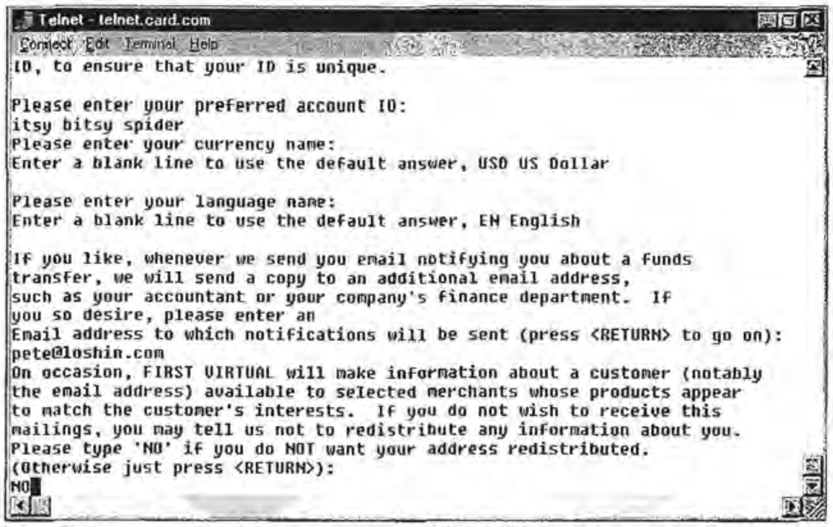
FIGURE 6-11 *Entering your address and telephone number while applying for a First Virtual account. Reprinted with permission from First Virtual Holdings Incorporated, 1996.*



```
Thank you.  You are almost finished now.

You need to choose an "account id" that you will use in order
to buy or sell information.  The account id is similar to your account
number on a credit card, or to your login name on a computer system.
It should be easy for you to remember, but not too easy for others to guess
if they happen to know your name or email address.

Account identifiers can be up to 30 letters and numbers, and can also
include punctuation, which does not count towards the limit of 30.
FIRST VIRTUAL may add one randomly-selected word to your chosen
ID, to ensure that your ID is unique.

Please enter your preferred account ID:
itsy bitsy spider
Please enter your currency name:
Enter a blank line to use the default answer, USD US Dollar

Please enter your language name:
Enter a blank line to use the default answer, EN English
```

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.



```
ID, to ensure that your ID is unique.

Please enter your preferred account ID:
itsy bitsy spider
Please enter your currency name:
Enter a blank line to use the default answer, USD US Dollar

Please enter your language name:
Enter a blank line to use the default answer, EN English

If you like, whenever we send you email notifying you about a funds
transfer, we will send a copy to an additional email address,
such as your accountant or your company's finance department.  If
you so desire, please enter an
Email address to which notifications will be sent (press <RETURN> to go on):
pete@loshin.com
On occasion, FIRST VIRTUAL will make information about a customer (notably
the email address) available to selected merchants whose products appear
to match the customer's interests.  If you do not wish to receive this
mailings, you may tell us not to redistribute any information about you.
Please type 'NO' if you do NOT want your address redistributed.
(Otherwise just press <RETURN>):
NO
```

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.*

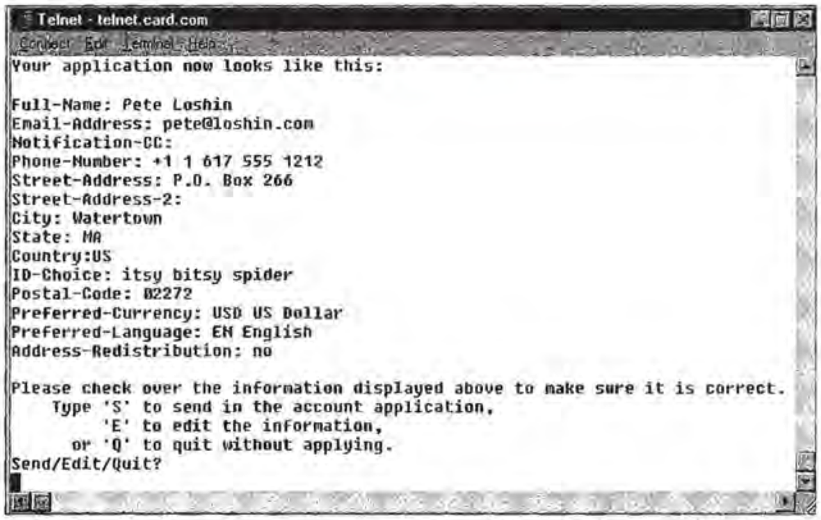
When all account information prompts have been completed, you can move on to the next step, reviewing and submitting your application.

