

**FRAUD ON THE INTERNET: SCAMS AFFECTING
CONSUMERS**

HEARING
BEFORE THE
PERMANENT
SUBCOMMITTEE ON INVESTIGATIONS
OF THE
COMMITTEE ON
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED FIFTH CONGRESS
SECOND SESSION

—————
FEBRUARY 10, 1998
—————

Printed for the use of the Committee on Governmental Affairs



U.S. GOVERNMENT PRINTING OFFICE

46-902 cc

WASHINGTON : 1998

COMMITTEE ON GOVERNMENTAL AFFAIRS

FRED THOMPSON, Tennessee, *Chairman*

SUSAN M. COLLINS, Maine	JOHN GLENN, Ohio
SAM BROWNBACK, Kansas	CARL LEVIN, Michigan
PETE V. DOMENICI, New Mexico	JOSEPH I. LIEBERMAN, Connecticut
THAD COCHRAN, Mississippi	DANIEL K. AKAKA, Hawaii
DON NICKLES, Oklahoma	RICHARD J. DURBIN, Illinois
ARLEN SPECTER, Pennsylvania	ROBERT G. TORRICELLI, New Jersey
BOB SMITH, New Hampshire	MAX CLELAND, Georgia
ROBERT F. BENNETT, Utah	

HANNAH S. SISTARE, *Staff Director and Counsel*

LEONARD WEISS, *Minority Staff Director*

MICHAL SUE PROSSER, *Chief Clerk*

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

SUSAN M. COLLINS, Maine, *Chair*

SAM BROWNBACK, Kansas	JOHN GLENN, Ohio
PETE V. DOMENICI, New Mexico	CARL LEVIN, Michigan
THAD COCHRAN, Mississippi	JOSEPH I. LIEBERMAN, Connecticut
DON NICKLES, Oklahoma	DANIEL K. AKAKA, Hawaii
ARLEN SPECTER, Pennsylvania	RICHARD J. DURBIN, Illinois
BOB SMITH, New Hampshire	ROBERT G. TORRICELLI, New Jersey
ROBERT F. BENNETT, Utah	MAX CLELAND, Georgia

TIMOTHY J. SHEA, *Chief Counsel and Staff Director*

MARY D. ROBERTSON, *Chief Clerk*

CONTENTS

Opening statements:	Page
Senator Collins	1
Senator Glenn	3

WITNESSES

TUESDAY, FEBRUARY 10, 1998

Susan Grant, Director, National Fraud Information Center, Vice President, Public Policy, National Consumers League	5
Tatiana Gau, Vice President of Integrity Assurance, America Online, Inc.	9
Barry D. Wise, Certified Public Accountant, Victim of Fortuna Alliance Inter- net Pyramid Scheme, Matthews, North Carolina	24
Hon. Robert Pitofsky, Chairman, Federal Trade Commission, accompanied by Jodie Bernstein, Director, Bureau of Consumer Protection	31

ALPHABETICAL LIST OF WITNESSES

Gau, Tatiana:	
Testimony	9
Prepared Statement	62
Grant, Susan:	
Testimony	5
Prepared Statement	45
Pitofsky, Hon. Robert:	
Testimony	31
Prepared Statement with attachments	78
Wise, Barry:	
Testimony	24
Prepared Statement	75

APPENDIX

EXHIBIT LIST

* May Be Found In The Files of the Subcommittee	Page
1. Slide presentation of Tatiana Gau, Vice President of Integrity Assurance, America Online, Inc.	240
2. Background material regarding Fortuna Alliance, including printout of Fortuna Alliance Web Site as of January 1998, miscellaneous news releases on Fortuna Alliance, and copy of <i>FTC v. Fortuna Alliance, et al.</i> , FTC Complaint, Temporary Restraining Order and Stipulated Final Judgment	267
3. Slide presentation of the Honorable Robert Pitofsky, Chairman, Federal Trade Commission	300
4. Memoranda prepared by Rena M. Johnson, Counsel, and Dennis McCar- thy, Investigator, Permanent Subcommittee on Investigations, dated February 5, 1998, to Permanent Subcommittee on Investigations' Mem- bership Liaisons regarding Internet Fraud	312
5. Supplemental Questions for the Record of The Honorable Robert Pitofsky, Chairman, Federal Trade Commission	351
6. Supplemental Questions for the Record of Susan Grant, Director, Na- tional Fraud Information Center	355

IV

	Page
7. Supplemental Questions for the Record of Tatiana Gau, Vice President of Integrity Assurance, America Online, Inc.	358
8. <i>Federal Trade Commission, Bureau of Consumer Protection—Fighting Crime on the Internet</i> (Material on law enforcement and consumer and business education.)	*
9. National Fraud Information Center (NFIC) informational sheet	360
10. “Statistics Show Internet Fraud Rising,” <i>NCL Bulletin</i> , May/June 1997 ..	361
11. Selected news articles on America Online, Inc.	*
12. Selected news articles on Federal Trade Commission (FTC)	*
13. Selected news articles on Internet fraud issues	*

FRAUD ON THE INTERNET: SCAMS AFFECTING CONSUMERS

TUESDAY, FEBRUARY 10, 1998

U.S. SENATE,
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS,
OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 9:35 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Susan Collins, Chairman of the Subcommittee, presiding.

Present: Senators Collins and Glenn.

Staff Present: Timothy J. Shea, Chief Counsel/Staff Director; Mary D. Robertson, Chief Clerk; Rena M. Johnson, Counsel; Dennis M. McCarthy, Investigator; Lindsey E. Ledwin, Staff Assistant; Kirk E. Walder, Investigator; Bob Roach, Counsel to the Minority; Leonard Weiss; Nanci Langley; Marianne Upton; Lynn Kimmerly; Myla Edwards; Jeff Gabriel; Michael Loesch; Steve Abbott and Felicia Knight.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. The Subcommittee will please come to order. This morning the Subcommittee begins its hearings on fraudulent schemes on the Internet. The Internet is emerging as a phenomenal tool of commerce and communication. One hundred seventy five countries are connected to the Internet, and approximately 50 million Americans use the Internet. By the year 2000, it is projected that there will be half-a-billion Internet users worldwide.

There is no question that the Internet has been a boon to business. The remarkable ease and speed with which transactions can be conducted over the Internet provide businesses of all sizes with access to millions of customers. For example, I am familiar with a small, family-owned business in northern Maine that uses the Internet to market its delicious lobster stew. Without the Internet, this small business would never be able to afford the marketing costs in reaching millions of customers.

For their part, consumers have the ability to engage in a variety of commercial activities across State and national borders, including shopping, banking and investing, all from the comfort, privacy and safety of their own homes. Unfortunately, those who would use the Internet to defraud can also work from the comfort, privacy and safety of their own homes or anywhere else, for that matter.

Because it can be used to transfer text, pictures, and sounds, as well as money, credit card numbers, and personal information, the potential for criminal use of the Internet is infinite. Corresponding

to the explosive growth of the Internet, the number of consumer complaints of cyberfraud to the National Fraud Information Center has increased by nearly 300 percent in the past year. The Federal Trade Commission receives between 100 and 200 Internet fraud complaints per month.

Law enforcement officials are quickly learning that almost any crime that can be committed in the real world can also be committed in the virtual world. In fact, by using the Internet, criminals can target more victims more quickly, more cheaply, and with much less chance of getting caught.

Through these hearings, the Subcommittee seeks to accomplish two goals. First, we hope to educate consumers about the potential for fraud on the Internet. While the Internet provides limitless opportunities for commerce and communication, the con artists who roam in cyberspace cause some consumers to avoid using the Internet to its full potential, much to the dismay of actual and potential online businesses.

In order to combat fear of the unknown, consumers must be armed with the knowledge of how to detect online fraud and how to avoid becoming a victim. Consumers must also be confident in the knowledge that there is a sheriff in cyberspace to whom they can report Internet fraud when they encounter it and who will investigate their complaints.

Our second goal is to determine Congress' proper role in the prevention and prosecution of online fraud. Congress must approach its role with caution. Too much regulation will hamper, if not destroy, the development of online commerce and the spirit of the Internet as a society of free and open communication.

On the other hand, too little regulation or inadequate laws will erode consumer confidence to the extent that the full potential of the Internet as a vehicle of commerce and communication may never be realized. We begin this hearing keeping in mind the delicate balance that Congress must strike. This hearing is the first in a series of hearings focusing on fraudulent schemes being perpetuated over the Internet.

The first thing that strikes you when you begin to examine Internet fraud is the old adage, "The more things change, the more they stay the same." There is nothing new or unique about many of the frauds being committed with the Internet. Instead, what is happening is that such old-fashioned frauds as work-at-home scams, pyramid schemes, fraudulent sweepstakes promotions and others have gone high-tech.

Moreover, as the chairman of the SEC testified at a previous hearing held by this Subcommittee, the Internet provides the appearance of legitimacy at a far lower cost. In such cases, the type of fraud being committed is not new; rather, it is the use of the Internet as the means of commission that is new and that poses obstacles to law enforcement and traps for the unwary Internet user.

In addition to these very traditional types of fraud, we will examine some not-so-traditional frauds that have spawned a new vernacular in Netspeak, with such labels as "Trojan horses" and "sniffers." What is particularly alarming is that the inexperienced Internet user may not even realize that he or she has been tar-

geted as a victim until well after the crook has absconded with the victim's money.

We will hear today from three panels of witnesses. Our first panel will consist of the Director of the National Fraud Information Center of the National Consumers League and the Vice President of Integrity Assurance at America Online. These witnesses will describe the types of fraud prevalent on the Internet and give us some helpful advice on how consumers can protect themselves from becoming Internet fraud victims. Our next witness will be a victim of Internet fraud who lost thousands of dollars to a pyramid scheme that was ultimately investigated and shut down by the Federal Trade Commission. Finally, I am pleased that we will hear this morning from the chairman of the Federal Trade Commission, the lead Federal agency charged with protecting consumers from this type of illegal activity. The chairman will describe Federal efforts to combat Internet fraud.

It is now my pleasure to recognize the Ranking Minority Member of the Subcommittee, the senior Senator from Ohio, Senator John Glenn, for any statement that he may wish to make.

OPENING STATEMENT OF SENATOR GLENN

Senator GLENN. Thank you, Madam Chairman, and I want to commend you for holding this hearing. The tremendous expansion of the Internet as a vehicle of communication and commerce raises an array of important security, consumer and legal issues that need to be addressed if we are to tap the full potential of this new technology. I think it is important that this Subcommittee keep on top of the important issues in this area.

Two years ago, the Subcommittee held a series of hearings about security in cyberspace. And today we look at a different but no less important topic, and that is consumer fraud over the Internet. The movement toward electronic commerce is a true cyberspace revolution. It has the potential to change the nature of the way people and firms conduct business. It can link millions of consumers and businesses, speed transactions, lower entry costs for new businesses.

Already a majority of banking and security transactions are conducted electronically. Now more and more private citizens are buying, selling and banking over the Internet. One study reported that the Internet market exceeded \$1 billion in 1995, and that is expected to grow by the year 2000 to more than \$23 billion. From \$1 billion to \$23 billion in just a 5-year period.

However, a technological breakthrough that brings new opportunities often creates new vulnerabilities. The same characteristics that make the Internet a convenient medium for commerce also make it an attractive vehicle for con artists and illegitimate businesses. In December, 1996, a task force of Federal, State and local agencies, led by the FTC, surfed the Internet and identified 500 likely pyramid schemes. How long did that search take? They did that in just 3 hours. These were not proven cases, but they appeared to be cases where some sort of fraud or wrongdoing was underway. And that was in 3 hours. One can only imagine how many more were out there then and how many more have come online since.

We will hear today from the National Consumers League reports of possible online and Internet fraud have increased from 32 per month in 1996 to 100 per month in 1997. If businesses and consumers lose confidence in transacting business electronically, the Internet's commercial potential will never be realized. Unfortunately, even a relatively small percentage of fraudulent activity can taint the entire medium and discourage its use among the general public.

To maintain business and consumer confidence in electronic commerce, we must be able to effectively police the medium for illegal behavior. Today we will hear about the proliferation of fraud and the types of fraud being perpetrated. Some of them are the conventional schemes that are committed through the mail and over the telephone, and some are unique to the Internet. All of this begs the question of what can be done by regulatory and law enforcement agencies to prevent this fraud and apprehend and punish the perpetrators.

Today we will hear what private and governmental agencies are doing to alert and educate consumers and what our regulators and law enforcement personnel are doing to apprehend and to punish the perpetrators. Do we need new legislation? We do not know. That is one thing we would like to determine from these hearings. Unfortunately, there are not a lot of easy answers. We cannot assume the traditional mechanisms used to control fraud in other communications media will be effective against Internet fraud.

Control of Internet fraud raises some complicated, technical, jurisdictional, even constitutional issues. The Internet makes it easy for con artists to remain anonymous. The international nature of the Net facilitates international criminal activity which impairs prosecution even if the perpetrators are identified. Moreover, efforts to regulate and control conduct at the front end can often run up against constitutional issues of privacy and speech.

And we are up against something here, too, in that—I want to emphasize the international nature of things. Even if we have constitutional problems in our own country here, it may not be against the constitution in some other country where some of this fraud is taking place. And how do we deal with that? So it is a very, very complex situation.

Finally, the implementation of controls requires a delicate balancing act. Too much regulation could discourage electronic commerce and waste the tremendous potential offered by the Internet. Too little regulation could leave millions of consumers and businesses victimized by fraudulent schemes and erode confidence in electronic commerce.

We need to explore how our law enforcement and consumer protection system can effectively react to this new type of crime within the legal and technical parameters that it must function. We should also discuss what responsibilities can and should be placed upon the Internet service providers, who are really the gatekeepers to the Internet. Do we need changes in current laws, rules or regulations? Are they adequate, but just inadequately enforced? How do we get into this and what kind of monitoring devices do we set up?

The Governmental Affairs Committee has two responsibilities normally in a hearing like this; one is just vent this and let it be

known so the publicity will let people be more aware of the problems and take their own methods of protection; and the second role of this Committee, of course, is to see if we need additional legislation or, if existing rules and regulations under existing law are inadequate, then we need to take action in that direction, also. So we will be investigating all these this morning.

Madam Chairman, thanks again for having this hearing. I think it is much needed.

Senator COLLINS. Thank you very much, Senator Glenn.

I would now like to call our first panel of witnesses. I would like to welcome Susan Grant, the Vice President of Public Policy for the National Consumers League, and Tatiana Gau, the Vice President of Integrity Assurance for America Online, Inc. Ms. Grant is also the Director of the League's National Fraud Information Center and Internet Fraud Watch projects, which provide advice to the public concerning Internet fraud and reports of suspected fraud to appropriate law enforcement agencies.

Pursuant to Rule 6, all witnesses who testify before the Subcommittee are required to be sworn. So at this time, I would ask you to stand and raise your right hand. Do you swear that the testimony you are about to give before the Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Ms. GRANT. I do.

Ms. GAU. I do.

Senator COLLINS. Thank you. Because of time limits, I am going to ask each of you to limit your oral testimony to 15 minutes, but any other materials you want to provide will be included in full in the hearing record.

And, Ms. Grant, we will start with you, if you will please proceed?

TESTIMONY OF SUSAN GRANT,¹ DIRECTOR, NATIONAL FRAUD INFORMATION CENTER, VICE PRESIDENT, PUBLIC POLICY, NATIONAL CONSUMERS LEAGUE

Ms. GRANT. Thank you, Madam Chairman, Senators. On behalf of the National Consumers League, America's pioneer consumer organization, I am pleased to provide you with information about the newest frontier of consumer fraud, the Internet. Some of the scams that we see, such as pyramid schemes, are as old as the league, and we will be celebrating our 100th birthday in 1999. Others are new, as advanced technology has created new opportunities for legitimate marketing and, unfortunately, also for fraud.

The National Consumers League has a bird's-eye view of Internet fraud through our Internet Fraud Watch program. Created in 1996, the Internet Fraud Watch operates in tandem with our National Fraud Information Center, which was established in 1992 to fight telemarketing fraud.

The Internet Fraud Watch and the National Fraud Information Center are unique programs that provide advice to consumers about telephone and Internet solicitations and relay reports of possible fraud to law enforcement agencies. Consumers can call our

¹The prepared statement of Ms. Grant with attachments appears in the Appendix on page 45.

toll-free number, 1-800-876-7060, or they can visit our Web site at www.fraud.org for information that helps them size up telemarketing and Internet solicitations and avoid fraud.

We receive an average of 1,500 telephone calls a week and an equal number of E-mails. We also receive dozens of letters from consumers every week, mostly asking for advice. By offering that advice in English and in Spanish, our trained counselors help to prevent consumers from becoming fraud victims.

Another important function of our Internet Fraud Watch and National Fraud Information Center programs is to relay consumers' reports about fraud to law enforcement agencies. We submit those reports daily to the electronic database maintained by the Federal Trade Commission and the National Association of Attorneys General. Our own data system also automatically faxes consumers' fraud reports to over 160 individual Federal, State and local law enforcement agencies according to criteria that those agencies have set for what they wish to receive. This alerts those agencies to scams that they may not even yet know about and provides them with the documentation that they need to shut down illicit operations.

Our free consumer and law enforcement services are supported by the members of the National Consumers League and by contributions from concerned businesses and trade organizations that are concerned about telemarketing fraud and Internet fraud. We would welcome government support for the vital services that we provide. As has been alluded to before, fraud reports to our Internet Fraud Watch have tripled since its inception in 1996, averaging about 100 per month by the end of 1997.

While this is probably just the tip of the iceberg, it enables us to provide you with a snapshot of the emerging problem of Internet fraud. In 1997, the top 10 subjects of Internet fraud reports were: (1) Web auctions: items bid for, but never delivered, value of items inflated, shills suspected of driving up prices; (2) Internet services: charges for services that were supposedly free, payment for online or Internet services that were never provided or were misrepresented; (3) general merchandise: sales of everything from T-shirts to toys, calendars to collectibles, goods never delivered or misrepresented; (4) computer equipment and software: sales of computer products that were never delivered or falsely advertised; (5) pyramids and multi-level schemes in which profits are really made from recruiting others, not from sales of goods or services to the end users and benefits of participation misrepresented; (6) business opportunities and franchises: empty promises of big profits with little or no work by investing in pre-packaged businesses or franchises; (7) work-at-home plans: materials or equipment sold with false promises of payment for piece work performed at home; (8) credit card issuing: false promises of credit cards, usually to people with bad credit on payment of an up-front fee; (9) prizes and sweepstakes: requests for up-front fees to claim winnings that never materialize; and (10) book sales, genealogies, self-improvement books and other publications that are either never delivered or misrepresented.

Bogus investments, empty offers of travel, scholarship-search scams, health fraud, and other abuses also abound on the Internet.

I should hasten to add that there are obviously many legitimate offers for goods through auction sites, for multi-level distributorships, for Internet services and other products and services on the Net. And that is precisely why it is so important to be aware of Internet fraud and to deter it.

Con artists are lurking everywhere on the Net, in flashy-looking Web sites, in classified ad sections, in unsolicited E-mail, and even in chat rooms and news groups. In our written testimony, we provided some examples, including a magazine sales scam that involved E-mail solicitations disguised as testimonials from fellow members of news groups.

We also described the technologies that have enabled new types of scams to emerge, like the Moldova case, in which consumers who downloaded a free viewer program to see pictures were unwittingly disconnected from their regular Internet service providers and reconnected to the Internet through a phone number in Moldova, resulting in huge international telephone charges.

There is no limit to the creativity with which crooks seek to use new technologies to snare their victims. Those crooks are located everywhere on the Net. If we could have the chart of the company location,¹ you will see that these are the top 20 locations. They are in many States but also in other countries. The category of locations outside of the U.S. and Canada is at number 12, tied with Arizona. Ontario is number 13 and British Columbia is number 20.

It is easy to hide who you are and where you are on the Internet, because you can supply false information to register a Web site and you can mask your return address for E-mail. Moreover, the Internet makes geographic boundaries meaningless in terms of the ability for consumers and sellers to communicate with one another. But geographic boundaries are still relevant to jurisdiction for prosecution, a fact that is well understood by con artists who take advantage of the fact that it is difficult or more difficult for law enforcement agencies to go after them if their victims are one place and they are located in another.

Another difference between the physical world and cyberspace can be seen in the problem with auctions. Sellers can offer their wares to millions of potential buyers for a very low fee. But unlike physical auctions where consumers can actually touch the merchandise and actually verify that it exists before they bid on it, you cannot do that in a Web auction, nor can the auctioneer necessarily verify that the goods exist or that they are authentic.

And there are also numerous private sellers that are selling through these Web sites, which raises several issues, including the fact that private sales are not regulated in the same way as sales by businesses. While the Internet opens the doors to honest individuals and small companies for low-cost entry into this new marketplace in cyberspace, it also provides ready access to people who are either inexperienced in business or who have fraudulent intent.

Victims of Internet fraud can also be found in every State and other countries, as well. These are the top 20 locations of the victims. Obviously, we hear from victims not only in the United States, but number 8 is the category of outside of the U.S. or Can-

¹ Charts submitted by Ms. Grant appear in the Appendix on pages 57-61.

ada. In general, victims can be found predominantly in the states that have the highest populations, not surprisingly.

No one is immune to Internet fraud. We hear from consumers of all walks of life and of all ages. If we could have the age chart, please. While people in their thirties, forties and fifties are most likely to report Internet fraud to our Internet Fraud Watch, we also have received reports from youngsters of 17 and seniors of 78.

Consumers pay for goods and services promoted through the Internet in a variety of ways. Alarming, cash is the fourth most frequent method of payment reported to our Internet Fraud Watch in 1997. This is dangerous because it leaves consumers with no documentation of the transactions and it obviously also allows crooks to avoid their tax obligations.

Though consumers are more likely to pay with checks, money orders and cash than with credit cards, we generally encourage people to use credit cards whenever they are making substantial advance payments for products or services because of their ability to dispute the charges for non-delivery or misrepresentations.

As more and more people go online, more consumer education is obviously needed to make people aware of the danger signs of Internet fraud and help them take advantage of what is on the Net without being victimized. Through our Web site and through other fora, various methods of public education that we conduct, the National Consumers League is leading the way in this effort. We also work with government and the private sector to get the word out to both consumers and to businesses about the proper use of the Internet as a tool for communication and commerce.

And as more needs to be done on the educational front, so must law enforcement's ability to go after the cybercrooks be made easier. Cross-border cases pose especially difficult challenges to investigators and prosecutors because of the legal restrictions of information sharing between different countries, the expense of transporting witnesses and the complications of using different legal systems.

Congress can help by removing any information constraints between the U.S. and other countries that still exist, setting up a fund to aid in cross-border actions, and supporting consumer and law enforcement services such as ours. We also believe that the Federal telemarketing sales rule should be expanded to cover the Internet. Many of the same disclosure requirements and prohibited acts could be tailored to fit Internet and online promotions. State law enforcement authorities would be able to go into Federal courts to obtain injunctions and judgments that would protect consumers in every State, as they can now for telemarketing fraud. And if the statute was amended to provide jurisdiction where either the victims or the perpetrators are located for State consumer protection authorities, it would enable them to go after crooks that are based in their backyards but are targeting consumers in other States, an occurrence that we see frequently.

The promise of the Internet as a means of communication and commerce is dimmed by the presence of fraud. The National Consumers League is committed to working with Congress and others to ensure a brighter and safer future for the marketplace in cyberspace.

Thank you.
Senator COLLINS. Thank you very much, Ms. Grant.
Ms. Gau.

TESTIMONY OF TATIANA GAU,¹ VICE PRESIDENT, INTEGRITY ASSURANCE, AMERICA ONLINE, INC.

Ms. GAU. Thank you, Madam Chairman and Senator Glenn. My name is Tatiana Gau, Vice President of AOL Integrity Assurance. Founded in 1985, America Online is the largest Internet service provider and has over 11 million members. I appreciate the opportunity to appear before you today to discuss how the industry is working to promote online safety and security and fight Internet fraud and abuse. Thank you for providing this forum to bring these important issues to the public.

At AOL, we are focused on preventing fraud on many fronts. To give you some insight into these initiatives, let me explain to you my department's mission. From log-on to log-off, AOL Integrity Assurance manages all of the company's safety and security measures in order to ensure the integrity of our member experience.

The prevention of Internet fraud and the promotion of online security are critical to cyberspace. It is also critical to the future development of all interactive media. We believe that the principles of education, prevention, and cooperation are key to these efforts. Identifying and tackling Internet fraud and educating all consumers on how to protect themselves and enhance their online experience is our goal.

We need to inform consumers how they can protect themselves and prevent purveyors of fraud and promote cooperation of the industry and with law enforcement. The vast majority of those who utilize the online medium are contributing positively to this vibrant community. Like any environment, however, the unfortunate reality is that there are individuals who aim to harm.

As more and more new Internet users come online, combating fraud becomes even more important. These new users are not familiar with the technology and they require special protection and attention. Fulfilling the enormous promise of the interactive medium depends on consumers and families being safe and secure online. Online integrity, therefore, is a top priority both at AOL and across our industry. All of us with a stake in cyberspace security are focused on this issue, both pursuing their own strategies and working together.

The Subcommittee has asked that I speak to you about the types of fraudulent scams that exist online. While it is difficult to provide you with a comprehensive list of these frauds, as the dynamics of the scams are constantly changing and evolving. I can provide you with a sampling of those that are most common. There are several different kind of scams that I am going to speak about. These include password scams, credit card scams, Web-based frauds and junk E-mail, commonly known as "spam." So let us begin with password scams.

¹The prepared statement of Ms. Gau appears in the Appendix on page 62.

As you will see on the slide,¹ there are two categories of password scams. There is overt password solicitation, which basically consists of social engineering tactics to lure a user into providing their password, and the concealed variety, where the user is not necessarily aware of the fact that what they are about to do is going to compromise their password.

The first example is a password “phishing” attempt via instant message. First of all, the term “phishing” has been developed in the Internet industry, P-H-I-S-H, kind of a takeoff on that, and it is now used quite widely.

Senator COLLINS. I thought it was a band. [Laughter.]

Ms. GAU. Instant messages are real time, one-on-one communications that can be transferred between one user to another, and they are private communications that only go to the designated recipient and they are real time. What scam artists often employ is a technique where they impersonate either a billing service representative of the Internet service that that user is accessing the Internet with, or they might take on the guise of a phone company representative coming up with some type of claim that there is trouble with your phone line, please provide your password. One of the things that AOL has done to try to raise awareness of this issue is on the window of the instant message, when it comes to you, there is actually a warning in red letters that states, “AOL will never ask you for your password or billing information.”

The next example via E-mail is very similar to the previous example I discussed in that they employ similar tactics, either as a billing service representative or a phone company rep or a security rep for the company, but they send it via E-mail. And these can sit in an E-mail box, can get mixed up with other personal mail, and when a user goes to read it, they may not be as vigilant as they should be in deciding whether or not they really should believe this and send in their password.

A first example of concealed password scams is what is called the “Diag.dat”, phishing via instant message. “Diag.dat” is a file where the password is recorded on your computer, and different services have different names for that file. And what scam artists will do is they will send you an E-mail under the pretext that they have malfunctioning software and could you help them out and send them a copy of your file so they can get their software working again. And, again, the rule of thumb to follow here is not only do not accept things from strangers and if it sounds too good to be true, it probably is, but also do not give out things to strangers unless you really know what you are giving.

The second example of concealed password solicitations are Trojan horses. Trojan horses are programs that come in attachments to E-mail that are sent to you under the guise of some type of beneficial offer for free: “Here is a great new animated video. Download it and enjoy.” And they take different approaches to try to entice the user to download it. And when the user does download it, in fact, at that point, they have become infected and have the poten-

¹ See Exhibit No. 1, slide presentation of Tautiana Gau, America Online, appears in the Appendix on page 240.

tial of either having their password compromised or even having files deleted, a variety of different things, depending on the Trojan.

This slide actually shows the area on America Online where we have posted safety tips for our members to understand what Trojan horses are and the telltale signs of Trojan horses, as well as linking them to an area where they can get special antivirus software that protects against Trojan horses.

This is an example of a scam using a screen-saver approach. It states, "Hey, this is cool. It's the latest coolarama screen saver. Download it and enjoy." Here the rule of thumb, of course, is to again be careful who you receive information from and do not download things from people you do not know.

A second example of an approach to provide a Trojan to someone is to take on the guise of a software company. And in this situation, the scam artists will impersonate software companies and will send a message stating, "This is the upgrade you have requested," or "This is the upgrade that you need. Please download as soon as possible."

I will discuss three more areas of password vulnerabilities. All of these scams that I have mentioned via instant message and E-mail can also occur on Web sites. Fake log-in procedures can be posted on Web sites to try to entice you into entering your password and other information that they might be requesting. There are also Web sites that take on the appearance, say, of an Internet service provider billing or registration page where, in fact, they are asking for the member to provide their registration information along with their password.

Password guessing is becoming more frequent in that recent studies have shown that approximately 60 percent of users on the Internet have insecure passwords in that they are either names of their spouses or words in the dictionary or names of their pets, whatever the case might be. And if a scam artist chooses to target one particular person, they can, in fact, just through raw attempts try to guess the password, entering and entering until they finally get in.

Password cracking is a higher level of that kind of guessing in that scam artists use an automated program to actually, through brute force, continue to prompt a password field in order to try to get into the account. This is why, of course, it is so important for users to choose safe passwords for their E-mail accounts. In fact, the password is the key to the E-mail account. And this is an area where education on the part of consumers is greatly needed.

Credit card and billing scams, there are two categories in this section. There are those scams that affect users and those scams that affect the services. Here is an example of a billing service scam, and this takes a similar approach as taken in password phishing in that this time it might say that the database is contaminated and your full name, address and credit card number and expiration date is needed in order to make sure your account will stay alive; if not, it will be turned off within 24 hours, usually taking some guise of that sort.

A slightly more complex version of that is when the E-mail that is received by the user then links the user to a Web site where, as I mentioned previously, a Web site has been put up mimicking

that service provider's design and layout to confuse the user so that they think, in fact, that this might be a legitimate site. And again, to prevent users from falling for these types of scams and to avoid their falling victim to them, AOL has posted warning messages on the E-mail screens, as well, again stating that AOL staff will never ask for personal or billing information.

There is also another example of a billing scam that I will quickly mention, and that is an approach where you receive an E-mail that says you have won a prize, whether it is a laptop or a stereo or whatever the case might be. And the E-mail goes on to describe how wonderful this prize is. And then at the bottom of the E-mail, it says, "So please reply back to us with your name and mailing address and include your credit card number to cover shipping and handling." And, of course, at the other end, the scam artist never sends the supposed prize and has the user's credit card number, and name and address, in their hands.

Subscription fraud is the first example of scams that affect the services. Scam artists can obtain on the Internet programs that are called credit card generators, and what these programs do is create fake credit card numbers that can be used to sign up with online services. They can also forge their name and address and a variety of other things, and that is why it is so important for services to have strong registration processes, as well as them being real-time verification processes.

In a lot of the business on the Internet, oftentimes the verifications are not done in real time; rather, they are done in 24 to 72 hours. And at that point, you have let the scam artist onto the service and have allowed him to spend 24 hours wreaking havoc on that service. This particular slide shows some of AOL's checks during the registration process.

A second example of fraud that affects services or, rather, merchants, is transaction fraud. And here, again, scam artists are using the credit card generator numbers that they get from the Internet or using stolen credit card numbers. And, of course, in those cases, the user or the owner of that credit card may not realize that their credit card has been stolen until they receive the next monthly bill.

One thing to keep in mind in both of these frauds is that these are not unique to online. These frauds occur in the real world, as well, whether it is signing up for a service or registering with a membership club or whatever the case might be—or making a purchase at a store. And, as we all know, in stores now they run immediate checks on your credit card number, and that is what needs to be done in the Internet, as well, to ensure that no fraud is undertaken.

There are a number of other Web frauds. Fake store fronts—those are transaction frauds that affects users, where they enter a credit card number and the site is actually a fake. Virulent active content, Trojan horses, are different types of things that can be pushed onto your computer, and thus all users should be sure to have antivirus software and browser—setting their browser security alerts.

I am going to run through this very quickly, given the limit on time—just to move through, I have a number of examples of scams,

the marketing scam, which is a weight-loss program in this case. And, again, typically in these situations, the product does not live up to its claims. Here is a get-rich-quick scam, make a million dollars from home, or in this case, make \$800,000 from home. And, also, there are varieties of pyramid schemes, as well.

Forged headers are what I call a category of identity fraud in that the sender of the E-mail has chosen to disguise their identity by using forged headers and thus making it difficult to identify that user. One important item that I would like to stress is that users are not without protection. AOL fundamentally believes that a combination of education and technology tools that we make available to our members are the answer to solving the fraud problem as it exists today. We also believe fundamentally that law enforcement needs to play an important role in this, and we have an ongoing relationship with law enforcement to cooperate on cases that come up.

What I will run through here quickly are some of the tools that are available. Mail controls actually allow a user to designate who they can receive E-mail from in their account and who they cannot receive E-mail from, who they do not want to. It also allows them to block instant messages, and this is particularly useful for families that have children who are using the Internet, where they do not want their children exposed to these kinds of things.

The file download alert is a warning against Trojan horses. This message pops up any time a member goes to download a file attached to E-mail that contains a Trojan horse. The Neighborhood Watch is both an educational area on America Online, but is also a centralized point to link to all the different tools that are available by AOL to their members, to customize their online experience.

Notify AOL is our notification mechanism. Members send in reports of fraud that they either witness or fall victim to, and we have staff that monitors those reports 24 hours, 7 days a week, and will take action, such as terminating the account of the offender if appropriate and, if illegal, referring the matter on to law enforcement.

Spam tools include AOL proprietary blocking technology against spam, as well as the mail controls that I discussed previously. Parental controls—this is a one-stop shopping for parents to set up again these accounts for their children that are customized so that their children are not exposed to things believed to be beyond their age level.

And finally, in summary, I would just like to reiterate some of the safety tips that I mentioned through the presentation: Choosing a safe password and making sure you protect that password by not giving out the information to anyone. Similarly, do not give out personal information. Just like in the real world, you would not give out your Social Security number, you should not be doing it online. Do not download files from strangers or, as I like to call it, do not take candy from strangers. If a Web site is unfamiliar, look into the company's background before you do business with them. And perhaps most importantly, do not believe everything you read; if it sounds too good to be true, it probably is.

Thank you.

Senator COLLINS. Thank you very much, Ms. Gau.

Ms. Grant, I would like to start with some questions to you. It was very helpful for us to have the list of the top 10 Internet frauds that have been reported to you, but as you pointed out, legitimate businesses are also included in each of those categories. A lot of people order books through the Internet with very satisfactory results. Are there any warning signs that you can give the public for when it is likely that an offer is fraudulent within those top 10, because the difficulty is in distinguishing between legitimate online offers versus the fraudulent schemes?

Ms. GRANT. That is really difficult for consumers, and that is one thing that we try to help them with when they contact us. First, offers of things for free or for ridiculously cheap prices ought to be suspect. The Trojan horses that were referred to are one example of something that somebody is supposedly giving you as a gift. And you have to ask why; there is usually a string attached. If someone is trying to get you to buy expensive computer equipment for a very low price, you have to wonder why that is. Promises that you can make money in business very easily with little or no work have to be suspect. Promises that you can get huge returns on an investment with little or no risk are also suspect.

Many of the same pieces of advice that we give for telemarketing fraud, we also give for Internet fraud, that it is illegal for somebody to ask you for a fee up-front to get a prize. That is an illegal lottery and something that should be a red flag to you. Some other warning signs are promises of loans or credit cards to people with bad credit because legitimate lenders and card issuers generally do not extend credit to people with credit problems. So we try to warn people that if someone is promising you that, it is probably not true.

Senator COLLINS. My impression is that consumers who never would have fallen victim to a fraudulent solicitation if it had come in the mail or via the telephone will nevertheless be sucked in by one that is offered on the Internet, that somehow consumers are under the false impression that if something is on the Internet, it has been screened or it somehow conveys an aura of legitimacy.

What makes consumers—first of all, would you agree with that? And, second, what makes consumers so susceptible to fraudulent schemes on the Internet?

Ms. GRANT. I agree with what you have said and I think that consumers also are under the same misconceptions with magazine and newspaper and television advertising, where they think that there is more screening than actually exists in most cases. But another part of this is that I think that consumers are seduced by the novelty and excitement of being on the Net and that they are not necessarily looking at these promotions with the same cold eye that they need to and that they would if somebody was knocking at their door and offering them something.

Senator COLLINS. Despite all our best efforts to educate consumers, what should a consumer do if they feel they have been a victim of Internet fraud?

Ms. GRANT. Report it to our Internet Fraud Watch program, for one thing. They may also want to contact their own State attorney general or State securities commission, or whatever would be the

appropriate agency locally for their problem. But the most important thing is to report it, because that is the only way that these kinds of fraudulent operations can ultimately be shut down.

Senator COLLINS. Ms. Gau, does AOL encourage its customers to report fraudulent activities to you, and if so, what do you do if you get a complaint of that nature?

Ms. GAU. We do indeed try to encourage our members to do that, and one of the ways in which we accomplish that is by putting promotion buttons on the welcome screen, which is the first screen that AOL members see when they sign on. And that button takes them to the Notify AOL area and provides them with guidelines on how to report frauds or different types of problems they may come across online.

On the question of how do we respond to them, as I indicated previously, we do have staff that is there 24 hours, 7 days a week, to respond to the reports. If appropriate, they will terminate the account of the offender, and if it is illegal, they will refer it on to law enforcement.

Senator COLLINS. One reason consumers can get trapped in a fraudulent scheme is that a Web site looks so elaborate and looks so legitimate. Could you explain, as part of our efforts to educate consumers, how easy it is to set up a Web site and whether or not it is difficult to dismantle one once the fraud has been perpetuated?

Ms. GAU. Yes. And perhaps in that regard I would like to quickly provide a response to one of the questions you asked Susan, in terms of is it because people are on their computers in the safety of their home that they fall victim to some of these scams? I would add to that the fact that in effect there is this false sense of security, of users who are on the computer in the safety of their home. Not only are they thrilled by this new medium and all the technologies that it offers, as Susan Grant mentioned, but also they believe that they are untouchable because the computer has been something that has been very familiar to people for many years, where you wrote your documents that nobody else could read. And so there is an assumption that that continues along, as well.

Now, to answer your question directly, Web sites can be set up relatively inexpensively. It can cost as little as a couple of hundred dollars to set up a Web site. As far as dismantling Web sites, it all depends on who is the host provider for that Web site. In the case of certain domain names that are registered and where Web sites pop up on frequently, they even disappear themselves within a couple days because they do not want to stay up too long and they move around.

If one needs to dismantle a Web site, like in some cases we have been alerted by our users that there is an Internet site out there that is collecting information under the guise of being an AOL billing page, we then contact the service provider that is hosting that Web site and ask them to take it down, obviously under the due diligence procedures and in legal compliance.

Senator COLLINS. Ms. Grant, does the National Fraud Information Center follow up on the complaints that it refers to law enforcement agencies?

Ms. GRANT. No, we do not, and in fact we tell consumers who are contacting us that we will provide their information to law enforce-

ment agencies, that we do not investigate it ourselves, and not to contact us again to find out the status of their report because we do not have that information. We really do not have the resources to follow up.

We find out sometimes what agencies are doing with those reports because they will contact us to ask for more information or we will receive a press release saying that an enforcement action has been taken against a company that is very familiar to us.

Senator COLLINS. Have you found that law enforcement agencies have—I realize you do not do actually follow-up—but in general, are they receptive to the complaints that you forward? Do you have an impression that they are investigated? My concern is that I think it is very confusing for consumers who are ripped off to figure out where to go and to figure out what is the right agency.

As Senator Glenn pointed out, we have an unusual jurisdictional issue involving the Internet. We may be dealing with a fraudulent company that is not even located in the United States.

Ms. GRANT. Yes. Actually, last summer we surveyed the law enforcement users of our system to find out what they thought about our services in providing them with reports about telemarketing and Internet fraud. They said that the information was extremely valuable to them, not only to tip them off about things that they may not have even been aware of, but to give them information about victims and witnesses that could help them make their cases.

So they are very appreciative of these services.

One of the most difficult aspects of Internet fraud is that you have victims scattered so far, that it is often hard for an agency to find out about everything that is going on when consumers are most likely to contact their own local agencies about their own problems. If the perpetrator is located in one State, but the victims are all in another State, then the attorney general's office in the State where the perpetrator is located may not be hearing about that. The consumers may be complaining to the attorneys general in their own States.

Senator COLLINS. Ms. Gau, how do the con artists that use spam as their weapon get the addresses, the E-mail addresses, of their victims?

Ms. GAU. They do so in a variety of ways. They can obtain programs on the Internet that are called harvesting programs, and they can go into a chat room and, in effect, harvest or copy all of the screen names or the E-mail names of the people in that room. They can also use this tool to collect names off of message boards, off of member directories for different service providers, and collect a mass of names to which they can send their E-mail.

Senator COLLINS. I would like to now turn to what may be some additional remedies to this problem. Ms. Grant, in your testimony, you suggested that the FTC's telemarketing sales rules should be made to apply to online and Internet promotions. And we have the chairman of the FTC here today, so I am going to ask him about your suggestion. Could you please explain a little bit more to us about what the rule provides and how expanding its scope would help combat Internet fraud?

Ms. GRANT. The rule basically has two parts; one is a set of required disclosures and the other is prohibited practices. Just to use

sweepstakes and prize offers as an example, there are certain disclosures that are required concerning the odds of winning and the values of the prizes and so on, which would, I think, be properly applicable to Internet promotions that involve prizes and sweepstakes.

There are also a host of prohibited practices, for instance, asking for a payment up-front to extend credit or a loan. Again, I think that such a prohibition for Internet and online promotions would make sense. A lot of the same types of scams that we see on the Internet are things that have been long-time abuses in telemarketing fraud and that the telemarketing fraud rule was promulgated to prevent and to give law enforcement agencies more tools to prosecute.

Senator COLLINS. Do you believe, Ms. Grant, that online providers such as AOL should also be doing more to educate consumers up-front about the possibility of fraud and to do more referrals to law enforcement? Is there an obligation that they should undertake, as well?