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.



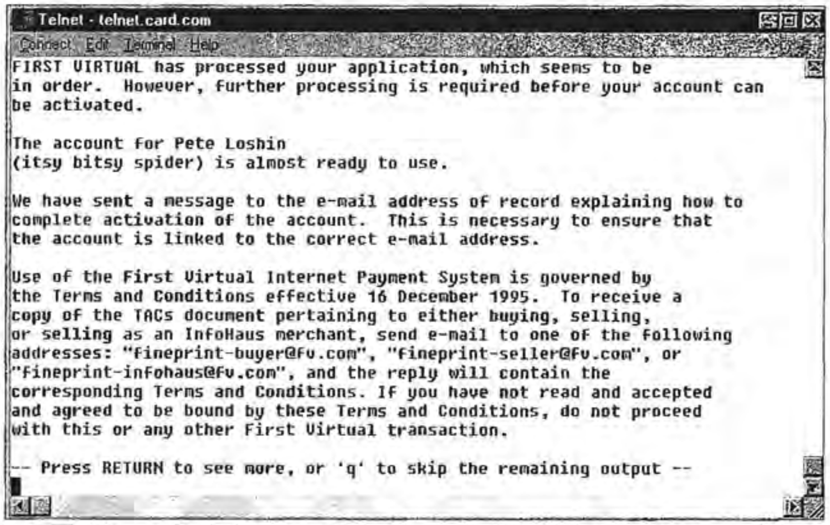
```
Your application now looks like this:

Full-Name: Pete Loshin
Email-Address: pete@loshin.com
Notification-CC:
Phone-Number: +1 1 617 555 1212
Street-Address: P.O. Box 266
Street-Address-2:
City: Watertown
State: MA
Country:US
ID-Choice: itsy bitsy spider
Postal-Code: 02272
Preferred-Currency: USD US Dollar
Preferred-Language: EN English
Address-Redistribution: no

Please check over the information displayed above to make sure it is correct.
    Type 'S' to send in the account application,
         'E' to edit the information,
      or 'Q' to quit without applying.
Send/Edit/Quit?
```

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.

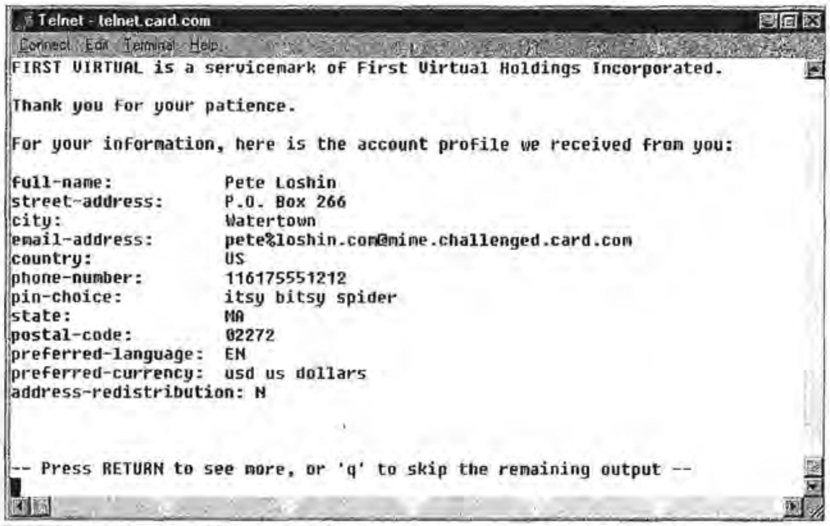
One last screen contains the exact contents of the application just submitted. You may wish to print this out for future reference; an example is shown in Figure 6-16.

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.