Ms. GRANT. I think there is. I think that most of the major Internet service providers are stepping up to the plate, as AOL is, and doing that through the educational messages that were demonstrated here today and reporting those problems when they hear about them to law enforcement agencies. There are, of course, a vast number of providers out there and not everybody is stepping up to the plate and helping to become part of a solution here.

Senator COLLINS. I appreciate very much the specific regulatory and law changes that you both included in your testimony. I am going to turn now to Senator Glenn for his questions.

Senator GLENN. Thank you very much. Senator Durbin could not be here this morning. He has done a lot of work in this area and is very interested in it. He is on Judiciary, and they are having some hearings or meetings on the tobacco situation, and so he could not be here this morning.

But his staff gave me something a moment ago that I was not even aware of. We now even have magazines out, Internet Shopper, that I had not seen before, and I was just leafing through it here. I was not reading a cowboy story or something up here. I was looking through this. [Laughter.]

And I am amazed at some of this stuff. I was not aware until this moment about the extent of some of this. We have 50 national companies and thousands of Internet service providers listed in here State by State. I count 65 in my own State of Ohio, and 50 national. Illinois has, I think, more than that. I did not count them, but probably 80 or so in Illinois, where Senator Durbin is from, of course.

And I am going back to the office and click in on one of these. It says, "Click and win 1,000 roses, Valentine's Day coming up, www.," and I will not give the rest of it. But this has gone beyond anything that I was even aware of, even with the briefings that I received for this hearing. I had not seen that particular magazine before and I am not recommending everybody go get a subscription.

These things, you know, "Click and win 1,000 roses for Valentine's Day, detail and registration at," and gives it. That is it, that is pretty seductive.

Ms. GRANT. That could be legitimate.

Senator GLENN. Could be.

Ms. GRANT. But I do not know as I would smell those roses yet.
[Laughter.]

Senator GLENN. Could be. But if everybody who clicks in is expected to win 1,000 roses, they have a lot of roses going out. And Annie is going to like that once I get back to the office and click in on that. But we knew this was big stuff, and it is even bigger than I realized it was when the Chairman planned these hearings.

Do we need stiffer civil and criminal penalties on these, Ms. Grant?

Ms. GRANT. I am always in favor of stiffer civil and criminal penalties. I think you need to hit white-collar crooks in the pocket.

Senator GLENN. But you have to get a balance here. Somewhere you get into personal rights and constitutional rights and things like that. Are we at the point where we shouldn't go further, or are we way short of that point and need more legislation?

Ms. GRANT. Even in telemarketing, there are ongoing discussions about enhanced penalties for targeting certain vulnerable populations or for certain really egregious violations. And I certainly think, especially if we are talking about fraud, if we are talking about intentionally robbing people of their money, that those people ought to be put in jail.

Senator GLENN. Now, Ms. Gau, you look at it from an industry standpoint. Do you think we need more regulation? I know the industry has preferred to look at this that they can self-regulate, and yet the record has not been very good in that regard.

Ms. GAU. We do, in fact, believe that education and technology tools are the way to provide consumers with real-time information that can allow them to protect themselves when they go online.

When it comes to the role of the government, we believe the government does need to play a role, just as they do in the real world, the off-line world, in protecting consumers against fraud. And Congress should thus appropriate the necessary resources to the agencies that are charged with enforcing anti-fraud statutes.

We would agree that enhancing penalties would be a beneficial way to deter other criminals from conducting such activities, but we also believe that one needs to take a look at the juvenile issue, because a number of the scam artists that are perpetrating these frauds are, indeed, juveniles.

Senator GLENN. Well, OK. The Internet service providers have been termed as being the gatekeepers, and many consumers who use the Internet will form their opinions of the medium through the relations that they have with the ISP's. And I guess you folks have about as much control about what goes on the Internet as anyone, and yet the track record hasn't been all that good for the industry.

I don't know when you came with America Online, but it is discouraging to read that three of the largest ISP's, including America Online, were charged by and settled with the FTC for engaging in practices that I would look at as being similar to the consumer scams we are talking about here today.

Let me just run through them real quickly here:

Offering free trial subscriptions and not adequately disclosing that consumers would be billed as subscribers after the trial period unless they affirmatively canceled their membership. I wouldn't want to be treated that way, and I don't think you would either. In mail, years ago, some businesses would send a gift through the mail and then they billed you for it unless you paid the postage to return it. Well, we have corrected that through the years, and that is not done now.

Another one was debiting checking accounts before receiving authorization to do so. I don't want anybody debiting my checking account, and you wouldn't either, unless I gave specific permission to do it.

Failing to give consumers advance notice of the amounts to be transferred from their accounts.

Now, America Online was also cited for failing to adequately inform consumers that 15 seconds of connection time was added to each session. Well, I don't know how major these things are. I know that they were settled somehow with FTC. I don't know how they were settled or what the penalties were. And maybe this didn't happen on your watch. But when the leaders in the industry are being hauled up for things like this, we have got a major problem. What are we going to do about it?

Ms. GAU. Well, my first comment would be to say that we have, indeed, corrected those problems in that we are providing more disclosure on exactly the policies. And I think that that is very dissimilar from the fraud that is occurring on the Internet where it is strangers that approach you—

Senator GLENN. Well, it is a different level. I will grant you that.

Ms. GAU. You may recall that one of my safety tips was not to do business with a Web site or a service, even, if you don't know that company's background. And there, really, I do believe that, in fact, we were not adequately, perhaps, disclosing all these specifics to our consumers, but we have rectified that at this point.

Senator GLENN. Well, this showed a mind-set of what they were trying to do, maximize the money coming in and don't worry about whether the person was being treated fairly or not, it seems to me. Has that mind-set been changed now so that you are looking at it from the consumer's standpoint? You are a consumer, too.

Ms. GAU. Yes.

Senator GLENN. If you call and you get a service from somebody, you don't want to be treated like that. Has this all been corrected now? And how are we handling this?

Ms. GAU. Absolutely. This is being corrected, and it actually was one of the reasons for my appointment at America Online in late 1996. It was to create the position of integrity assurance in that area—

Senator GLENN. Very good.

Ms. GAU [continuing]. As part of the assurances to members that they are being looked out for and actually acting as somewhat of an ombudsman for members.

Senator GLENN. Well, I hope your being brought on has corrected all this, and I hope you are keeping them on a mind-set that looks at it from the consumer's standpoint. Because if this goes on like this, I can guarantee you we are going to have tough new regula-

tions and tough new standards, and we will have to set up a big enforcement group, we will expand FTC, and we will do all sorts of things, whatever we have to do, because this is the wave of the future. This is not a little thing where we are going out on the Internet momentarily and all the Internet stuff will pass away in a year or two. We are just at the beginning of the Internet way of doing business and financial transactions.

So if the companies don't police themselves, they are going to get policed. I will tell you that right now, and you can carry that back. If the same people are in charge that let this stuff happen to begin with, then bringing you on as one person down below in the hierarchy isn't going to correct the problem, if the mind-set of everybody else is that they are out to skim what they can off the people. And that is from one of the biggest companies in the business.

Ms. GAU. I would again like to reiterate that those issues have been corrected, and, indeed, moving forward, they are situations that are not going to happen again.

Senator GLENN. Just those three or four things that I read off, were estimates ever made or did FTC prepare any estimates of what consumers lost as a result of these practices? Because as I understand it, no recompense was made, no payback was made to people that were dealt with unfairly. Is that correct?

Ms. GAU. My understanding is that, in fact, there were settlements made, but I don't know the specifics of them.

Senator GLENN. Did FTC make an estimate of that, do you know?

Ms. GAU. I don't know.

Senator GLENN. OK. We will ask and see if they have any estimates on that later when they testify.

Recently, America Online went to court to stop a junk mailer that threatened to publicize the addresses of all 5 million customers of American Online if your company did not allow it to send junk mail. That sounds like the worst kind of extortion, with the customers as the innocent victims. Luckily, it sounds as if you were successful in stopping the firm.

Could you tell us about that case and explain how the company was able to obtain the E-mail addresses? And I would like you also to address, once it had them, did it in turn sell them to others? Is this a scheme where one company sells to another, to another, to another, and so the fact that you have corrected it with one company, the horse is out of the barn, and it may have gone to half a dozen companies eventually? Is that correct?

Ms. GAU. Yes. The site collected the names of AOL members through harvesting techniques, as I explained previously.

Senator GLENN. Yes.

Ms. GAU. Not only do they pass them on to other spammers, but they also sell them via spam. In those cases, you will receive an E-mail, saying, "Want to grow your business? Send \$25, and we will send you 5 million screen names you can send your promotion material to."

So, in fact, there is this constant continuing circle of spammers to spammers, and then also selling those lists to individual users as well.

Senator GLENN. Do all the ISP's have a policy or do most of them have a policy of selling their customer list to others?

Ms. GAU. I am not familiar, no.

Senator GLENN. How about America Online? Do they sell their customer list to others or rent them?

Ms. GAU. No.¹

Senator GLENN. Either one?

Ms. GAU. Not anything providing the actual identity of the user in terms of their screen name on AOL.

Senator GLENN. I am not sure what you mean by that. Say I am going into business, could I contact America Online and could I get a list of people? Or how would I do that? Would I buy them?

Ms. GAU. No, you could not.

Senator GLENN. I could not. Could I rent them?

Ms. GAU. No, you could not.

Senator GLENN. From the accounts I have read, it sounds like an ISP already has the authority and technical capability to refuse to send out unsolicited E-mail and to enable its subscribers to block it. Is that correct?

Ms. GAU. That is correct.

Senator GLENN. What standards do you apply when deciding whether or not to send out unsolicited commercial E-mail? What is the criteria?

Ms. GAU. What is the criteria for AOL in deciding to send out?

Senator GLENN. What standards do you apply when deciding whether or not to send out unsolicited commercial E-mail?

Ms. GAU. We apply the concept of a previous existing business relationship or, in fact, that if we have to send mail to our members, it is because we have a member relationship with them.

Senator GLENN. Well, what is your business relationship? What does a business relationship consist of, then?

Ms. GAU. I am sorry? Excuse me.

Senator GLENN. Define business relationship.

Ms. GAU. A pre-existing relationship in which either a transaction has occurred or there is an ongoing business relationship.

Senator GLENN. Well, OK. So if anybody had come in online, if anybody had tapped in and used your service at all, then they could be the subject of having unsolicited E-mail sent to them in the future because you have had a business relationship with that person. Is that correct?

Ms. GAU. Perhaps I would like to make a clarification. What I am discussing right now is mail that AOL might send to its members. I am not discussing mail that comes from the Internet which is of a spam nature, and junk E-mail. Mail that AOL sends to its members consists of advisory notices about different things relating to the service, letters from Steve Case, the chairman and CEO, and materials of those sort that are meant to enhance the member experience, but they are, if you want to call them, unsolicited.

Senator GLENN. There have been some recent articles about AOL subscribers being the targets of E-mail scams to steal such things as account numbers, passwords, credit cards. In one scam to obtain

¹See Exhibit No. 7 for clarification of this answer which appears in the Appendix on page 358.

credit card numbers, a perpetrator pretended to be AOL's Member Services Department and had a fake letter from AOL's chairman.

Do you know how the con artists were getting your subscribers' addresses? And how do you guard against that?

Ms. GAU. The example you just mentioned was one of the examples that—types of examples I illustrated in my presentation. The scam artists harvest names, again, for these types of scams, collecting names from people in chat rooms, member profiles, message boards, whatever the case might be, and then, in fact, target the individual.

Senator GLENN. Let me address this to both of you. Should there be a requirement in law or by regulation that requires ISP's to screen commercial sites more carefully, to set some criteria and make them screen for those criteria?

Ms. GAU. At AOL we do, indeed, engage in screening processes with the commercial sites that are allowed to be set up within the AOL environment. As far as the Internet is concerned, when users go out onto the Internet, they, in fact, are entering areas where AOL does not have control over those sites.

Senator GLENN. Ms. Grant, do you think there should be requirements, certain criteria set by government, that they would have to adhere to in screening commercial sites more carefully?

Ms. GRANT. We have long advocated that newspapers and other forms of media that have advertising do a better job of voluntary screening. I am not sure how feasible it would be to actually screen everything on the Net except perhaps things that are just within a certain proprietary service, like AOL. But I think that if a better job of self-screening isn't done, maybe that is something we should look into in the future.

Senator GLENN. Should the ISP's be required to report customer complaints to the FTC?

Ms. GRANT. I think with the consumer's permission they should. When consumers report fraud to us, we tell them that, with their permission, we will report this information to law enforcement agencies.

Senator GLENN. Ms. Gau.

Ms. GAU. I would absolutely agree that we would need the member's consent to forward the message on. But we do, indeed, refer any illegal activity to law enforcement, so I think that the combination of both of those would be a good step.

Senator GLENN. Well, there were already two pieces of legislation introduced that deal with unsolicited commercial E-mail, and given the proliferation of this activity and the technical and consumer problems it creates, there is likely to be even more legislation proposed unless the problem is controlled.

You people are more familiar with this than I am, certainly, and I presume the Chairman, also. But what do we need to do? What do you suggest at this point? Ms. Gau.

Ms. GAU. Unfortunately, spam is constantly changing in terms of the techniques that they use to attack Internet service providers. They are using ever-changing techniques, whether it is changing the source addresses from which the spam is coming or forging headers to disguise where the message is actually coming from, that make it extremely complicated not only to create effective

blocking software that would, in fact, prevent any spam from getting through, but also poses problems for some of the legislation currently being proposed as the dynamics are continually changing and they will continue to change, and next week we probably will have one more problem to deal with.

Senator GLENN. Could ISP's levy extra fees on those who want to send unsolicited commercial E-mail? Would that control it?

Ms. GAU. We are not in favor of unsolicited commercial E-mail, so that is not something that we are looking at right now.

Senator GLENN. Well, just to sort of summarize here—and I know I am probably over my time, Madam Chairman—let me just say that the issues are how much we are going to regulate to protect those interests, who will regulate, and are we moving fast enough. Two big concerns are consumer protection and individual privacy. And I don't know whether we ought to require opt-in systems so businesses can't collect personal information unless the consumer first gives his or her permission. Maybe we are coming to that one of these days. I don't know. And children, we haven't dealt with that one at all, didn't even question on that. Kids have far more computer knowledge than I have, I can guarantee you that, and they are into these things all the time. And what happens if someone says go get daddy's credit card and do whatever? How do we deal with children? That is another big one here.

I don't know how long the FTC wants to wait on self-regulation by the industry before we step in with other regulations, but that is what is coming if the industry doesn't do it itself.

Thank you.

Senator COLLINS. Thank you, Senator Glenn. I want to commend you for your probing questions on this very important issue.

I just want to second your comments about the need for the ISP's to set a very high ethical standard. If they are going to be the ones that are helping to educate consumers about fraud, certainly their own activities have to be above reproach, and I think that is an excellent point.

Senator GLENN. I have to leave early. I am going back to get those thousand roses for Annie. [Laughter.]

Senator COLLINS. Could I have a few?

I just have one final question for Ms. Grant. Ms. Grant, we had hearings last year on fraud in the securities industry, and we are starting to see the Internet used as a medium for that kind of fraud. And I know that you have a long history, the league, in this area.

I propose to the industry as well as the Chairman of the Securities and Exchange Commission that there be adopted what I call a zero tolerance policy so that if a licensed individual in the industry commits a serious breach of ethical standards or a fraud, that that individual be banned from the industry forever, because what we have seen is rogue brokers going from firm to firm.

Do you think that such an action would be helpful in trying to curb the use of the Internet for securities fraud?

Ms. GRANT. I think it probably would. I think that more action has to be done to keep repeat offenders from victimizing consumers both in the physical world and in cyberspace.

Senator COLLINS. I want to thank you both very much for your testimony today and your cooperation with our investigation. We very much appreciate your being here.

Ms. GRANT. Thank you.

Ms. GAU. Thank you.

Senator COLLINS. Our next witness is Barry Wise, a certified public accountant and a certified fraud examiner, from Matthews, North Carolina.

Mr. Wise unfortunately was a victim of a pyramid scheme conducted over the Internet. I very much appreciate his willingness to share his experience with us. It shows that even an individual with financial training can become a victim of cyberspace fraud. So we very much appreciate your being here.

As I explained earlier, pursuant to Rule VI, all the witnesses who testify before us are required to be sworn in, so I would ask that you stand and raise your right hand. Do you swear that the testimony you will give to the Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. WISE. Yes.

Senator COLLINS. Thank you.

We look forward to hearing your testimony today. Because of time constraints, including an upcoming vote, I would ask that you limit your testimony to 10 minutes, and we will put your prepared statement as part of the hearing record.

Please proceed.

TESTIMONY OF BARRY D. WISE,¹ CERTIFIED PUBLIC ACCOUNTANT, VICTIM OF FORTUNA ALLIANCE INTERNET PYRAMID SCHEME, MATTHEWS, NORTH CAROLINA

Mr. WISE. Actually, I have already learned a lot from what I have heard.

Madam Chairman and Members of the Subcommittee, my name is Barry Wise, and it is my pleasure to be here today to share my experiences with you of being defrauded by a company known as Fortuna Alliance.² I am currently employed by the Duke Energy Corporation as a senior internal auditor. I am also a certified public accountant and recently became a certified fraud examiner. Obviously I wish I had become a certified fraud examiner when I was considering my investment with Fortuna Alliance.

I am also a husband and a father of two young children. The intention of my investment with Fortuna was meant to benefit my children's future, not the financial heartache that resulted instead.

I would also like to express my appreciation to the Federal Trade Commission at this time for the help that they have given with this case.

In April of 1996, I was told by a colleague that a company known as Fortuna Alliance was advertising on the Internet. The company was supposedly offering a good investment opportunity with a high rate of return. My associate informed me that he knew of a person who had already received some return on the investment, so it must be legitimate. I later discovered that this person had some

¹The prepared statement of Mr. Wise appears in the Appendix on page 75.

²See Exhibit No. 2 for background material on Fortuna Alliance which appears in the Appendix on page 267.

type of relationship with the founder of Fortuna Alliance and the return on investment probably was nothing more than bait money to create an air of legitimacy to the scheme.

I visited the Fortuna Alliance Web site as well as numerous other individual sites that had been created by its members. These members were people who had already invested with Fortuna and were actively recruiting new investors which would be directly to their benefit. The Fortuna Alliance site explained that each membership would pay out a maximum of \$5,000 per month when a matrix of approximately 300 was filled with names of new investors. The matrix was supposedly based on their "unique mathematical formula: The Fibonacci Sequence." The Web site informed that Fortuna was about to begin a massive advertising campaign to solicit new members; therefore, I would not have to recruit anyone or do anything to get a return on my investment. I would not have to work at filling up the matrix because Fortuna Alliance's advertising campaign would accomplish that for me. However, the recruitment of new investors was encouraged because that would fill up the matrix faster, which in turn would initiate a flow of money to Fortuna Alliance members.

Another part of the Fortuna Alliance business was a co-op through which products and services would be sold in the matrix. I understood that a commission would be paid to me for any purchases made in the co-op by people in my matrix. It should be noted I never received any literature from Fortuna that explained what goods were for sale and how to purchase them. Fortuna stated there was a money-back guarantee of my entire initial investment if after 90 days I was not completely satisfied for any reason. The offer really made me feel that I had nothing to lose with this potentially lucrative investment.

In late April of 1996, after carefully studying the Fortuna Alliance Web site and several of the individual member sites, I decided to make an investment. I purchased 15 elite membership at \$250 each and two premier memberships which cost \$600 each. My total investment was \$4,950 which I hoped would result in a monthly income check from Fortuna Alliance. Fortuna insisted that I pay this investment by money order or certified check only. When I received a very elaborate package of investment information from Fortuna for each of my memberships, I read this information carefully and continued to understand I did not have to actually do anything to receive a return on my investment.

Shortly after purchasing these memberships, I tried to call Fortuna Alliance several times in order to verify my investment was properly recorded in their computer system. My telephone calls were always answered by an automated voice system that never connected me to an actual person.

In late May 1996, I was roving the Internet while working on a project with the search word "fraud." During this search, I came across a notice by the Federal Trade Commission that Fortuna Alliance had been shut down for operating an illegal pyramid scheme and making false claims. I immediately sent a letter to Fortuna Alliance requesting a refund of my money. They never refunded any of the \$4,950 initial investment. I also filed a claim with the Federal Trade Commission.

Upon discovering that I had been the victim of a fraud via the Internet, I started to do some investigation on my own. I determined that in order to be a legitimate multi-level marketing company, commission needs to be paid on actual goods and services sold. Fortuna Alliance was supposedly going to pay commissions only based on one-time fees paid to purchase a membership—in other words, money was just being funneled to people at the top of the pyramid. During my research, I noted several other companies on the Internet which appeared to be operating illegal pyramid-type schemes.

In the spring of 1997, I received a letter from Gilardi & Company in San Rafael, California. Gilardi & Company had been appointed by the Federal Trade Commission to be the claims administrator for Fortuna Alliance. The correspondence I received from Gilardi & Company indicated that my account consisted of only three elite memberships, when I had actually purchased 15 elite membership and two premier memberships. Evidently, Fortuna Alliance's records of my purchases did not properly account for my entire investment. I subsequently filed a claim of \$4,950 with proper documentation to Gilardi & Company. In a telephone conversation with representatives of Gilardi & Company, I determined that my claim of \$4,950 was accepted and verified by them as accurate.