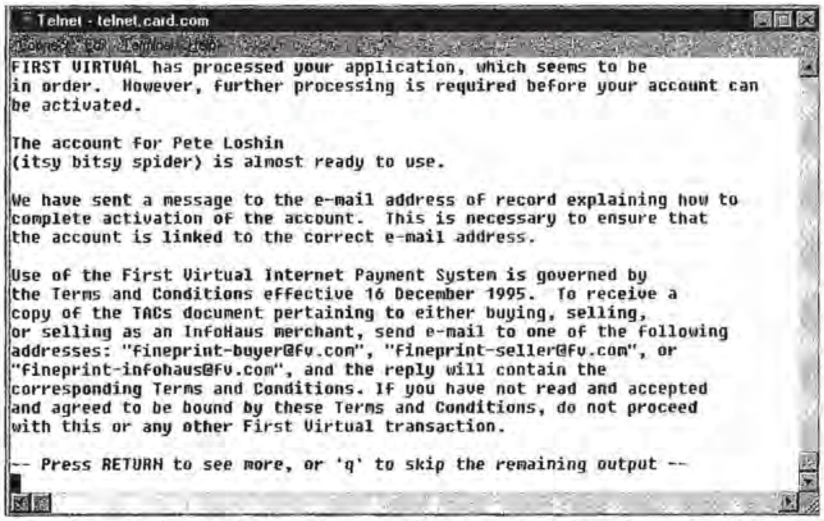
```
FIRST VIRTUAL has processed your application, which seems to be
in order.  However, further processing is required before your account can
be activated.

The account for Pete Loshin
(itsy bitsy spider) is almost ready to use.

We have sent a message to the e-mail address of record explaining how to
complete activation of the account.  This is necessary to ensure that
the account is linked to the correct e-mail address.

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.

-- Press RETURN to see more, or 'q' to skip the remaining output --
```

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



```
FIRST VIRTUAL is a servicemark of First Virtual Holdings Incorporated.

Thank you for your patience.

For your information, here is the account profile we received from you:

full-name:           Pete Loshin
street-address:      P.O. Box 266
city:                Watertown
email-address:       pete%loshin.com@mime.challenged.card.com
country:             US
phone-number:        116175551212
pin-choice:          itsy bitsy spider
state:               MA
postal-code:         02272
preferred-language:  EN
preferred-currency:  usd us dollars
address-redistribution: N


-- Press RETURN to see more, or 'q' to skip the remaining output --
```

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



```
FIRST VIRTUAL has processed your application, which seems to be
in order.  However, further processing is required before your account can
be activated.

The account for Pete Loshin
(itsy bitsy spider) is almost ready to use.

We have sent a message to the e-mail address of record explaining how to
complete activation of the account.  This is necessary to ensure that
the account is linked to the correct e-mail address.

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.

-- Press RETURN to see more, or 'q' to skip the remaining output --
```