Shortly after my dealings with Gilardi & Company, I received a letter from Fortuna Alliance which stated they had been cleared of all charges and were continuing to do business as Fortuna Alliance II. They also encouraged me not to request a refund and continue to invest with Fortuna Alliance II. I disregarded this letter and its message as being completely bogus.

It is my understanding that the Federal Trade Commission has collected enough funds from Fortuna Alliance thus far to cover 60 percent of investors' claims. On January 6, 1998, the court issued a compliance order that would allow over 8,600 Fortuna Alliance members to begin receiving partial refunds which would cover approximately 60 percent of their individual claim amounts.

I appreciate this opportunity to share my story. This concludes my statement. I would be pleased to answer any questions.

Senator COLLINS. Thank you very much, Mr. Wise.

Let me start by just clarifying some of the facts in this case. This essentially was a pyramid scheme—is that correct? Where there was an effort to recruit a lot of investors and eventually it was going to collapse?

Mr. WISE. That is right.

Senator COLLINS. Did you ever recover the nearly \$5,000 that you invested?

Mr. WISE. No, but it is my understanding per a conversation with Gilardi & Company that on February 11, 60 percent of that money will be mailed to me. And it should be on its way shortly.

Senator COLLINS. So you hope to recover about 60 percent of your initial investment due to the action taken by the FTC?

Mr. WISE. At least at this time. I am not sure what the outcome is going to be between them and the Federal Trade Commission as far as recouping the other 40 percent. But I do know that the Federal Trade Commission is aggressively pursuing that remaining 40 percent.

Senator COLLINS. How much experience did you have using the Internet prior to your dealings with Fortuna Alliance?

Mr. WISE. I think prior to that I had had Internet service for about a year, but not a whole lot of experience using the Internet.

Senator COLLINS. Had you had experience with investing via the Internet prior to your dealings with Fortuna?

Mr. WISE. No, I had never invested on the Internet. And I never will, also.

Senator COLLINS. Did it cause you—were you more concerned, did you have a higher level of wariness that you were dealing through the Internet rather than in person with a financial advisor, for example?

Mr. WISE. Not really, because an individual had told me about it and plus they had one Web site of their own and probably numerous other Web sites that were out there by some of your individual investors, which sort of added a legitimacy to what was going on.

Senator COLLINS. You have mentioned that there were these other Web sites.

Mr. WISE. Right.

Senator COLLINS. It is my understanding that Fortuna Alliance instructed its investors to create their own Web sites. Is that correct?

Mr. WISE. That is my understanding.

Senator COLLINS. And that was a means of soliciting new members to try to sustain the pyramid a little bit longer. Is that correct?

Mr. WISE. Yes. At the time, I pulled up all the individual Web sites, just did a search word "Fortuna," and I think there were probably three or four complete pages that would come up. When a search engine would pull up Fortuna, you would see page after page of just nothing but Fortuna, Fortuna, Fortuna. And you would go to another page, and you would see more lines of Fortuna. So there were numerous Web sites out there.

Senator COLLINS. Did the existence of all these other related Web sites confer to you a certain legitimacy of the enterprise? Did it reassure you that it must be legitimate or otherwise why would there be all these Web sites?

Mr. WISE. Yes, that did, plus they also had a 90-day money-back guarantee, which I guess at that time added some legitimacy. But in hindsight, money-back guarantees really don't mean anything.

Senator COLLINS. That certainly seems to have been the case.

You discovered that you were a victim of fraud really by chance. Is that correct?

Mr. WISE. That is right. I don't think if I had searched—had been on the Internet with the search engine "fraud, I don't even know if I would have ever known about it.

Senator COLLINS. What did the FTC statement say that you chanced upon when you were browsing on the Internet?

Mr. WISE. I can't recall the exact—what the FTC said. I just know once I hit that search engine, there was a big alert that came up, and it gave a lot of details of what the Federal Trade Commission did as far as what they had. They had raided their complex.

They had been shut down, could not do business anymore, and they were in the process of legal action against Fortuna.

Senator COLLINS. So the FTC site specifically identified Fortuna Alliance as a fraudulent enterprise that it was taking action against?

Mr. WISE. That is right.

Senator COLLINS. And had it not been for your stumbling across the FTC's fraud Web site, do you think you would have discovered that you were a victim of fraud as quickly?

Mr. WISE. No.

Senator COLLINS. You stated that you received a letter from Fortuna Alliance indicating that they had been cleared of all charges and urging you not to request a refund. And it is my understanding that this letter was written after action was taken against the company by the FTC.

Did you report that additional letter that you received to the FTC?

Mr. WISE. I did not. In hindsight, I probably should have, but the reason I didn't, because I know that the FTC at that time was aggressively pursuing Fortuna and had already one legal action against them.

Senator COLLINS. As a consumer, did you find it troubling that Fortuna Alliance could make such claims and so quickly could emerge with a new identity as Fortuna Alliance II?

Mr. WISE. Yes. I would have had more concern if they would have set up business in the realm of the United States. But when they set up Fortuna Alliance II, they did that outside of the country, which really makes—

Senator COLLINS. So this was an offshore enterprise?

Mr. WISE. Right, which really makes it difficult to do anything with anybody that does something like that.

Senator COLLINS. Again, I see a parallel with the hearings we held on securities scams where a rogue broker will go from one firm to another, set up a new base of operations, and it becomes difficult to track and catch these individuals.

Did you try to use the information resources of the Internet to do some background research on Fortuna Alliance prior to or at the time of your investment?

Mr. WISE. No. I will have to plead ignorance to that.

Senator COLLINS. Given your experience—and, again, I would emphasize that you are much more sophisticated than a lot of people who are doing investments via the Internet. You are a CPA. I know how prestigious a designation that is. And yet you got trapped.

I guess I have two final questions for you. One, why do you think you did get taken in? And, second, what advice would you have for other consumers so that they can avoid the kind of fraudulent investment that you made?

Mr. WISE. I was mainly taken in with the 90-day money-back guarantee, which, like I said earlier, I now know means absolutely nothing. They were obviously offering a good return on the investment. Probably greed comes into play, which in turn clouds your thinking ability to a certain extent.

As far as the normal investor or anybody on the street, as long as they know that to be legitimate, especially in a multi-level marketing scheme like this, commissions need to be paid solely on goods or services that are sold. If they knew that, that would probably eliminate at least some of the people that would get involved in an illegal pyramid scheme.

Senator COLLINS. Thank you very much, Mr. Wise.

Senator Glenn.

Senator GLENN. Thank you very much, Madam Chairman.

I was interested in some of the material that Fortuna Alliance sent out where even an educated person like yourself, an auditor, who is familiar with accounts and how these things work, you could be drawn into something like this. And the company has all the things down there, “no recruiting necessary, no investment, no”—a whole bunch of things, just on and on and on here. And then its latest publication talks about how the FTC came in with armed people and so on, and the company says down here it has made some changes “to protect it from interference by governmental agencies of any country,” and so on.

The gist of this is these people are so brazen, they have now set up Fortuna Alliance II.

Mr. WISE. That is right.

Senator GLENN. It is offshore, I guess. Where is it based now?

Mr. WISE. I have no idea. I have sort of disconnected myself from them. [Laughter.]

Senator GLENN. You are not a new investor—

Mr. WISE. I would like to add one other thing that I thought was, to me, almost amusing at the time that the Federal Trade Commission went in and raided Fortuna. Based on my knowledge, there was a good percentage of Fortuna Alliance memberships that were so—became so, I guess, sucked in with Fortuna that they were actually, I guess, mad at the Federal Trade Commission for shutting down Fortuna and were sending, I guess, letters and complaining about the Federal Trade Commission as being a tyrannous-type organization, which in hindsight that was far from the fact in this particular case.

Senator GLENN. Well, they say here that Fortuna Alliance offices in the United States were “raided by armed members of a U.S. regulatory enforcement agency known as the Federal Trade Commission.” I didn’t know the Federal Trade Commission went around packing guns, but maybe they do now. [Laughter.]

Maybe we will get some testimony on that a little bit later. Fortuna Alliance was forced into receivership by order of a Federal judge and so on. But they have opened up again offshore. That is the point I am making.

Mr. WISE. Right.

Senator GLENN. They have opened up again. They are still going, and I guess they are back on the Internet and didn’t even change their name except they now make it Fortuna Alliance II. And, “The new Fortuna Alliance II will be similar to the original Fortuna Alliance in most ways. It was very good as it was, and the primary reasons to change any part of it are, one, to protect it from interference by governmental agencies of any country; and, two, to take advantage of all the founder, Augie Delgado”—that sounds great—

“and executive team learned from this most devastating experience at the hands of a brutal U.S. regulatory agency, the Federal Trade Commission,” and so on.

And the one that I like, too, is they have—this is in their quotes, “a unique mathematical formula: The Fibonacci Sequence.” At least the first syllable is right, the “fib” part, anyway.

Mr. WISE. That is right.

Senator GLENN. We know that. So, anyway, these things, you squash them here and they pop up somewhere offshore, I guess.

We are on five lights up there, and I know we have got to vote, Madam Chairman, but this is very interesting, and I hope it gets enough publicity that people are not subscribing to things like this.

Senator COLLINS. Mr. Wise, I do want to thank you very much for sharing your experience. It certainly is a cautionary tale for all of us, and we appreciate your willingness to come forward.

Thank you very much.

Mr. WISE. All right. Thank you.

Senator COLLINS. We are now in the middle of a vote, and I expect a second vote back to back. So I regret to inform our next witness, with great apologies, that we are going to need to take a 15-minute recess. But we will resume in 15 minutes.

Thank you.

[Recess.]

Senator COLLINS. The Subcommittee will be back in session. I apologize for the delay. We were on Senate time, which I have yet to get used to, and the vote was held for a couple of Senators, so I apologize for the delay.

Our final witness this morning is the Hon. Robert Pitofsky, the chairman of the Federal Trade Commission. The chairman’s testimony will provide the Subcommittee with an overview of the roots of Internet fraud from the Federal perspective, as well as a discussion of the FTC’s civil enforcement action and consumer education efforts.

I would note that the FTC’s enforcement led to the dismantling of the pyramid scheme about which the previous witness just testified. It is my understanding that the chairman may wish to have an individual accompany him, and I would at this time introduce Jodie Bernstein, the Director of Consumer Protection, and anyone else that you would like to have, Mr. Pitofsky, we would welcome their participation.

As I have explained, pursuant to the rules of the Subcommittee, all witnesses who testify are required to be sworn, so I would ask that you stand and raise your right hands.

Do you swear that the testimony you are about to give to the Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. PITOFSKY. I do.

Ms. BERNSTEIN. I do.

Senator COLLINS. Thank you.

Again, Mr. Pitofsky, my apologies for the unavoidable delays. I know you have a busy schedule, and I appreciate your willingness to participate in these important hearings. And I would ask that you proceed with your statement.

TESTIMONY OF HON. ROBERT PITOFSKY,¹ CHAIRMAN, FEDERAL TRADE COMMISSION, ACCOMPANIED BY JODIE BERNSTEIN, DIRECTOR, BUREAU OF CONSUMER PROTECTION

Mr. PITOFSKY. Thank you, Madam Chairman. I am delighted to be here, and I want to compliment the Subcommittee for holding hearings on this important and, I think, sometimes somewhat neglected subject, and that is, marketing fraud on the Internet and in this country generally.

With your permission, I would like to submit my full testimony for the record and just summarize it this morning.

Senator COLLINS. It will be included in the record in its entirety. Thank you.

Mr. PITOFSKY. And may I introduce Jodie Bernstein, who is director of our Bureau of Consumer Protection, and who is in charge of enforcement in this area, and also very active on the consumer education front.

As you know, the FTC is the primary agency at the Federal level authorized to challenge fraud and deception. We do so under Section 5 of the Federal Trade Commission Act, which outlaws unfair and deceptive acts and practices in commerce. Section 5 gives the Commission the authority not only to combat fraudulent activity by issuing administrative cease and desist orders, but also by going directly into Federal court to seek injunctive relief and consumer redress.

We have noted several times already this morning that the Internet is growing by leaps and bounds.² Fifty-eight million potential consumers are already online, and we expect Internet commerce to grow exponentially over the next few years. Online advertising is expected to grow to \$4.35 billion by the year 2000, and as Senator Glenn's reference to the Internet Shopper pointed out, online commerce is growing. We think it might be as much as \$220 billion by the year 2001.

In this expanding marketplace, consumers often will receive new goods and services faster and at lower prices. They will receive more information to make informed decisions. In general, I think of the Internet as a pro-competitive, pro-consumer opportunity.

We also know, however, that the growth of the Internet will generate an increase in fraud and deception. To combat these problems, we will combine traditional law enforcement with new types of consumer and business education.

The Commission has already brought over 25 Federal actions against deceptive and fraudulent activity on the Internet. That has just occurred in the last year and a half or so. Most of these cases have involved old wine in new bottles, traditional types of scams that have migrated to cyberspace. For example, we have seen credit repair scams and business opportunity schemes, that look very much like the traditional programs that we have seen in telemarketing and elsewhere.

It has also given new life to a kind of fraud that we thought we had virtually wiped out 10 or 15 years ago, and that is the pyramid

¹ The prepared statement of Mr. Pitofsky and additional copy submitted for the record appears in the Appendix on page 78.

² See Exhibit No. 3, slide presentation of the Honorable Robert Pitofsky, Chairman, Federal Trade Commission which appears in the Appendix on page 300.

fraud. In one of the largest Internet cases, which has been discussed, the Commission sued Fortuna Alliance to halt an alleged pyramid scheme that took more than \$7 million from consumers.

We have also pursued more sophisticated schemes on the Internet, and you heard about the Audiotex case where the Commission sued a Web site operator that allegedly hijacked consumers' computer modems and silently placed very expensive international telephone calls to a Moldovan telephone number. That is a former republic of Russia. And, of course, consumers ended up with very large telephone bills at the end of the month.

In addition to law enforcement, the Commission has fought Internet fraud through aggressive consumer education because, in the long run, consumer education really is the best way for people to protect their own interests. The Commission has used technology on the Internet to establish informative Web sites and teaser pages. The Commission home page receives over 100,000 visitors per month and provides consumers with access to everything from fraud alerts to Federal court pleadings. The public can easily find information either by clicking into a category like Consumer Line or by placing simple key words into our search engine.

The Commission also has established another Web site with other Federal agencies. This site provides one-stop shopping for people with consumer questions about automobile recalls, drug safety, other topics. And we have tried to reach out to consumers through educational teaser pages.

The "Ultimate Prosperity Page" is an example of a teaser site posted by the Commission. It mimics an online business opportunity scam promising high earnings for little or no efforts. Clicking through this site, a consumer will eventually arrive at the last page, which states, "If you responded to an ad like this, you could get scammed." This page warns consumers about fraudulent business opportunities and provides a link back to the ftc.gov Web site for more information.

The Commission also fights Internet fraud by reaching out to businesses, especially new entrepreneurs who may be entering the marketplace for the first time and may not know the basic principles of consumer protection law. We have pursued partnerships with private industry, asked Silicon Valley executives for assistance in working with us, and we have developed road shows and seminars to present to small business and their lawyers.

The Commission also educates businesses through projects that it calls surf days. During a typical surf day, the Commission and its law enforcement partners surf together for a few hours, searching the Internet for a specific type of problem, and after compiling a list of potentially deceptive sites, the Commission sends the operators at those sites a message. The message discusses the problem targeted by the surf day and outlines the law in that particular area.

Looking ahead, the Commission expects that old-fashioned types of fraud will continue to plague the Internet. At the same time, the Commission expects that new high-tech schemes will present new challenges. Combatting Internet fraud will be a daunting task, but we will continue to attack it with law enforcement and education, always looking for ways to turn new technology to our advantage

and ways to boost consumer confidence in this emerging marketplace.

Finally, we must consider the question of how many resources we have to deal with this problem, and the chart demonstrates something along that line. As you will see, the tall block on the screen is total consumer protection resources each year during the last 3 years. They haven't changed much at all, but our resources committed to challenging fraudulent behavior on the Internet have gone from 4 percent to 11 percent to 16 percent. Something like 53 people at the Federal Trade Commission are now working in this area.

I think we are doing as much as ought to be done. On the other hand, in order to come up with these resources, we really did have to reduce resources in other areas of our consumer protection mission. And I have no doubt that this is not the end of the growth of Internet fraud or of our response to it.

Thank you, and I would be glad to answer your questions.

Senator COLLINS. Thank you very much, Mr. Chairman.

One of the complaints that the Subcommittee has heard from consumers is there is a perception that there is, as I put it, no sheriff in cyberspace. Consumers feel that if their fraud involves only a few hundred dollars that nobody is going to pay attention to it, that Federal agencies or law enforcement officials are only interested in the big-dollar frauds.

What would be your response to that concern? Can consumers come to you if they have lost, say, under \$500? Which may be a great deal to that particular consumer.

Mr. PITOFKY. Of course. Absolutely. Let me start by saying that I think the perception that the Internet is a wild west frontier and there is no law and there is no regulation, that is one of the things that needs to be combatted, because we want consumers to have confidence in the Internet in order to see that constructive and useful marketplace grow.

Now, it is true if we see something like Fortuna, where we are talking about millions and millions of dollars of fraud, we are going to be quicker off the mark than we would be for smaller-scale frauds. But we have brought actions where relatively modest amounts of money have been defrauded away from consumers.

Jodie, do you want to add to that?

Ms. BERNSTEIN. In fact, the first five cases, I think, that the Commission brought early on were against small companies with small amounts of losses per consumer. But in total, it added up to a lot of money. That means that there was a lot of loss involved.

We did that in part to establish the Commission's jurisdiction to attack fraud and deception in this particular marketplace and because we wanted, as the Chairman said, to establish that there will be protection for consumers in this new medium.

Senator COLLINS. I would like to talk a little bit more about the Fortuna Alliance case. What is the present status of the FTC's actions against Fortuna Alliance?

Mr. PITOFKY. We challenged their behavior, and later settled the case. We are trying to get restitution for defrauded consumers. Restitution did not occur promptly, and with the help of the Department of Justice, we have pursued these people to Antigua.

That is where they are located now. And we were able to get the court to enforce an order which would require very substantial restitution to consumers.

I understand that tomorrow is the date when they are committed to pay back to consumers 60 percent of the monies that they have committed to pay back, which I think is in the range of about \$6 million. But I must tell you, until that money is in the hands of consumers, I am not prepared to declare victory here.

This is a very difficult enforcement process. They have made it difficult for us. But we are pursuing it, and we will continue to pursue it and get the money back if we can.

Senator COLLINS. It is very troubling to me that this company could pop up with the same name with just "II" after it and move its operations offshore. Does the company's ability to move offshore make it more difficult for the FTC to pursue this kind of fraudulent activity?

Mr. PITOFKY. Absolutely, and we have often seen this business of people who are caught in one place moving to another jurisdiction, changing their names, and going right back into business. We have seen that a lot in telemarketing. This is not all that unusual.

What is unusual is going across a national border because the Internet respects no borders, and when you get to these foreign jurisdictions, sometimes they have no comparable consumer protection law or it is very difficult to enforce your judgment in a foreign country. It just makes our job all the more difficult, and yet we know that that is what is going to happen more and more as time goes on.

Senator COLLINS. Isn't the company essentially violating at least the spirit if not the letter of the agreement that it reached with the FTC?

Mr. PITOFKY. We have moved for contempt against the company on grounds that they are violating the previous order.

Senator COLLINS. In a case like this, does the FTC, Mr. Chairman, consider a referral to the Justice Department for a criminal prosecution? I know you can't comment on a specific action, but—

Mr. PITOFKY. I can't. The general policy is we are increasingly thinking about these kinds of fraud, telemarketing and Internet, as deserving criminal enforcement. Some of these frauds are extremely raw. People are taken advantage of. They are injured very badly. And some of these people engaged in the fraud deserve to be treated criminally.

Ms. BERNSTEIN. Madam Chairman, in this case, we can also disclose because it is public that a Federal grand jury in Seattle has issued subpoenas to individuals associated with Fortuna, and the FBI is also conducting interviews.

Senator COLLINS. Ms. Bernstein, I notice that the victim we had who was testifying today talked about some of the customers of Fortuna Alliance actually being angry at the FTC for closing down what clearly was a fraudulent pyramid scheme. Were these customers who got in at the ground level and thus made some money before the whole pyramid collapsed? Or could you tell us a little bit about that? I thought that was just fascinating. I would think they would be grateful to you.

Ms. BERNSTEIN. Well, not only were they complaining about our conduct, I believe they complained to various Members of Congress that the FTC was interfering with their ability to be winners in this scheme.

I think the voices that were heard were people who really believed if we, the FTC, had held off for a little while longer, they would be among the early winners, and they weren't too concerned, I think, about the downstream potential victims. We believe that is what happened in that situation, and it often does in pyramid schemes.

Senator COLLINS. I noticed that you provided to the Subcommittee some terrific consumer brochures and sort of warning tips. But I have to say this is the first that I have seen these materials, which I think are excellent.

What do you do, Mr. Chairman or Ms. Bernstein, to make sure that consumers get hold of these kinds of very useful warning publications? What is your plan for distributing them?

Ms. BERNSTEIN. The first thing that we have done, obviously we have tried to move away from what used to be called government brochures that were not very readable and not very intriguing to people. We have tried to use new techniques.

Second, we formed partnerships with legitimate companies who were anxious to assist us with our consumer education. Various companies have taken on the task of distributing materials very broadly. We have over 100 companies as part of our consumer education partnership that we established some time ago.

And, third, and perhaps I should have said this first, we are on the Web with these materials. Our home page allows you to know what is available, how to get it, and you can print it out directly from the Web page.

So we are trying to use, as best we can, every technique that these fraud operators are using to get to consumers. We hope the teaser pages, particularly, are very specific, and like our previous witness said, it was one of those pages and one of our alerts that caused him to be suspicious of his investment in Fortuna.

So we are using every technique that we know of and that experts in dissemination and communication have helped us with.

Senator COLLINS. I was wondering whether it would be worthwhile trying to get some of the service providers, the Internet service providers, to include some of your publications when they sign up a new customer. For example, the "Don't get scammed" publication, the little bookmark, would be very easy to stuff in as a mailer, it seems to me.

Have you pursued that sort of idea?

Ms. BERNSTEIN. We have, and they have been very cooperative, the service providers we have worked with, AOL and the others, to be of assistance on that. And some have actually included some of our consumer education material in the billing notices. I hope it doesn't turn people off from the message when they have to pay the bill, but it is a very good device. You are absolutely right. It is a very good device for having a consumer see it at the time they are thinking about the service.

Senator COLLINS. Both Senator Glenn and I in our opening statements talked about the importance of striking the right balance

here, because the Internet really is a tremendous means for small businesses in particular, which don't have the money for large advertising budgets, to reach consumers. Yet, on the other hand, that same ease of transactions and speed and low cost are an invitation to the fraudulent person as well.

I am interested—and I will start with you, Mr. Chairman—in what specifically you would recommend that Congress do as far as new legislation in this area. Is there new legislation that is needed to make it easier for you to police the Internet or to discourage this kind of fraud? Are our current penalties tough enough? What would your recommendations be to us?

Mr. PITOFISKY. Well, let me start by saying how much I agree with what you say. There are legitimate people who are marketing on the Internet, and this new marketplace creates a great opportunity for easy entry, for good service, for information and so forth.

I think that in the long run it may very well be that Congress is going to have to act in this area, as it did with respect to telemarketing fraud so very effectively.

On the other hand, I think maybe we are just a little bit premature at this point in looking to legislation, for several reasons. One is this whole Internet marketing phenomenon is only a few years old. We are just beginning to learn about how it works, what the frauds are, who is vulnerable and so forth.

I think it is a good idea, before we move too quickly into legislation or rulemaking by an agency like this, to get a better fix on where the problems are. Also, some of these problems are unique to the Internet, like the password thefts that we talked about before.

We held several sets of hearings bringing consumer groups, industry groups, and academics together to talk about what the problems are on the Internet, and we received some pretty clear promises from the industry that, through technology or self-regulation, they thought they were capable of cleaning up a lot of the problems on the Internet.

We are going to surf the Net very broadly next month. That was a commitment we made to Congress some time ago, and we will be filing a report to Congress before the end of June of this year in which we evaluate self-regulation, in which we look carefully at what has been done and what hasn't been done, and we may be making legislative recommendations.

I heard Senator Glenn say earlier that if self-regulation doesn't happen, Congress should and likely will act, and I think that is exactly right. In that event, Congress should act. It is up to the industry at this point. They have made a lot of promises. Some people have come through in excellent fashion in proposed self-regulation programs, but we have got a long way to go. And we will be ready to report to the Congress by the end of June of this year.

Senator COLLINS. One of our witnesses earlier today, Susan Grant of the National Consumers League, made a specific recommendation with regard to the FTC's telemarketing sales rule, and she proposed that it be expanded to cover promotions via the Internet and online services so that Federal and State prosecutors can go into Federal court to take action on interstate violations.

Do you agree with that recommendation? What is your reaction to that specific proposal?

Mr. PITOFISKY. Two reactions. One is, again, I think we are a little ahead of where we ought to be. The telemarketing sales rule, first of all, wouldn't fit exactly for some of the Internet problems that we see. On the other hand, my second reaction is the best thing about the telemarketing sales rule is the way Congress adopted the rule—or adopted a law, authorized us to promulgate a rule, and then allowed not only the Federal Government but State officials to go into Federal court to enforce that rule. That has led to an extraordinary level of cooperation, and I think some success in challenging telemarketing fraud.

So I think if there is to be legislation, it ought to be along that model. As to what the exact provisions ought to be in dealing with Internet fraud, I think we ought to allow a little more time to pass to see how self-regulation works and have a little more experience with what the frauds are.

Senator COLLINS. Thank you.

Senator Glenn.

Senator GLENN. Thank you, Madam Chairman. Sorry I was a little late getting back. I got tied up over there on the floor.

Do you think the ISP's should be required to screen commercial sites more carefully? I presume you believe that that is a starting point, at least.

Mr. PITOFISKY. I do, and we have urged them to do so.

Senator GLENN. Should they be required to report customer complaints to FTC?

Mr. PITOFISKY. I don't know about—well, require. They do now. We received many of our complaints from the service providers. I think they are well advised to do that. But I think for the most part they are doing that.

Senator GLENN. There are two pieces of legislation that have been introduced that deal with unsolicited commercial E-mail. I have not looked in detail at those. Have you looked at those? And do you favor either one of them, or do you have some suggestions how we could either use those as a basis for legislation or should we be putting in separate legislation or let well enough alone right now?

Mr. PITOFISKY. Well, I think spam, unsolicited E-mail, is a real problem, in part because we—there are probably certain kinds of spam that are injurious, and yet we can't reach it under our statute.

We can challenge the kind of unsolicited E-mail that contains some deceptive content to it: False return address, false claims within the four corners of the presentation. But if it is just straight spam, I am not at all sure that we can get at it. And unless self-regulation—again, we have had all these promises that self-regulation and technological fixes would do the job. Unless it does, I think Congress would and will become involved. But I haven't looked at these two bills.

Senator GLENN. Is this akin to junk mail that we get in our mailbox every day? And we haven't learned how to regulate that. We do have laws for truth in advertising that cover that. Now, should those same laws be extended here, or do they already apply?

Mr. PITOFSKY. Oh, they already apply, and we would enforce that law. But, yes, it is junk mail raised to a higher power. We are talking about a million people who may get this kind of unsolicited E-mail at a very cheap cost to the sender.

Senator GLENN. Could the ISP's levy extra fees on those who want to send unsolicited E-mail?

Mr. PITOFSKY. I think they could. I heard the testimony earlier that they have no intention of doing do. I don't know exactly where that stands as far as what their policies are.

Senator GLENN. What do you need to more effectively fight Internet fraud? Do you need more people? Do you need more resources? You need what?

Mr. PITOFSKY. Well, I am glad you asked me that question, Senator.

Senator GLENN. We did not have that arranged in advance, I would add. [Laughter.]

Mr. PITOFSKY. There is a chart that I mentioned earlier in my testimony. The red block is our appropriation across the board for consumer protection. The green block shows that we are now spending four times as much of our resources, 16 percent of our total consumer protection resources, on Internet monitoring and regulation, and we know that that block is going to continue to grow.

I think we can cover our responsibility right now, but the way things are going, two things are happening. One is we are robbing Peter to pay Paul. We are taking resources away from other valuable activities in order to cover the Internet. And, second, that block is going to grow, and I think if we are to address Internet problems, we are going to need more people and more money.

Senator GLENN. You heard us earlier—I know you were in the room—when we talked about America Online and some of the other companies that were hauled up and after due course made a settlement of some kind with the FTC. They were three of the largest and supposedly most reputable ISP's.

Do you have any estimate of how much the consumers lost because of improper practices of either of those three or in general across the board?

Mr. PITOFSKY. I don't. And, incidentally, that case is not yet final, so let me—I would be limited in what I can say about it. But let me make two points about that.

One is that we jumped into that matter very early in the game. I don't think that behavior was going on too long before we learned about it from a very wide variety of consumer complaints. And, second, my recollection is that the companies, as soon as we started our investigation, abandoned the practices. They didn't wait for us to complete our enforcement action.

And so we settled with an order that required them to discontinue the four practices that you mentioned earlier this morning and also commit some money for consumer education. But as to getting money back for consumers, I don't have an estimate as to how much money was involved there.

Senator GLENN. Have we made any effort—the Fortuna case is one that just sort of pops out at me, Mr. Wise—Barry Wise is still in the room and let me just say for the record here, Barry, I admire

your coming forward, and I hope that your company gives you full credit when you get back home for being honest enough to come up here and I think they are to be commended for letting you come up here and testify on these matters today, because it is too easy to get a scam and say I am ashamed of what I did in this and just clam up. And you have got guts enough to come up and testify before a Senate Committee and say where you got scammed and admit it and hopefully prevent this from hurting other people. And your company was willing to let you come up and make that kind of testimony, and I think both the company and you are to be given a lot of credit for being willing to do that. If we had more people willing to come forward instead of just covering up things like this, why, it would be a big help toward getting some eventual solution to this. So I want to compliment you for coming up this morning.

But what happened with Fortuna that Mr. Wise testified about was the company got whacked, and so they just go offshore, and they have got the same thing going again and didn't even change the name, now Fortuna Alliance II, and even the parentheses, "TM," which I guess means trademark, which is the ultimate insult, I guess. I presume that is what it means. I don't know.

But how are we going to get into this? Because we have got people on the Internet now from all over the world, you can have people operating out of any little country that has no regulation whatsoever. They could be set up in some place that doesn't even have much business law or whatever. And yet they are just as much a scam on the international Net as anybody else.

How are you going to address that? Are there any plans to hold some international organization or conference that addresses this and tries to get agreements with other nations? It is a very tough problem you are up against here. How are you going to deal with the international aspects?

Mr. PITOFSKY. It is one of the most serious problems, and it is going to grow as time goes on.

I think long term—I am going to ask Ms. Bernstein to address this because she has negotiated with some of these foreign countries. But I think long term we are going to need bilateral agreements with countries like Canada and the E.U., Australia, Mexico, and so forth. The kind of agreements that we have begun to develop in the antitrust field, we are going to have to expand that to consumer protection so that we can get some help.

The problem isn't identifying the crooks. The problem is when you have identified them and you know what they have done, bringing an enforcement action that can be enforced in a foreign country is where the difficulty is.

Now, Jodie, do you want to add to that?

Ms. BERNSTEIN. Yes. At least in connection with our relationships with Canada, we have had a good deal of success in establishing bilateral relationships already, sharing data with them, pursuing joint actions and so forth. We really have a very good working arrangement with them because the first sign of movement was initially into Canada or Canadians coming here in order to escape either country's laws. And that sets a good model for us, at least initially, because we are part of a joint law enforcement initiative, in addition to which a committee, an international com-

mittee, has been set up—I think it was a couple years ago, maybe a year and a half—called the International Marketing Supervisory Network, in which we were trying to work as other international organizations have, to extend that international—extend the law enforcement Network to other countries as well so that we can quickly alert each other and work together to try to pursue this.

It certainly is a long way from being in completion, but at least we have an organization that we have been participating in with other countries at the same time.

Senator GLENN. Fortuna, though, is a good example. I understand they are operating now out of Antigua. Is that correct?

Ms. BERNSTEIN. Right.

Senator GLENN. Well, that would just show they could be in Antigua, they could be in Burma, they could be on an island, in Diego Garcia. They could be anywhere in the world, almost.

Ms. BERNSTEIN. Well, we did have some success in working through the Justice Department in Antigua, and the courts down there, after we, through the Justice Department, had local counsel retained, which is required by law down there, to be able to pursue them there. The courts down there have been quite—very supportive of reaching them in Antigua.

Senator GLENN. Just as a last statement, Madam Chairman, I am not quite as optimistic about this self-regulation as you indicated you might have hopes for. It hasn't worked with banks, SEC, auto dealers, doctors, lawyers, you name it. We have laws all over the place. In fact, our whole body of regulatory law in this country is based on the fact that people are not operating under the golden rule, not operating under fairness, and so we have to have some sort of regulation.

This is such a tough one to get your arms around that I don't know where you go with it. But I will pledge you my support for what time I have left in the Senate here the rest of this year. Mr. Pitofsky, I don't know whether it is possible to do this or whether you people at the FTC are over there like the little Dutch kid with the finger in the dike. You are just waiting for the dam to burst in some way over there and that we are at that stage of this whole thing right now. I think you do need more resources than you are probably going to get to deal with a problem of this magnitude. But it is a tough one, and I hope we can be working with you on this and that you will keep us advised on what you think is necessary so that we can give you the maximum support possible.

It is never pleasant to have to come up and appear at a hearing and answer a lot of questions. I know that. But we are really all working together on this thing, and we have one part of the puzzle here. If we can put it together to help you, that is what we want to do.

Thank you.

Senator COLLINS. Thank you, Senator.

Mr. PITOFSKY. May I just—

Senator COLLINS. Yes.

Mr. PITOFSKY. I don't want to be misunderstood here. I completely agree with you that self-regulation is going to be difficult here. We have heard many promises. We have had some constructive evidence of moving forward, but not a great deal.

My own view is that if self-regulation doesn't work after all those promises, that is all the more reason for Congress to step in aggressively in this area.

Ms. BERNSTEIN. The Chairman has also made clear that any self-regulatory mechanism that they propound will have to have a strong enforcement mechanism so that we can monitor it and the public can monitor what the effects of self-regulation are.

Senator COLLINS. Mr. Chairman, in one of my previous incarnations, I was a commissioner in State government in charge of the department that had a broad consumer protection mandate and included securities regulation. As I am listening to the testimony today, it strikes me that there are a lot of cross-jurisdictional issues right within our own country, and I am interested in whether or not there is good cooperation with State and local law enforcement officials, but also whether you have considered some sort of interagency task force. The SEC obviously has a role in the area of securities fraud being perpetrated over the Internet.

What is the status of cooperative efforts such as those?

Mr. PIROFSKY. On the Federal-State front, I would say the cooperation is better than anything we have seen before. It is outstanding. We work constantly together. Congress, as I said, made a very good call here by allowing States and the Federal Government to enforce laws in this marketing fraud area.

Now, we are all short of resources, but we certainly maximize our resources and leverage our resources, I should add that the FBI, the Department of Justice, the SEC and others are active in this area.

At the Federal level, you are absolutely right. There are some overlaps here. There is some gray area. There are some cross-lines. In specific areas, there are groups that are working together. For example, we hardly have mentioned privacy considerations today, and yet they are going to influence profoundly the willingness of consumers to buy products on the Internet.

We have a good working group going with respect to privacy. I think we have a ways to go, and I think more coordination at the Federal level will occur as time goes on.

Senator COLLINS. Finally, I want to turn to one aspect that we haven't discussed today, and that is, we have talked a lot about the cyber crooks, if you will, the people who are deliberately, intentionally defrauding individuals. But I suspect there is also a category of online fraud that occurs that is undertaken by people who are just ignorant of the law or who are very unsophisticated, think that they have come up with a scheme that is legitimate, when, in fact, it is downright illegal.

When you do your surveillances and visits to Web sites, how much is that a problem, of an unsophisticated person putting together a scheme that is, in fact, illegal and yet the person is unaware of that?

Mr. PIROFSKY. They don't have a large law firm and a general counsel to advise them. That is exactly right. We see a lot of it. And I think what we are trying to do is to get back to some of these people and let them know that they are on thin ice, they are in an area where they may be approaching or have stepped over the line with respect to fraud.

I am going to ask Ms. Bernstein, again, because she is responsible for developing a program of advising the small business community about this. I will ask her to develop the point.

Ms. BERNSTEIN. Thank you. We have actually conducted what we call surf days, eight surf days on different fraud topics over the last couple of years, and the purpose of it, Madam Chairman, really was to do exactly what you have referred to, because we know there are a lot of small entrepreneurs and others who aren't—some of them, we think, have never heard of the FTC, leave alone that there is a law against deception or false advertising.

So what we do is join together with States and other law enforcement folks, look at the surf in a block of time, say, for example, the first one we did was on pyramid sites, gather them up, and then those that we believe have violated the law, we send warning letters to saying: You may not be aware that your practice here violates Federal law, etc., and we are going to give you a chance to basically clean up your act. And then we go back and surf after 30 days.

On the very first one, we found when we went back that 18 percent of the sites had improved or had taken them away entirely in 30 days. Others in business opportunities, almost 25 percent either disappeared or had cleaned up what they were proposing and so forth.

We have done eight of them, one on credit repair, get-rich-quick schemes, and the last one we did was what we called our false spam harvest. We sent out 1,000 letters to fraudulent, unsolicited E-mail communicators with the same purpose in mind. We just did that last week. Interestingly enough, they didn't give us their E-mail address, so we had to send it by "snail" mail. But we will be following through on that, and that was a very aggressive kind of program that we have put in place to try to get that, to clean up that part of a new type of business.

Senator COLLINS. Senator Glenn, do you have any further questions?

Senator GLENN. I just have a couple to wrap up, Madam Chairman, if I could.

In your testimony I believe you testified that you have brought about 25 civil cases, I think.

Mr. PITOFKY. That is right.

Senator GLENN. Let me just run through this. You had 25 civil cases. Were those all done within the FTC itself, or did you refer those to Justice?

Mr. PITOFKY. Oh, no. These are FTC cases, although in most instances we went to court. We didn't enforce it within the administrative process.

Senator GLENN. OK. But you have your own counsel and your own staff of people there to do this on civil cases.

Mr. PITOFKY. We do.

Senator GLENN. I presume that on criminal cases you have to go through Justice; is that correct?

Mr. PITOFKY. We refer those to the Justice Department.

Senator GLENN. And have you done any of that? Have you referred criminal cases to Justice?

Mr. PITOFKY. Well, this Fortuna case—

Senator GLENN. That was a criminal case.

Mr. PITOFSKY. Yes. I don't think we have had any other criminal cases with respect, narrowly, to Internet fraud thus far.

Senator GLENN. Do we have any extradition agreements with other countries that cover this?

Mr. PITOFSKY. I think we do not, but I would have to check on that and find out.

Senator GLENN. Do you know?

Ms. BERNSTEIN. I don't know, Senator.

Senator GLENN. And my follow-up to that was going to be has it ever been exercised. If so, how many have we extradited?

That may be an area where we could help out some on this. Since the con artists are moving, shuffling off to other countries when they have a problem in this country, that may be an important area that we could help on as far as getting extradition agreements and things like that. So if you could furnish that for the record, we would appreciate it.

Thank you, Madam Chairman. I think it has been a good hearing this morning.

Senator COLLINS. Thank you very much, Senator Glenn.

Each of the witnesses that we have heard from today have emphasized a common theme, and that is that we need to do more to educate consumers so that they can distinguish more easily between fraudulent offers on the Internet from legitimate offers. We don't want to stifle legitimate commerce, and yet we do want to take steps to protect the consumer who may be out there with very little guidance on what is a fraudulent scheme.

We also need to make certain that consumer complaints in this area are vigorously pursued and that agencies like the FTC have the tools needed to do the job. In that regard, I would invite you, Mr. Pitofsky, and your staff to continue to work with the Subcommittee on legislative or regulatory reforms when the appropriate time comes and to share with us the report that you mentioned that will be available in June.

I also want to echo Senator Glenn's commendation of Mr. Wise for coming forward today. It is never easy to come forward and concede that you were ripped off, but it was his testimony that allows us to understand that even a sophisticated consumer can be taken advantage of. And he has done, indeed, a great public service.

Finally, I want to thank Susan Grant and America Online and other witnesses today for sharing their information as well. We hope to build on these hearings to further the consumer education efforts we are all involved in and also to identify legislative reforms that may be needed.

I finally want to thank my staff for their hard work on this hearing. Rena Johnson, Tim Shea, and Kirk Walder all worked very hard, as did the rest of the staff and the minority staff as well. We will be continuing hearings into this area, and we look forward to continuing to work with you.

Senator COLLINS. The Subcommittee is now adjourned.

[Whereupon, at 12:27 p.m., the Subcommittee was adjourned.]

A P P E N D I X

**Fraudulent Schemes on the Internet
Remarks to the Senate Permanent Committee on Investigations
by Susan Grant
Director of the National Consumers League's
National Fraud Information Center/Internet Fraud Watch Programs**

February 10, 1998

On behalf of the National Consumers League, the oldest nonprofit consumer organization in the United States, I am pleased to provide the Senate Permanent Committee on Investigations with information about the newest frontier of consumer fraud -- the Internet. The League has advocated for fairness in the marketplace since its founding in 1899. Some of the scams we see on the Internet, such as pyramid schemes, are as old as the League. Others are more recent, springing from advancements in technology that have created new types of products and services.

Fraudulent promoters always seize the same opportunities as legitimate companies to use new ways to reach consumers. The challenge before Congress, law enforcement agencies, and consumer groups such as the League is to protect the public from abuse while ensuring that the Internet realizes its full potential as a means of communication and commerce.