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
```

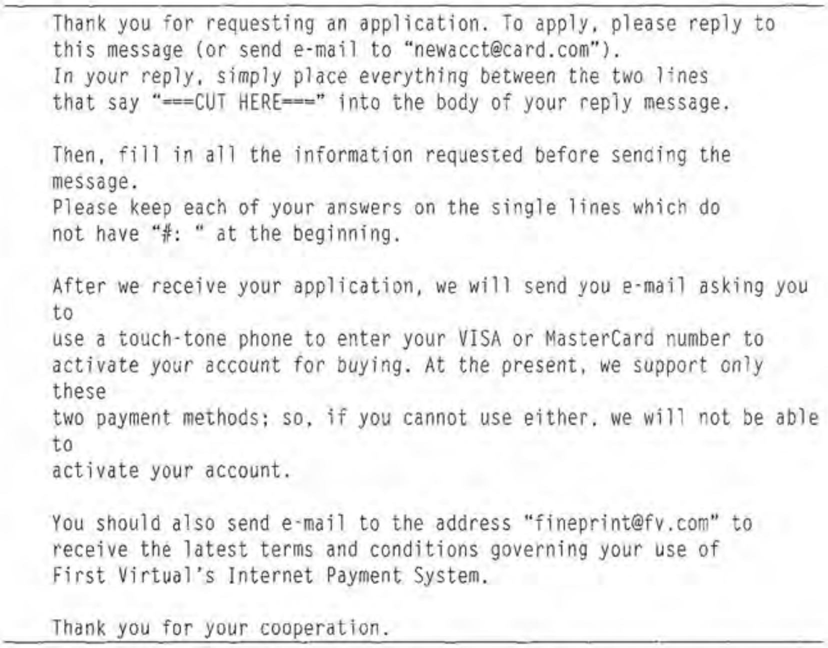
It is not necessary to put anything in the body of the message you send, nor is a subject required. This address responds automatically to messages it receives by sending out a text-only application form in an e-mail message. The e-mail version of the application is shown in Figures 6-18 through 6-22,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



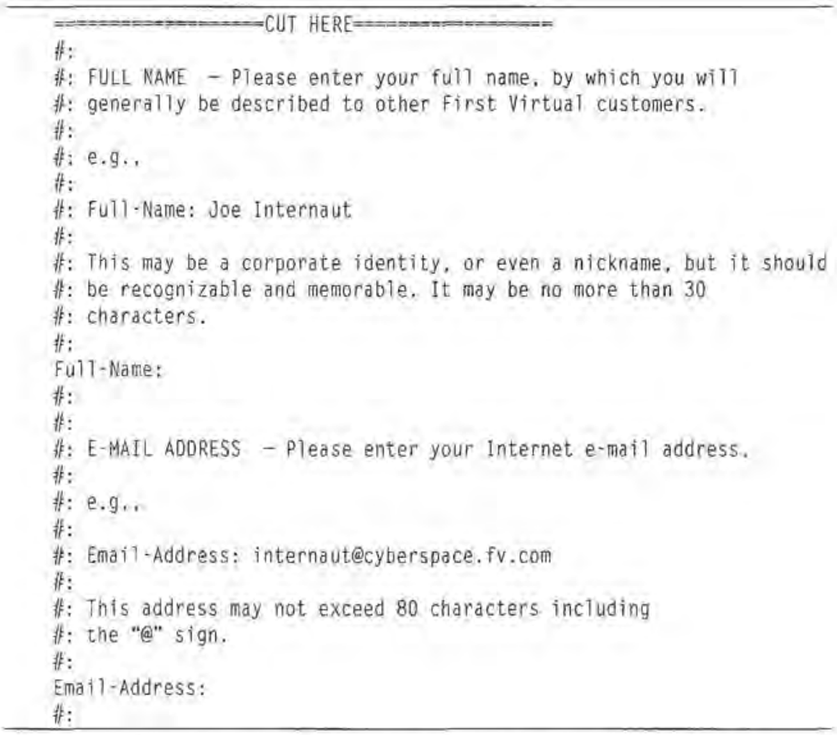
```
Thank you for requesting an application. To apply, please reply to
this message (or send e-mail to "newacct@card.com").
In your reply, simply place everything between the two lines
that say "===CUT HERE===" into the body of your reply message.

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
```

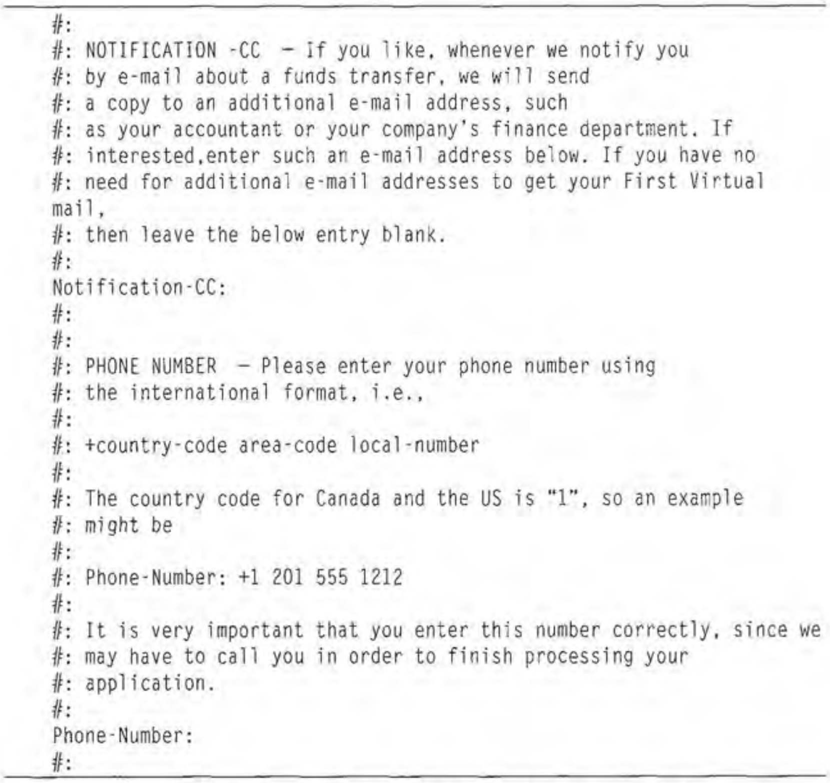
The applicant is also urged here to get a copy of the terms and conditions of the First Virtual account.



```
===================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.*

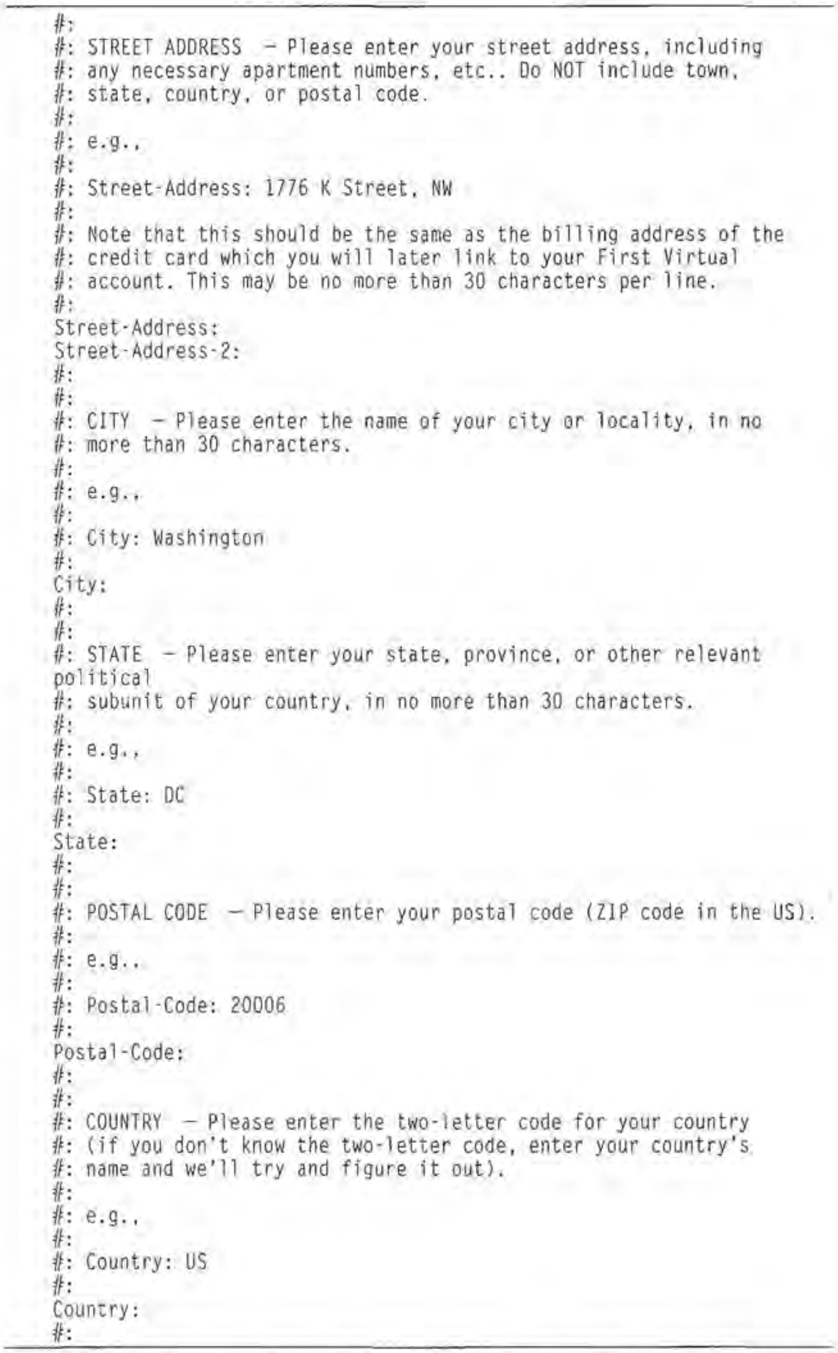
The next part of the account application, shown in Figure 6-19, is for entering your name and e-mail address. Note that the explanatory material is preceded by the symbols "#:" while the parts that you must fill out begin with the name of the information item you need to provide. The next section, shown 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