NCL's Initiatives to Combat Internet Fraud

To meet that challenge, in February of 1996 the League created the Internet Fraud Watch. It operates in tandem with our National Fraud Information Center, which was set up in 1992 as a toll-free hotline that consumers could call for advice about telephone solicitations and to report telemarketing fraud. Now consumers can get tips on avoiding both telemarketing or Internet scams and report those types of fraud through our web site, www.fraud.org, or by calling the

hotline at 1-800-876-7060. Though the web site was launched only two years ago, we have had more than 5 million visitors to date.

Every week, the National Fraud Information Center and Internet Fraud Watch programs receive an average of 1,500 calls and an equal number of e-mails, plus dozens of letters. Most of the consumers who contact us are seeking advice about solicitations they have received. While we do not provide the public with information about specific companies, we do help people identify the danger signs of fraud. By doing so we prevent them from becoming fraud victims.

We also take reports from consumers about possible telemarketing or Internet fraud and relay them to a variety of federal, state and local law enforcement agencies in the United States and Canada. Our data system uploads new reports daily to an electronic database maintained by the Federal Trade Commission and the National Association of Attorneys General. In addition, the system automatically faxes consumers' reports to over 160 individual agencies according to preset criteria. In essence, we provide an early-warning system for law enforcement agencies, alerting them to scams they may wish to investigate and supplying them with information about potential witnesses.

At the same time, we are assisting consumers who have been victimized by routing their fraud reports to the myriad and often confusing array of agencies that may be appropriate to receive them. There is no charge for the consumer or law enforcement services that we provide. These programs are sustained by the members of the National Consumers League and by charitable donations from foundations, corporations and trade associations that are concerned about the integrity and safety of the Internet.

A Snapshot of Internet Fraud

Since no other organization, private or public, acts as a central point for collecting reports of scams in cyberspace, the National Consumers League is in a unique position to offer the Senate a snapshot of this emerging problem. No one knows the full extent of Internet fraud. Not all victims contact our Internet Fraud Watch program; some go directly to their state attorneys general or other law enforcement agencies, others to private attorneys, and many consumers probably do not report the crime at all. However, we do know that we are hearing from more people than ever before.

E-mail inquiries have increased ten-fold since the inception of the Internet Fraud Watch program and reports of possible Internet fraud have tripled, from an average of 32 per month in 1996 to nearly 100 per month in 1997. While the 1,152 fraud reports we received last year are just the tip of the iceberg, they present a revealing picture of the types of scams that are proliferating on the Internet and how they work.

Top Ten Subjects of Reports to Internet Fraud Watch 1997

1. **Web Auctions** - items bid for but never delivered by the sellers, value of items inflated, shills suspected of driving up bids, prices hiked after highest bids accepted;
2. **Internet Services** - charges for services that were supposedly free, payment for online and Internet services that were never provided or falsely represented;
3. **General Merchandise** - sales of everything from T-shirts to toys, calendars to collectibles, goods never delivered or not as advertised;
4. **Computer Equipment/Software** - sales of computer products that were never delivered or misrepresented;

5. **Pyramids/MLMs** - schemes in which any profits were made from recruiting others, not from sales of goods or services to the end-users;
6. **Business Opportunities/Franchises** - empty promises of big profits with little or no work by investing in pre-packaged businesses or franchise operations;
7. **Work-at-Home Plans** - materials and equipment sold with false promise of payment for piece work performed at home;
8. **Credit Card Issuing** - false promises of credit cards to people with bad credit histories on payment of up-front fees;
9. **Prizes/Sweepstakes** - requests for up-front fees to claim winnings that were never awarded;
10. **Book Sales** - genealogies, self-help improvement books, and other publications that were never delivered or misrepresented.

Other prevalent scams reported to the Internet Fraud Watch in 1997 included bogus investments, empty travel and vacation offers, scholarship search services, loans that required advance fees and never materialized, dubious claims for health products and services, foreign lotteries, even services to supposedly help immigrants obtain green cards. The common elements of these scams are: requests for advance payment from sellers with whom the consumers are not familiar, who were usually located in another state, or even another country, and who have made exaggerated claims or false promises concerning the goods or services they offer.

I should note that obviously there are many legitimate offers on the 'Net for goods through auctions, multilevel marketing distributorships, Internet services, and other products and services. That is precisely why it is so important to be aware of fraud and to deter it.

Con Artists on the 'Net

Scams can be found everywhere on the 'Net -- on flashy-looking web sites, in online classified ads, in unsolicited e-mail, in newsgroup postings and in chatrooms. For example, last year the New York Attorney General prosecuted Kevin Jay Lipsitz for consumer fraud in connection with unsolicited e-mails sent to consumers, supposedly from fellow participants in newsgroups, touting his great prices and service for magazine subscriptions.

Those testimonials turned out to be fictitious, sent by Lipsitz himself to drum up business. Furthermore, his real customers, many of whom contacted our Internet Fraud Watch, never got the magazines they paid for.

The Federal Trade Commission has also used information from the Internet Fraud Watch and other sources to take action against web site operators promoting pyramids and other illegal schemes. In one interesting case, the FTC halted a "Trojan horse" scam in which consumers who thought they were downloading a free program from a web site to view pictures were unwittingly disconnected from their regular Internet service providers and reconnected to the Internet through a telephone number in Moldova, resulting in huge international phone bills. The perpetrators of the scheme were actually located in New York. Our Internet Fraud Watch was the first to receive reports of this scam and issue a general warning to the public.

Another Internet case brought by the FTC concerned the Fortuna Alliance, a pyramid scheme in which consumers were promised they would net at least \$5,000 per month if they paid an initial fee ranging from \$250 to \$1,750 to hire the company as their "personal marketing expert." Subsequent monthly fees would be deducted from the profits that would supposedly come from others joining the program. To that end, Fortuna supplied members with

promotional materials to use in recruiting others. The fact that it was an unsustainable pyramid was masked by the use of a complex mathematical formula showing how profits would be distributed. However, because pyramids must rely on an infinite number of new recruits, they invariably collapse, leaving only the originators to profit and the vast majority to lose. The defendants transferred their ill-gotten gains to a bank in Antigua.

The Internet is ideal for abuse because anyone can put up a handsome web site, as Fortuna did, making it difficult to distinguish fraudulent promoters from legitimate ones. The Internet also makes it possible to send e-mails to thousands of people at once at relatively low cost. Moreover, it is easy to post information in newsgroups or to lurk in chat rooms, offering phony stock tips or money-making opportunities. Return addresses can be masked to make them look like they are coming from one place when they are really coming from another. For instance, Kevin Lipsitz used a variety of return addresses to make it appear that his e-mails were from various individuals. Thus it is relatively easy for cyber crooks to hide their real identities and locations.

Furthermore, geographic boundaries are meaningless in cyberspace. Crooks targeting citizens in the United States may be based in Australia, Hong Kong, Malaysia, South America, the Caribbean, Europe -- all over the globe. As you can see from our chart showing the top 20 locations of fraudulent Internet operators in 1997, countries other than the United States or Canada ranked 12th. Con artists were also lurking in Ontario (ranked 13th) and British Columbia (ranked 20th). As in telemarketing fraud, California, Florida, Texas and other sunshine states are also popular roosts for cyber crooks.

New technology that makes it possible for legitimate vendors to offer new products and services also facilitates Internet fraud. For instance, the Moldova case illustrates how computer

programs can be devised to hijack consumers' Internet service and how telephone switching and billing systems can be used for fraudulent purposes.

Problems with web auctions also demonstrate how the ease of communicating via the Internet can be abused. These auction sites enable sellers to offer their wares at very low cost and buyers to bid for them without having to be at a physical auction location. The problem is that it is difficult for consumers to ascertain who the sellers really are, whether they actually have the items they are advertising, and whether those items are accurately described. There is no preview where potential buyers can physically examine the goods, nor can the auctioneer vouch for their authenticity. Many of the sellers appear to be private individuals, and it is possible that some are not bent on fraud but simply do not understand the need to represent the items they are selling accurately and fulfill their contractual obligations promptly. We suspect that others may be posing as private individuals when they are not, since we have seen the same sellers' names in multiple fraud reports. As the Internet opens the doors for honest individuals and small companies to participate in the new marketplace in cyberspace, it also provides ready access to those with fraudulent intent.

Internet Fraud Victims

Victims of Internet fraud can be also be found everywhere in the United States, as well as in other countries. In our chart showing the top 20 locations of consumers who reported scams to the Internet Fraud Watch in 1997, the states with the largest populations tend to rank highest, but we also heard from numerous consumers in countries outside of the United States and Canada, ranking 8th on the list.

In July of 1997, we made programming changes to our system to track the ages of consumers reporting fraud. Not everyone agrees to provide that information, but from those who have, we know that Internet fraud touches people of all ages. While most of the consumers who reported Internet fraud to us last year were in their thirties, forties or fifties, as the pie chart shows, we have heard from youngsters of 17 and seniors of 78.

Methods of Payment in Internet Fraud

Consumers pay for goods and services promoted through the Internet in a variety of ways. As the graph shows, checks and money orders were the most common methods of payment, but alarmingly, cash ranks 4th. In one scam reported to the Internet Fraud Watch last year, consumers received unsolicited e-mails offering loans of \$59,000 that never had to be paid back. The catch was that they had to send \$20 in cash to a Las Vegas address. The solicitation specifically stated that any other form of payment would be returned to the sender. To our trained eyes, the promotion appeared to be a combination of advance-fee loan and pyramid scheme, where each person would supposedly get a loan once enough people paid their \$20 into the program. Cash payments are often requested for cable television descramblers, adult videos, and other types of purchases that consumers may wish to make anonymously. Of course, cash payments also enable con artists to maintain anonymity and make it difficult to document fraud.

Telephone bills, ranked 5th in methods of payment, reflect the Moldova case, in which the charges for viewing the supposedly "free" pictures were assessed as international calls on victims' phone bills.

In cases where consumers did not provide the payment methods or where they reported attempted fraud but did not yet pay, the method of payment is listed as unknown. Relatively few people reported paying by credit card, which is ironic considering the fact that consumers have more protection in the event of fraud, deception or nondelivery under their legal dispute rights with credit card purchases than they do with other payment methods.

For this reason, we encourage consumers to use their credit cards whenever they make significant advance payments for goods or services, regardless of the medium used to promote them. It should be noted that we do not have information about how many consumers are actually making their payments online, but judging from the fact that checks, money orders and cash payment rank so high and that credit card payments could be made either online or offline, we must conclude that most transactions are consummated by mail or telephone.

Meeting the Law Enforcement Challenges Posed by Internet Fraud

As a global medium for communication and commerce, the Internet poses great challenges for law enforcement agencies. As has been alluded to before, it may be difficult to identify and locate the perpetrators of fraud. It may be even more difficult to prosecute them and to seize their ill-gotten gains. In cross-border cases, jurisdictional problems, such as the inability of the Federal Trade Commission to legally share information about investigations with agencies in other countries and the difficulty of obtaining search warrants, freezing assets and taking other legal actions in foreign courts are real impediments to law enforcement. Furthermore, the expense to send investigators and to transport defendants and witnesses can be prohibitive.

These problems must be addressed if cyberspace is to be a safer place for advertising and commercial transactions. While most state and federal laws against unfair and deceptive acts and practices apply to online and Internet promotions, the Federal Trade Commission's Telemarketing Sales Rule does not.

We believe that the Telemarketing Sales Rule should be expanded to cover promotions via the Internet and online services so that federal and state prosecutors can go into federal court to take action on interstate violations. It would also aid enforcement efforts if the enabling statute was amended so that states could sue in federal court when either the defendants or the victims are located within their jurisdictions. Currently, jurisdiction is victim-based.

In addition, federal law should be changed to make it easier for agencies in this country to share information with those in other countries and take legal action across borders. A funding pool should also be established to help state and federal agencies bring those actions. Moreover, government support for the law enforcement services that organizations such as ours provide would also be helpful in the continued fight against Internet fraud.

Preventing Internet Fraud

While clear legal ground rules for Internet promotions and good law enforcement mechanisms are crucial, public education must be a major component of any effort to curb Internet fraud. Consumers need to know how to check out the offers they see and the companies that make them. They need to learn how to identify the hallmarks of fraud in this new medium, how to protect their privacy, and what payment methods are safest. And in light of the fact that many private sales are occurring through auction sites, online classified ads, newsgroups and chat

rooms and that private sales are not usually covered by the same consumer protection laws and remedies that apply to sales by businesses, consumers must be educated about the ramifications of different types of transactions.

Businesses and individuals that use the 'Net to promote their goods or services must also be educated about their basic responsibilities. The National Consumers League has taken a lead role in educating the public about Internet fraud. One way we are doing this is by using the very same medium -- the Internet. Last September, we announced that we had remodeled our National Fraud Information Center web site. Among the improvements is a new Internet Fraud Watch section, which consumers can access directly at <http://www.fraud.org/ifw.htm> to find a wealth of free information on safe cybershopping and how to avoid fraud. The web site also has articles about enforcement actions and links to government agencies, the Better Business Bureau's BBBOOnline program, and other resources.

The National Consumers League also works with the private sector in coalitions such as the Online Public Education Network, Project OPEN. In partnership with the Interactive Services Association and major Internet and online service providers, we have produced materials for consumers on subjects such as privacy in cyberspace and unsolicited e-mails. By encouraging consumers to guard their privacy on the Internet and helping them sort out legitimate e-mail messages from fraudulent ones, we can reduce the potential for their becoming victims of scams in cyberspace.

Government must be a major partner in this effort as well, by helping to fund educational programs and lending other types of support. The contributions that we have received to help sustain the League's Internet Fraud Watch program from Bell Atlantic, Direct Selling

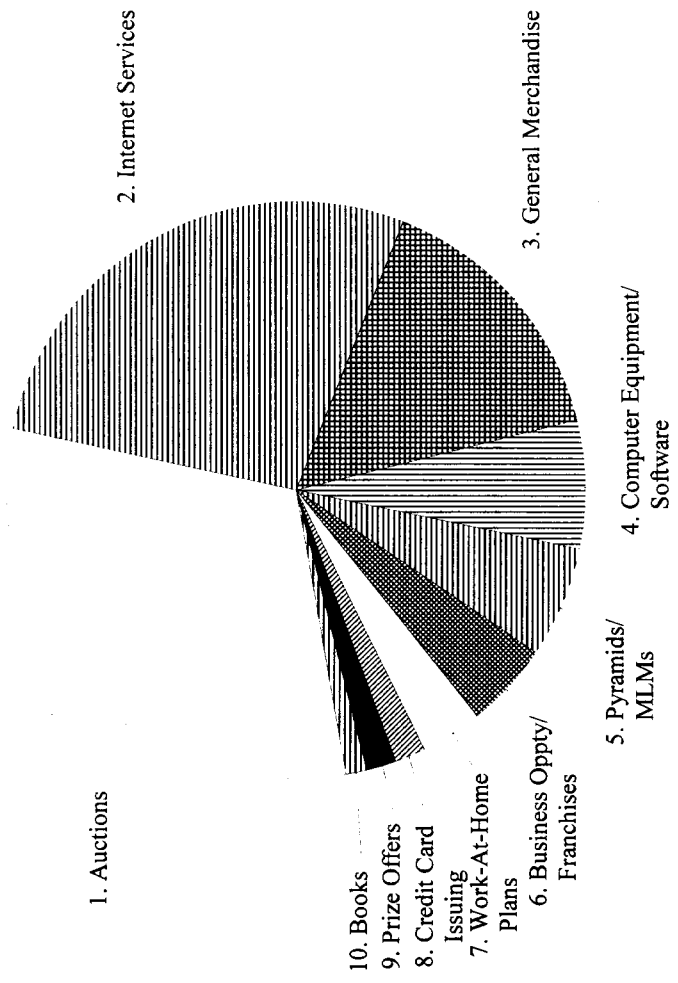
Association, MasterCard International, MCI and NationsBank do not cover the costs of the law enforcement services or public education we provide.

Copies of charts and graphs illustrating the 1997 Internet Fraud Watch statistics are appended to our written testimony. We applaud the Senate Permanent Subcommittee on Investigations for focusing attention on the emerging problem of Internet fraud and look forward to working with Congress and others concerned with making cyberspace a safer place for communication and commerce.

Respectfully submitted by:

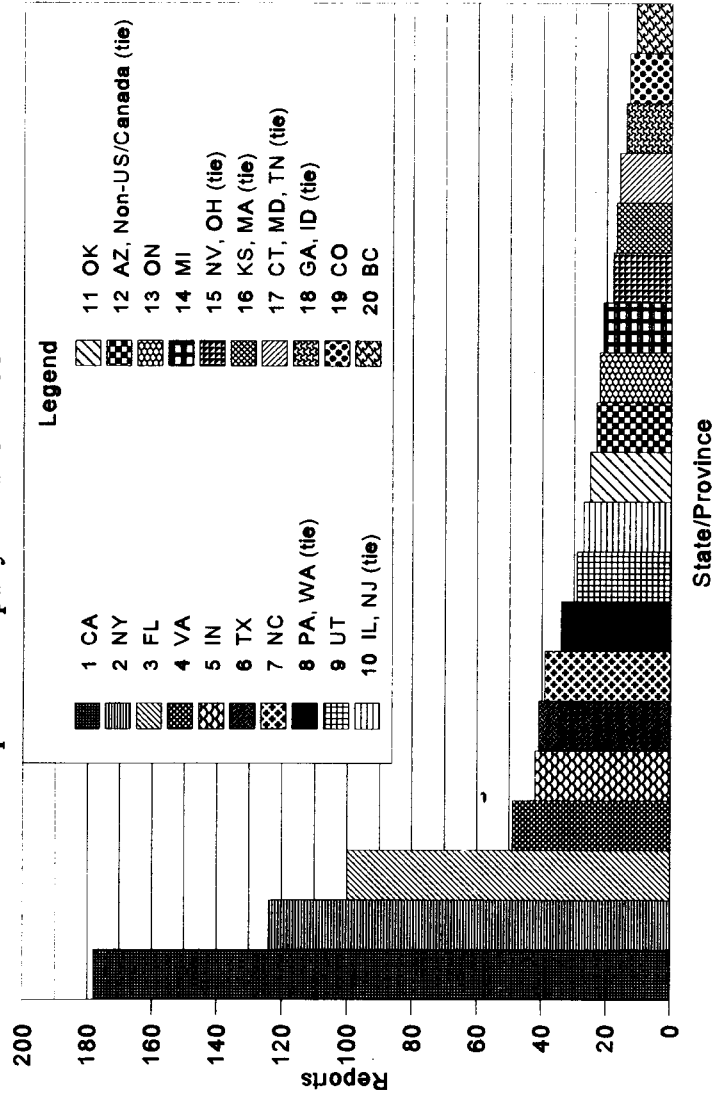
Susan Grant, Vice President for Public Policy
Director, National Fraud Information Center/Internet Fraud Watch Programs
National Consumers League
1701 K Street NW, Suite 1200
Washington, DC 20006
(202) 835-3323

National Consumers League Internet Fraud Watch Top Ten Frauds - 1997



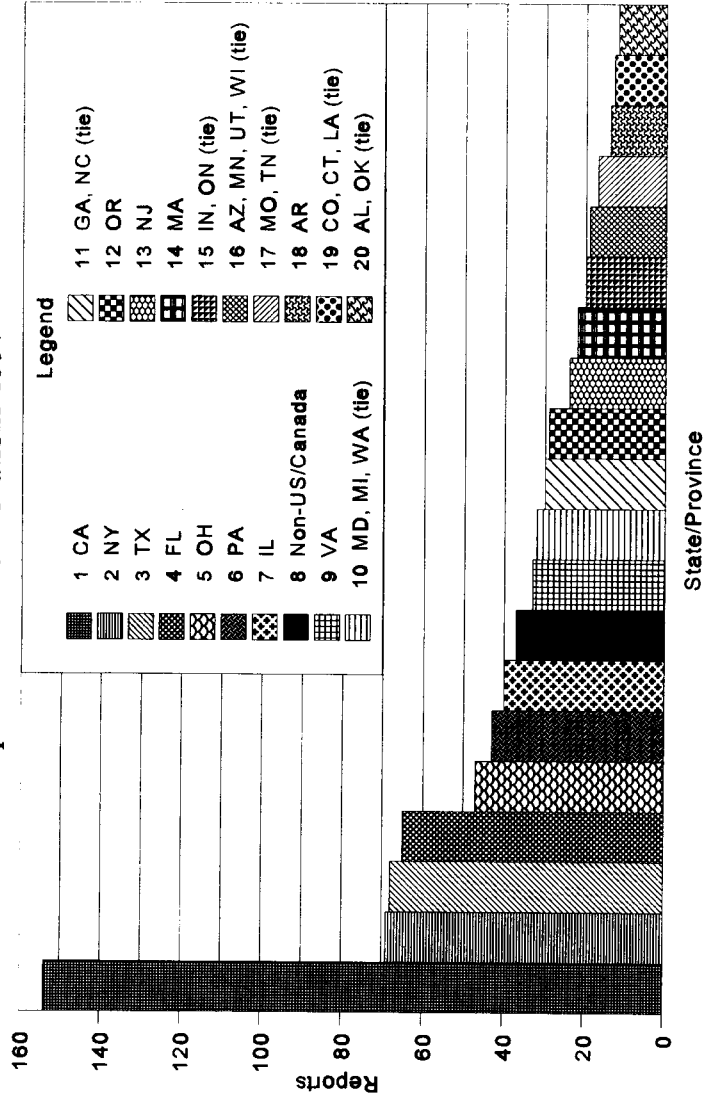
NCL Internet Fraud Watch

Top 20 Company Locations 1997

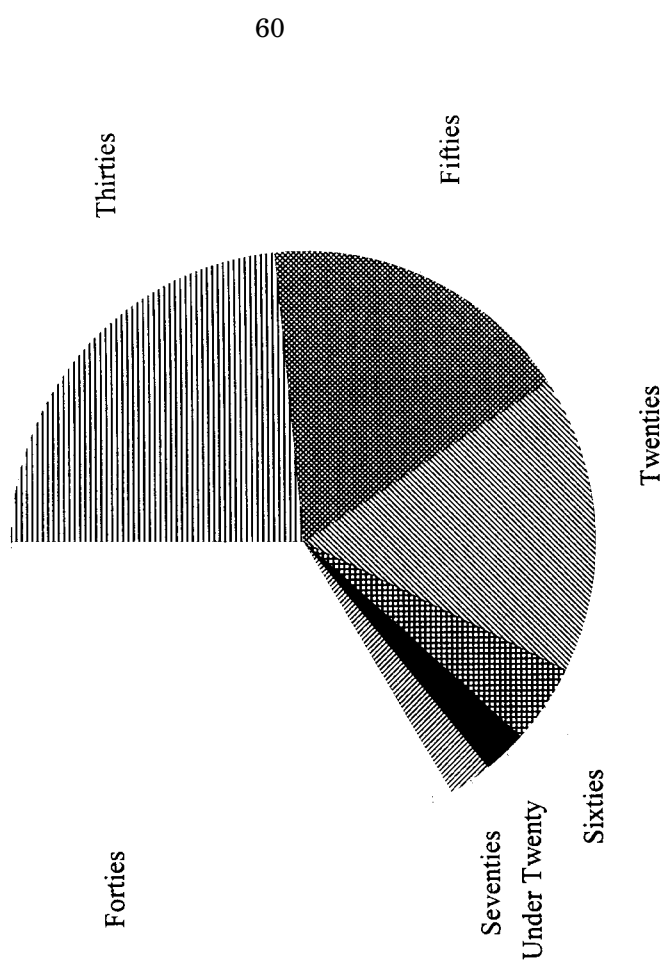


NCL Internet Fraud Watch

Top 20 Consumer Locations 1997

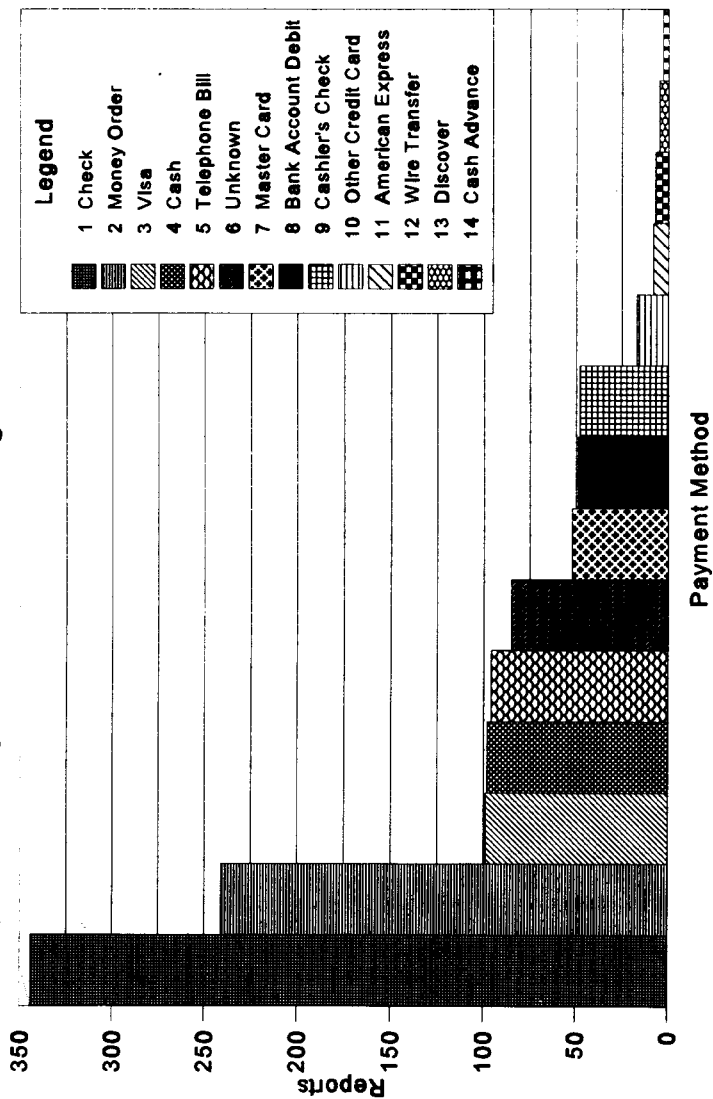


National Consumers League Internet Fraud Watch
Age of Consumers Reporting Birth Date, July - December 1997



NCL Internet Fraud Watch

Payment Method Ranking 1997



**TESTIMONY OF TATIANA GAU
VICE PRESIDENT, INTEGRITY ASSURANCE, AMERICA ONLINE, INC.,
BEFORE THE
UNITED STATES SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
COMMITTEE ON GOVERNMENTAL AFFAIRS
FEBRUARY 10, 1998**

**Susan M. Collins, Chairwoman
John Glenn, Ranking Minority Member**

SAFETY AND SECURITY IN CYBERSPACE

Thank you Madam Chairwoman, Ranking Member Glenn, and distinguished members of the Subcommittee. My name is Tatiana Gau, Vice President of Integrity Assurance for America Online. Founded in 1985, America Online is the largest Internet online service provider with over 11 million members.

I appreciate the opportunity to appear before you today to discuss how the Internet industry is working to promote online safety and security and fight Internet fraud and abuse. Thank you for providing this forum to bring these important issues before the public.

At AOL, we are focused on preventing online fraud on many fronts. To give you some insight into these initiatives, my department's mission is as follows: from logon to logoff, AOL Integrity Assurance manages all of the company's safety and security measures in order to ensure the integrity of our member experience.

The prevention of Internet fraud and the promotion of online security are critical to cyberspace consumers and to the future development of all interactive media. We believe that the principles of education, prevention and cooperation are key to these efforts. Identifying and

tackling Internet fraud and educating all consumers on how they can protect and enhance their online experience is our goal. Therefore, we need to inform consumers on how to protect themselves, prevent purveyors of fraud and promote cooperation of the industry and with law enforcement.

In discussing this critical topic, it is important to keep in mind the vast potential benefits that this medium offers. As a medium without borders, cyberspace is a powerful tool for bringing the world closer together, for understanding other cultures, and for engaging in commerce.

The Internet can help people stay in touch with family, friends, and colleagues and can also help foster new relationships. Cyberspace can help people manage their finances, or instantly purchase anything from gifts for family and friends, to a trip for themselves. It is an immensely powerful educational and informational tool, linking humankind's store of knowledge together through the click of a mouse.

The vast majority of those who utilize the online medium are contributing positively to this vibrant community. Like any environment, however, the unfortunate reality is that there are individuals who aim to harm. As more and more new Internet users come online, combating fraud becomes even more important. These new users are not familiar with the technology, and require special protection and attention.

Fulfilling the enormous promise of the interactive medium depends on consumers - and their families - being safe and secure online. Online integrity, therefore, is a top priority -- both at AOL and across our industry. All of us with a stake in cyberspace security are focused on this

issue, both pursuing our own strategies and working together.

Types of Fraud Seen Online

The Committee has asked that I speak to you about the types of fraudulent scams that exist online. While it is difficult to provide you with a comprehensive list, as the dynamics of scams are constantly changing, I can provide you with a sampling of those that are most common. [To be supplemented with visual presentation during oral testimony]. I will describe the types of fraud first and then the initiatives that AOL has engaged in to combat any fraud affecting our members. While sophisticated scam artists can be behind some of these frauds, by observing some basic rules of thumb, consumers can avoid being victims. Later in the testimony, I will provide a list of safety tips that AOL recommends consumers follow.

There are several different kinds of scams that we, in the Internet online industry, see with varying degrees of frequency. These include password scams, credit card scams, Web based frauds and junk e-mail, commonly known as "spam".

I. Password Scams

One of the most common activities of Internet hackers is to steal user information through password solicitation. During these types of scams on the Internet, users are approached and are asked to provide their password. This has become a fairly common practice on the Internet. In

fact, some Web sites are even fraudulently set up for the sole purpose of collecting passwords. Passwords are collected either by asking users to log in (and most of the time, people use their same password as their online service password), or offering users an entry into an area where they have to provide their passwords. Users need to make sure they have good passwords - preferably alpha-numeric combinations and not words in the dictionary - and they should never use the same password when asked to enter one at different places on the Internet.

The other type of password solicitation fraud occurs through one-to-one communications, either instantly or through e-mail. Instant Messages are ways of communicating in real time one-on-one. Some scammers will impersonate an Internet service staff member and pretend that a database has lost its data and needs a user's password again. They may even impersonate a telephone company representative stating that they need a user's password because something is wrong with the phone line. Another scam perpetrated through Instant Messages involves a hacker sending someone an Instant Message and asking the potential victim to send a copy of the file on the user's computer that stores the password. The request is generally made under the pretext of malfunctioning software.

Password solicitation can occur via regular e-mail as well. Scammers fabricate various ruses as to why a user might need to give up his or her password to someone in an e-mail message. For example, a hacker might ask a user to sign up for a contest (provide your name, address, e-mail, password, etc.) to "update your billing information," or to sign up for a bogus automated service.

Other hackers use Trojan Horses. These are fraudulent types of e-mail attachments that

appear as beneficial offers, but, when downloaded and executed, attach themselves to the computer, allowing a hacker to record a user's keystrokes and send his or her online service password back to the hacker. Homer's famous myth describes rolling the deceptive gift into Troy, and hackers try to pursue the same trick.

Password Cracking is a technique which hackers employ using automated programs that contain a list of all the words in the dictionary, common abbreviations and acronyms, and they put these programs to work on attempting to "crack" or "guess" a user's password. These programs are easily obtainable on the Internet and this is why it is important for users to create secure passwords.

II. Credit Card Fraud

Credit card solicitation is in many ways similar to password solicitation via Instant Messages or e-mail. However, in this situation, the user is asked for credit card information, most often under the guise of a "billing information update."

Other scammers pose as contest officials and send e-mail messages informing users they have won a prize. The e-mails make claims like: "you are the proud winner of a laptop... in order to redeem the prize, you must send in your name and mailing address - and a credit card number to cover the shipping & handling."

Similar to straight e-mail scams, billing impersonation can also originate with an e-mail that links you to a Web site that appears to be the user's Internet Service Provider and asks for the

entry of credit card information.

Scammers also create fake store fronts on the Internet. People order goods, submit their credit card information and never receive the merchandise. These Web sites commonly disappear within a few days.

There are also scams that affect Internet Service Providers, rather than users, directly. An example is Subscription Fraud, where hackers fraudulently register with an Internet Service Provider. They use programs called "credit card generators," which generate fraudulent credit card numbers that allow a hacker to sign up with an Internet service under a false identity. Internet Service Providers must have effective registration verification processes to prevent this type of fraud from occurring.

III. Other Web Frauds

There are many types of Web sites that can seek to defraud the consumer. An example of this is a Web site that contains virulent active content. These kinds of Web sites contain active content that can download information on to a user's computer without the user's knowledge and access personal files.

Other Web sites might contain Trojans. These sites try to automatically download the same Trojan programs mentioned earlier onto a user's computer to either steal personal information or delete files, among other things.

Lastly, there are also Impersonation or Hoax Web sites. These sites mirror official sites

in order to collect their data. In these situations, the Web site appears to the user to be legitimate but actually has no connection to the original site.

IV. Unsolicited Bulk E-mail (Spam)

Unsolicited e-mail is the most well publicized example of online fraud. While there are certainly many types of unsolicited messages that are perfectly legitimate, the rampant fraud in this context comes in two different forms: Fraud in content, and technological fraud.

Under the first scenario, commercial solicitations are sent to users offering products or services that are not legitimate and are intended to fool users into sending money for the products and services that either do not exist or fail to live up to the claims made about them. In the second instance, the fraud occurs because the senders of the mail fraudulently try to disguise their identity through forged headers.

Education of Members and the Provision of Technological Tools

Educating our members and providing them with easy to use technology tools they need to enhance their online experience is a top priority at AOL. To the extent online scams present a risk in defrauding people, it is a mission of AOL to educate members to protect themselves.

We believe one of the most powerful weapons against hackers and these other online problems is educating cyberspace users -- especially new people just coming onto the Internet.

At AOL, we post special alerts on our Welcome Screen, seen by all AOL members when they sign onto the service. We also have a regular feature that always appears on members' e-mail screens when they read their email, letting AOL members know AOL employees will under no circumstance ask for a member's password or billing information. In other words, members should ALWAYS deny any request to release their passwords online. We also work hard to get our safety and security messages out into the media. And our Chairman and CEO, Steve Case, regularly discusses these issues in his widely-read monthly update to members.

As previously mentioned, there are a list of safety tips consumers can follow to avoid being a victim of Internet fraud:

- 1) Choose a safe password, i.e. six alpha numeric characters
- 2) Do not give out your password or billing information to anyone
- 3) Do not give out personal information such as home address, telephone number or social security number
- 4) Do not download files from strangers
- 5) If a Web site is unfamiliar, look into the company's background before you do business with them
- 6) Don't believe everything you read; if it sounds too good to be true, it probably is

AOL fundamentally believes in the use of technology as another powerful weapon to fight fraud. From mail controls to Instant Message blocking, we proactively seek to protect members. We also raise members' awareness about such scams as Trojan Horses, through a

program called the "Download Sentry," a warning that pops-up on members' computer screens before they download an e-mail attachment that contains executable code. This warning reminds members to think twice before downloading a file sent from a stranger.

In addition, our efforts in combating fraud include a unique offering for parents to customize their children's online experience to block certain access to sites which they do not want their child to view. AOL's Parental Controls help members and their families control their online experience.

Parental Controls give parents the flexibility to shape their child's online experience by limiting their child's access to only pre-screened and child-approved World Wide Web sites, and establishing pre-approved addresses with which their child may correspond via e-mail.

Parents can also block their children from receiving e-mail attachments, which can contain inappropriate material, tailor their access to chat rooms (areas online which members in groups can communicate real time with one another), and block Instant Messages. In addition, AOL has a "Kids Only" area with specially designed proprietary content for children under 12 that is both educational and entertaining in nature. Parental Controls are offered to every AOL customer and can be turned on with a simple click of a button.

Another tool AOL offers members are sophisticated e-mail controls that allow members to choose the sources of their mail, and block mail they don't want. AOL has also taken the lead in fighting junk e-mailers by protecting members' mail boxes in court. In fact, AOL has filed suit against 10 companies that send fraudulent junk mail. On December 18, 1997, AOL won a significant victory in its battle against spam when Over the Air Equipment, Inc., a junk e-mailer

that advertised pornographic Web sites, surrendered in its fight against AOL and agreed to an injunction barring it from sending unsolicited e-mail to AOL members.

Cooperation with Law Enforcement

AOL also works hand-in-hand with law enforcement to track down computer hackers and other cyberspace lawbreakers, both on a coordinated and ad hoc basis. We have entered into a coordinated relationship with the National Association of Attorneys General, developing a protocol for cooperation. Under this arrangement, AOL officials provide training to state attorneys general and their offices about how online scams are perpetrated and provide referral information for ongoing investigations. In addition, AOL participates in the Innocent Images Task Force organized by the U.S. Department of Justice. In this context, we refer all complaints relating to the distribution of graphic files containing child pornography. Our cooperation with the task force involves forwarding complaints we receive from members to proper law enforcement authorities and ongoing assistance with Department of Justice investigations.

Recognizing the global nature of the Internet online medium, AOL has extended its law enforcement initiatives beyond the U.S., to the international law enforcement community. AOL has formed an alliance with Interpol, the leading law enforcement organization representing over 150 countries worldwide. AOL has participated in a number of conferences and workshops with Interpol's working committees on "Offenses Against Minors" and "Computer Crimes and Information Technology." Additionally, AOL has been invited by the Department of Justice to

participate in the upcoming P8 meetings in Paris to review the establishment of protocols between private industry and law enforcement in trans-national computer crimes investigations.

Cooperation within the Private Sector

Taking this commitment to cyberspace safety and security to a wider audience, AOL and other industry leaders have joined together with family advocacy groups to educate all cyberspace users. The goal of this is to work towards a uniform set of rules and responsibilities that are both effective and sensitive to how quickly this global medium is evolving.

Last December, industry leaders, family advocacy and educational groups participated with government and law enforcement officials and consumer advocates in the Internet Online Summit: Focus on Children. This two-day conference concentrated on what we can do together to make cyberspace a safer and more enriching place for children to explore, learn and just plain have fun. An outcome of the Summit was the formation of the Internet Safety Forum.

Several key initiatives emerged from the Summit, including:

**** The CyberTipLine, which will serve as a clearinghouse for tips and leads on cybercrime such as child pornography and incidents of preying on children. The CyberTipLine will be operated by the National Center for Missing and Exploited Children in conjunction with industry and with U.S. Government support. All leads will be acknowledged and forwarded to the appropriate branch of law enforcement.**

**** For specialized training in cyberspace law enforcement, summit participants have**

begun to create a training video and a nationwide series of hands-on training for law enforcement officials. The first session takes place next month in Washington, D.C. The video and training sessions, which AOL has helped develop, will raise awareness about the types and techniques of online crime. And they are designed to teach law enforcement agencies how best to adapt good old-fashioned police work to the pursuit of cyberspace criminals.

** We also are creating a national public education campaign -- "America Links Up: An Internet Teach-In" -- to help parents, educators, librarians and others learn how to provide their children with the safest and most enriching online experience possible. The slogan, "Think, then Link," will spearhead the campaign to encourage parental involvement in teaching kids safe online behavior and how to use the technological tools available to promote safety and access to appropriate online material.

Just two weeks ago, participants of the Summit came together in Washington for the first ever Cyber-Crimes seminar, assembling specialists from federal, state, and local organizations, along with Internet providers, to sponsor and conduct a series of online safety and enforcement training programs.

These initiatives underscore the industry's commitment to finding ways to make cyberspace safe and secure in close partnership with consumer groups, law enforcement and government agencies. The summit was an important step, but it was also just the beginning of our efforts and coordination. AOL and our industry will continue to be proactive in these efforts, working with our content partners and others in the Internet community to build a medium of which we can all be proud.

All consumers of this new medium must use common sense when it comes to their online experience. Consumers need to take the same precautions in the online world that they do offline, and supervise their children.

When going online, consumers need to know who they're dealing with. Just as you would never give out your ATM pin number to a stranger on the street, consumers have to know not to give out personal information like a credit card number or password, or download files from strangers when they are online.

Just as you might scrutinize a stranger hanging around your house, users should think twice before giving out any personal information to strangers through your computer. Most of the scams occurring on the Internet are variations of the types of fraud that occur in the real world. Users need to exercise the same common sense they apply in real life on the Internet.

If we as an industry can continue to work together, in partnership with consumers and with law enforcement, we can establish a safe and secure online experience that not only lasts, but helps this new medium reach its tremendous potential to have a positive impact on people's lives.

I would like to thank the Subcommittee for the opportunity to be with you here today and will be happy to answer any questions.

**STATEMENT OF
BARRY D. WISE
Before The
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Hearing On
FRAUD ON THE INTERNET:
SCAMS AFFECTING CONSUMERS
February 10, 1998**

★★★

Madam Chairman and Members of the Subcommittee.

My name is Barry Wise and it is a pleasure to be here today to share my experiences with you of being defrauded by a company known as Fortuna Alliance. I am currently employed by the Duke Energy Corporation as a senior internal auditor. I am also a Certified Public Accountant and recently became a Certified Fraud Examiner. Obviously I wish that I had been a Certified Fraud Examiner when I was considering an investment with Fortuna Alliance. I am a husband and the father of two young children. The intention of my investment with Fortuna Alliance was meant to benefit my children's future, not the financial heartache that resulted instead.

In April 1996, I was told by a colleague that a company known as Fortuna Alliance was advertising on the Internet. The company was supposedly offering a good investment opportunity with a high rate of return. My associate informed me that he knew of a person who already received some return on the investment, so it must be legitimate. I later discovered that this person had some type of relationship with the founder of Fortuna Alliance and the return on investment probably was nothing more than bait money to create an air of legitimacy to the scheme.