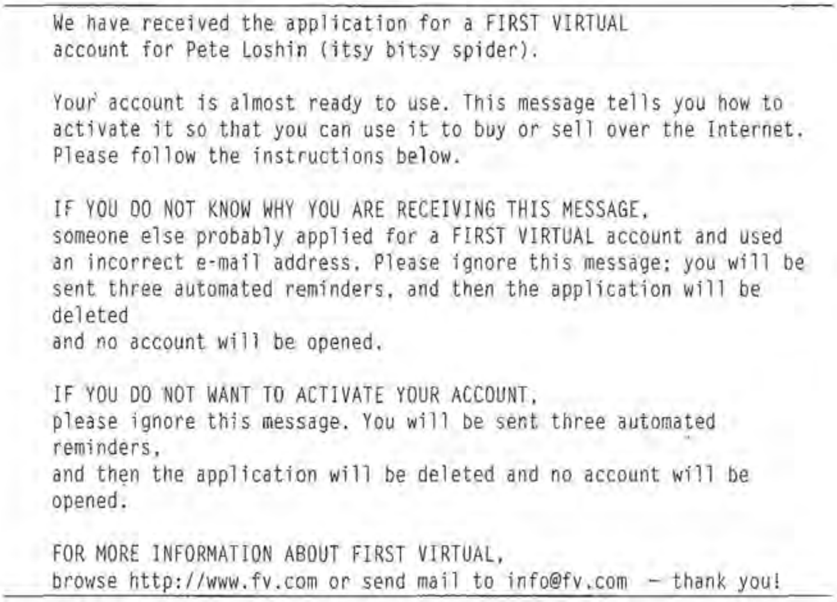
The first thing that happens after submitting your First Virtual account application, assuming that your application is in order, is that you receive an e-mail message at your main e-mail account. The start of this message was shown in Figure 6-01; the entire message is reviewed completely in this section.

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.

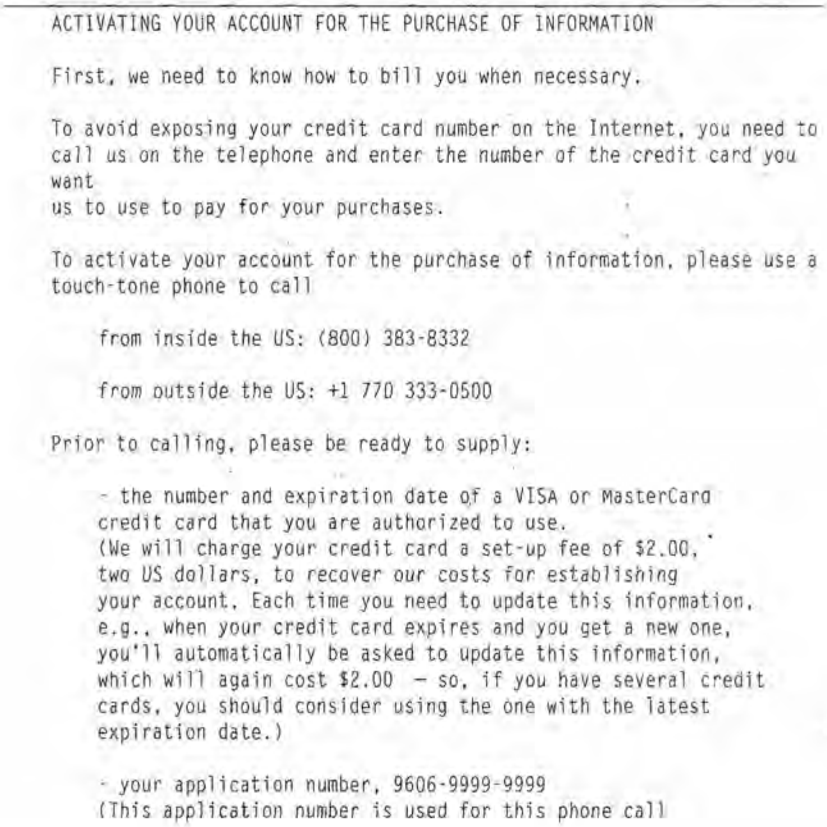


```
We have received the application for a FIRST VIRTUAL
account for Pete Loshin (itsy bitsy spider).

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
```