I visited the Fortuna Alliance Web site as well as numerous other individual sites that had been created by its members. These members were people who had already invested with Fortuna and were actively recruiting new investors which would be directly to their benefit. The Fortuna Alliance site explained that each membership would pay out a maximum of \$5,000 per month when a matrix of approximately 300 people was filled with names of new investors. This matrix was supposedly based upon their "unique mathematical formula: The Fibonacci Sequence." The Web site informed that Fortuna was about to begin a massive advertising campaign to solicit new investors, therefore, I would not have to recruit anyone or do anything to get a return on my investment. I would not have to work at filling up the matrix because Fortuna Alliance's advertising campaign would accomplish that for me. However, the recruitment of new investors was

encouraged because that would fill up the matrix faster which in turn would initiate a flow of money to Fortuna Alliance members. Another part of the Fortuna Alliance business was a co-op through which products and services would be sold to people in the matrix. I understood that a commission would be paid to me for any purchases made in the co-op by people in my matrix. It should be noted that I never received any literature from Fortuna Alliance that explained what goods were for sale and how to purchase them. Fortuna Alliance stated there was a money back guarantee of my entire initial investment if after 90 days I was not completely satisfied for any reason. That offer really made me feel that I had nothing to lose with this potentially lucrative investment.

In late April 1996, after carefully studying the Fortuna Alliance Web site and several of the individual member's sites, I decided to make an investment. I purchased 15 elite memberships at \$250 each and two premier memberships which cost \$600 each. My total investment was \$4,950 which I hoped would result in a monthly income check from Fortuna Alliance. Fortuna insisted that I pay for this investment by money order or certified check only. In return I received a very elaborate package of investment information from Fortuna for each of my memberships. I read this information carefully and continued to understand that I did not have to actually do anything to receive a return on my investment.

Shortly after purchasing these memberships I tried to call Fortuna Alliance several times in order to verify that my investments were properly recorded in their computer system. My telephone calls were always answered by an automated voice system that never connected me to speak with an actual person.

In late May 1996, I was roving the Internet while working on a project and did a search on the word "fraud." During this search I came across a notice by the Federal Trade Commission that Fortuna Alliance had been shut down for operating an illegal pyramid scheme and making false claims. I immediately sent a letter to Fortuna Alliance requesting a refund of my money. They never refunded any of my \$4,950 initial investment. I also filed a claim with the Federal Trade Commission.

Upon discovering that I had been the victim of a fraud via the Internet, I started to do some investigation of my own. I determined that in order to be a legitimate multi-level marketing company, commission needs to be paid on actual goods or services sold. Fortuna Alliance was supposedly going to pay commissions only based on one time fees paid to purchase a membership (i.e. money was just being funneled to people at the top of the pyramid). During my research, I noted several other companies on the Internet which appeared to be operating illegal pyramid type schemes.

In Spring 1997, I received a letter from Gilardi & Company, LLC in San Francisco, California. Gilardi & Company had been appointed by the Federal Trade Commission to be the claims administrator for Fortuna Alliance. The correspondence I received from Gilardi & Company indicated that my account consisted of only three "elite" memberships, when in actuality I had purchased 15 "elite" memberships and two "premier" memberships. Evidently, Fortuna Alliance's records of my purchases did not properly account for my entire investment. I subsequently filed a claim for \$4,950 with proper documentation to Gilardi & Company. In a telephone conversation with representatives of Gilardi & Company I determined that my claim for \$4,950 was accepted and verified by them as accurate.

Shortly after my dealings with Gilardi & Company I received a letter from Fortuna Alliance which stated that they had been cleared of all charges and were continuing business as Fortuna Alliance II. This letter also encouraged me not to request a refund and continue to invest with Fortuna Alliance II. I disregarded this letter and its message as being completely bogus.

It is my understanding that the Federal Trade Commission has collected enough funds from Fortuna Alliance thus far to cover approximately 60 percent of investors' claims. On January 6, 1998, the court issued a compliance order that would allow over 8,600 Fortuna Alliance members to begin receiving partial refunds which would cover approximately 60 percent of their individual claim amounts.

I appreciate this opportunity to share my story with you. This concludes my statement, Madam Chairman, and I would be pleased to answer any questions.

#

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON
"INTERNET FRAUD"**

**Before the
SUBCOMMITTEE ON INVESTIGATIONS
of the
GOVERNMENTAL AFFAIRS COMMITTEE
UNITED STATES SENATE**

Washington, D.C.

February 10, 1998

Madam Chairman and members of the Committee: I am Robert Pitofsky, Chairman of the Federal Trade Commission ("FTC" or "Commission"). I appreciate this opportunity to present the Commission's views on the important issue of fraud on the Internet.¹

Introduction

The Commission pursues its mission of promoting the efficient functioning of the marketplace by seeking to protect consumers from unfair or deceptive acts or practices and to promote vigorous competition. As you know, the Commission's responsibilities are far-reaching. Its primary legislative mandate is to enforce the Federal Trade Commission Act, which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.² With the exception of certain industries, this statute provides the Commission with broad law enforcement authority over virtually every sector in our economy;³ commerce on the Internet falls within the broad sweep of this statutory mandate.

¹ My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any other Commissioner.

² 15 U.S.C. § 45(a). The Commission also has responsibilities under approximately thirty additional statutes, *e.g.*, the Clayton Act, 15 U.S.C. § 12, which prohibits various anticompetitive practices; the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.*, which mandates disclosures of credit terms; the Fair Credit Billing Act, 15 U.S.C. § 1666 *et seq.*, which provides for the correction of billing errors on credit accounts; and the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, which establishes rights with respect to consumer credit reports. The Commission also enforces over 35 rules governing specific industries and practices, *e.g.* the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

³ Certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance are wholly or partially exempt from Commission jurisdiction. See Section 5(a)(2) of the FTC Act, 15 U.S.C. § 45(a)(2) and the McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

The advent of the Internet -- with its new methods of communicating through web sites, electronic mail, news groups, chat rooms, electronic bulletin boards, and commercial on-line services -- is an historical development much like the introduction of television or, a few generations earlier, the telephone. Like these earlier technologies, the Internet presents consumers with an exciting new means for them to purchase both innovative and traditional goods and services faster and at lower prices, to communicate more effectively, and to tap into rich sources of information that were previously difficult to access and that now can be used to make better-informed purchasing decisions.

The Internet's promise of substantial consumer benefits is, however, coupled with the potential for fraud and deception. Fraud is opportunistic, and fraud operators are always among the first to appreciate the potential of a new technology. This phenomenon was illustrated by the advent, flourishing, and near-demise of pay-per-call (900-number) technology as a commercial medium during the last decade. 900-number technology was the first interactive technology -- and still is the only interactive technology offering nearly universal access because all that is needed is a telephone. This technology has huge potential as an alternative payment system, since every telephone could serve as a payment terminal, and no credit cards, debit cards, or checks are needed. In 1991, there were \$6 billion in pay-per-call transactions. But fraud operators moved in to exploit the technology, and the industry was slow to respond to this challenge. As a result, the 900-number industry's reputation became tarnished by fraud and abuse, and sales plummeted to \$300 million annually. In 1992, pursuant to Congressional mandate, the FTC and the FCC promulgated rules to regulate the 900-number industry to ensure that consumers would receive price and other material information before incurring costs, and have the right to dispute allegedly

incorrect or unauthorized charges.⁴ Annual sales began to climb again, reaching \$450 million in 1995. The 900-number industry now seems poised to attract a higher volume of legitimate commerce because consumers can use 900-numbers with greater confidence.

Some of the same features that made pay-per-call technology a tempting field for fraud artists in the 1980s -- low start-up costs and the potential for big profits -- exist on the Internet today. Indeed, after buying a computer and modem, scam artists can establish and maintain a site on the World Wide Web for \$30 a month or less and solicit consumers anywhere on the globe. There is nothing new about most types of Internet fraud the Commission has seen to date. What is new -- and striking -- is the size of the potential market and the relative ease, low cost, and speed with which a scam can be perpetrated.

If the Internet is to avoid a fate similar to that of 900-number technology, the Commission believes it is important to address Internet fraud now, before it discourages new consumers from going on-line and chokes off the impressive commercial growth now in progress and potential for innovation on the Internet. According to some industry analysts, total Internet business will climb from \$2.6 billion in 1996 to \$220 billion by 2001.⁵ Much of this trade likely will involve business-to-business transactions. However, the on-line consumer market also is growing, and at an

⁴ The FTC and the FCC promulgated their regulations pursuant to the Telephone Disclosure and Dispute Resolution Act, 15 U.S.C. §§ 5701 *et seq.* The FTC's regulations are at 16 C.F.R. Part 308; the FCC's regulations are at 47 C.F.R. § 64.1501 *et seq.*

⁵ International Data Corporation, *Dramatic Growth of Web Commerce - From 2.6 Billion in 1996 to more than \$220 Billion in 2001* (Aug. 26, 1997) (reported at <http://www.idc.com/7HNR/ic2001f.htm>).

exponential rate. In early 1997, 51 million adults were already on-line in the U.S. and Canada.⁶ Of those people, 73% reported that they had shopped for product information on the World Wide Web, the interactive graphics portion of the Internet.⁷ By December 1997, the number of on-line users had risen to 58 million adults in the U.S. and Canada, and 10 million had actually purchased a product or service on-line.⁸ Perhaps most telling, analysts estimate that Internet advertising -- which totaled approximately \$301 million in 1996 -- will reach \$4.35 billion by the year 2000.⁹

If this trend and all the benefits that it implies are to continue, consumers must feel confident that the Internet is safe from fraud. Nothing is more likely to undermine their confidence than exploitation by scam artists using this new technology as yet another means to defraud consumers. Therefore, the Commission, like the Subcommittee, is concerned about fraud on the Internet and has taken strong action to combat it.

⁶ CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Spring '97 (March 12, 1997) (defining adults as individuals over 16 years old) (reported at http://www.commerce.net/work/pilot/nielsen_96/press_97.html) [hereafter *CommerceNet/Nielsen Demographic Study*, Spring '97]; IntelliQuest Communications, Inc., *Worldwide Internet/Online Tracking Service (WWITS™): Second Quarter 1997 Study* (Sept. 4, 1997) (reported at <http://www.intelliquest.com/about/release32.htm>).

⁷ *CommerceNet/Nielsen Demographic Study*, Spring '97.

⁸ CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Fall '97 (December 11, 1997) (reported at <http://www.commerce.net/news/press/121197.html>) [hereafter *CommerceNet/Nielsen Demographic Study*, Fall '97]. See also, Yankelovich Partners, *1997 Cybercitizen Report* (Mar. 27, 1997) (reported at <http://www.yankelovich.com/pr/970327.HTM>) (finding that 23% of users ordered and paid for a product over the Internet, i.e. "transacted" business online).

⁹ Jupiter Communications, *1998 Online Advertising Report* (Aug. 22, 1997) (reported at <http://www.jup.com/digest/082297/advert.shtml>) (figure includes directory listings and classified advertisements).

The Commission began to examine the potential for consumer protection problems on the Internet proactively, before on-line consumer transactions became common. In the fall of 1995, the Commission held public hearings to explore business and consumer issues arising from technological innovation and increasing globalization. Over 200 company executives, business representatives, legal scholars, consumer advocates, and state and federal officials presented testimony. A two-volume report was published summarizing the hearings. Volume II, "Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace," reflects principles that many participants urged the Commission to consider when addressing the Internet and other technologies in the new Information Age:

Consumer protection is most effective when businesses, government, and consumer groups all play a role. Meaningful consumer protection takes: (1) coordinated law enforcement against fraud and deception; (2) private initiatives and public/private partnerships; and (3) consumer education through the combined efforts of government, business, and consumer groups.¹⁰

Applying these principles, the Commission has taken the offensive against fraud on the Internet through a three pronged-strategy that emphasizes targeted law enforcement action, complemented by education of consumers and new Internet entrepreneurs, both of whom may be venturing into cyberspace for the first time. In all aspects of this strategy, but particularly in the Commission's consumer and business education efforts, the Commission has sought to form new partnerships with private industry and other government agencies, and the Commission has tried to turn new technologies to our advantage.

¹⁰ See Exhibit 1, Bureau of Consumer Protection, Federal Trade Commission, *Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace*, iii (May 1996).

Law Enforcement

First and foremost, the FTC is a civil law enforcement agency with strong and effective enforcement tools to combat fraud and deception. The Commission can issue administrative complaints and conduct administrative adjudications that may result in the issuance of cease and desist orders against practices found to be unfair or deceptive.¹¹ Further, in cases of fraud and other serious misconduct, the Commission has statutory authority to file suit directly in federal district court to obtain preliminary and permanent injunctive relief, redress for injured consumers, or disgorgement of ill-gotten gains.¹² The Commission also may seek the assistance of the Department of Justice in filing criminal contempt proceedings against persons who violate court orders issued at the behest of the Commission, or in filing criminal actions in egregious fraud cases.

The Commission has brought over 25 law enforcement actions against defendants whose alleged illegal practices used or involved the Internet. Several of these cases involved alleged deceptive advertising and billing practices of commercial on-line service providers.¹³ Most of the

¹¹ 15 U.S.C. § 45.

¹² 15 U.S.C. § 53(b). In addition, the Commission may request the Attorney General to file an action in the appropriate federal district court seeking civil penalties for violations of the Commission's administrative orders or trade regulation rules, and may file those actions on its own behalf if the Department of Justice declines to do so in the name of the United States. 15 U.S.C. § 56.

¹³ *America Online, Inc.*, FTC File No. 952-3331 (consent order subject to final approval, May 1, 1997); *CompuServ, Inc.*, FTC File No. 962-3096 (consent order subject to final approval, May 1, 1997); *Prodigy Services Corp.*, FTC File No. 952-3332 (consent order subject to final approval, May 1, 1997). These respondents allegedly made "free trial" offers to consumers without adequately disclosing that consumers would automatically be charged if they did not affirmatively cancel before the end of the trial period. (The Commission also alleged that AOL
(continued...)

Commission's law enforcement actions, however, have involved old-fashioned scams dressed up in high-tech garb.¹⁴ For example, the Commission has brought several cases to stop alleged pyramid schemes that recruit victims through the web.¹⁵ In the Commission's largest Internet pyramid case to date, *FTC v. Fortuna Alliance*,¹⁶ the defendants allegedly promised consumers that, for a payment of \$250, they would receive profits of over \$5,000 per month. The program spawned numerous web sites on the Internet and appealed to victims all around the globe seeking

¹³(...continued)

failed to inform consumers that 15 seconds of connect time was added to each online session, resulting in additional undisclosed charges, and that AOL misrepresented that it would debit customers' bank accounts only after receiving authorization to do so.)

¹⁴ *E.g.*, **Alleged credit repair scams:** *FTC v. Corzine*, No. CIV-S-94-1446 (E.D. Cal. filed Sept. 12, 1994); *FTC v. Consumer Credit Advocates*, No. 96 Civ. 1990 (S.D.N.Y., filed Mar. 19, 1996); *Martha Clark, d/b/a Simplex Services*, Docket No. C-3667 (consent order, June 10, 1996); *Bryan Coryat, d/b/a Enterprising Solution*, Docket No. C-3666 (consent order, June 10, 1996); *Lyle R. Larson, d/b/a Momentum*, Docket No. C-3672 (consent order, June 12, 1996); *Rick A. Rehem, d/b/a NBC Credit Resource Publishing*, Docket No. C-3671 (consent order, June 12, 1996). **Alleged business opportunity scams:** *FTC v. Intellicom Services, Inc.*, No. 97-4572 TJH (Mxx)(C.D. Cal., filed June 23, 1997); *FTC v. Chappie (Infinity Multimedia)*, No. 96-6671-CIV-Gonzalez (S.D. Fla., filed June 24, 1996); *Timothy R. Bean, d/b/a D.C. Publishing Group*, Docket No. C-3665 (consent order, June 10, 1996); *Robert Surveys, d/b/a Excel Communications*, Docket No. C-3669 (consent order, June 12, 1996); *Sherman G. Smith, d/b/a Starr Communications*, Docket No. C-3668 (consent order, June 12, 1996). **Alleged deceptive cash grant matching service:** *Randolf D. Alberton, d/b/a Wolverine Capital*, Docket No. C-3670 (consent order, June 12, 1996). **Alleged deceptive advertising of health product:** *Global World Media Corp. and Sean Shayan*, Docket No. C-3772 (consent order, Oct. 9, 1997). **Alleged misrepresentations about product characteristics:** *Zygon International, Inc.*, Docket No. C-3686 (consent order, Sept. 24, 1996). **Alleged non-delivery of ordered merchandise:** *FTC v. Brandzel*, 96 C. 1440 (N.D. Ill., filed Mar. 13, 1996).

¹⁵ *E.g.*, *FTC v. The Mentor Network, Inc.*, Civ. No. SACV96-1104 LHM (EEEx) (C.D. Cal., filed Nov. 5, 1996); *FTC v. Global Assistance Network for Charities*, Civ. No. 96-02494 PHX RCB (D. Ariz., filed Nov. 5, 1996); *FTC v. JewelWay International, Inc.*, CV97-383 TUC JMR (D. Ariz., filed June 24, 1997); *FTC v. Rocky Mountain International Silver and Gold, Inc.*, Action No. 97-WY-1296 (D. Colo., filed June 23, 1997).

¹⁶ Civ. No. C96-799M (W.D. Wash., filed May 23, 1996).

to get rich quickly for little effort. Yet sheer mathematics dictated that 95 percent of the consumers who joined the program could never make more than they paid in. The Commission obtained a temporary restraining order halting the unlawful practices and freezing the assets of the individuals who developed and operated the Fortuna program. The court order also required the defendants to repatriate the assets they had deposited overseas. In February 1997, the defendants stipulated to a permanent injunction that prohibited their alleged pyramid program and provided for redress to consumers who requested refunds. The defendants subsequently balked at paying many consumers, and the Commission filed a contempt motion. The court did not impose sanctions but issued a compliance order against the defendants on January 6, 1998. The compliance order clears the way for over 8,600 Fortuna members to begin receiving refunds.

Another alleged Internet pyramid scheme targeted in a recent Commission law enforcement action was Credit Development International.¹⁷ The scheme was propelled by allegedly false promises that those who joined CDI would receive an unsecured Visa or MasterCard credit card with a \$5,000 limit and a low interest rate, as well as the opportunity to receive monthly income of \$18,000 or more. The Commission filed its complaint on October 29, 1997, and on October 31, the court granted a temporary restraining order, appointed a receiver to oversee the corporate defendants, and froze both the corporate and individual defendants' assets. After a hearing, on November 20, 1997, the court issued a preliminary injunction against the defendants. The Commission's staff estimates that over 30,000 consumers collectively may have lost 3 to 4 million dollars in this alleged scam. This matter is still in litigation.

¹⁷ *FTC v. Nia Cano d/b/a Credit Development Int'l & Drivers Seat Network*, No. 97-7947 IH (AJWx) (C.D. Cal. filed Oct. 29, 1997).

The Commission's investigators discovered the Credit Development International scam as part of an ongoing effort to monitor "spam" -- also known less colloquially as unsolicited commercial e-mail ("UCE") -- on the Internet. One theme sounded in the Commission's recent privacy hearings was that an ever-increasing volume of UCE strains the capacity of on-line service providers and threatens the development of the Internet as a conduit for commerce. For example, at the Commission's privacy hearings held in June 1997, America Online ("AOL") reported that it handled 15 million electronic messages per day. By September 1997, that number had quadrupled to 60 million messages per day. Significantly, AOL has estimated that UCE comprises as much as one-third of all e-mail traffic.

Beyond the sheer volume and potential annoyance of UCE, many UCE messages may be misleading or deceptive.¹⁸ Alleged scams like Fortuna and Credit Development International generate huge quantities of UCE, because e-mail is unparalleled as a means of cultivating a "downline" -- additional recruits to a pyramid -- for virtually no cost and little effort. The same attributes make UCE attractive to other types of scams as a means to solicit millions of consumers for little cost.

Although most Internet fraud is fairly traditional, the Commission has taken action against one scheme that uniquely and ingeniously exploited what can be done on the Internet and *only* on

¹⁸ In addition, UCE often contains fake or altered routing information in the address portion of a message, *i.e.*, the "From," "Received from," or "Reply to" lines. Thus, consumers may not know who sent the e-mail or to whom they should reply. Fake "Reply to" lines also may send undeliverable or reply messages back to the wrong address, thereby tying up a legitimate business's computer. This may confuse consumers, but in addition, UCE may directly deceive them through misleading advertisements or solicitations that appear in the body of the e-mail itself. The Commission has received, directly or by referral from consumers, over 50,000 UCE messages. Our staff actively reviews these messages and investigates purveyors of UCE that may violate the FTC Act's prohibition against unfair or deceptive practices.

the Internet. The case *FTC v. Audiotex Connection, Inc.*, CV-97 0726 (DRH) (E.D.N.Y.), presented a scheme that allegedly "hijacked" consumers' computer modems by surreptitiously disconnecting them from their local Internet Service Provider (such as AOL) and reconnecting them to the Internet through a high-priced international modem connection, purportedly going to Moldova but actually terminating in Canada. On various Internet sites, the defendants offered access to free computer images through a special "viewer" program. If a consumer downloaded and activated the viewer software, the alleged hijacking automatically ensued, and an international long-distance call (and the charges for it) continued until the consumer turned off the computer -- even if he or she left defendants' sites and moved elsewhere on the Internet, or left the Internet entirely to use a different computer program.

Commission staff were first alerted to the *Audiotex* scheme by security experts at AT&T. The United States Secret Service assisted staff in ascertaining how this "Trojan horse" viewer software worked, and AT&T lent further assistance in tracing the software back to specific web sites. With this help, the Commission's staff completed its investigation, filed a complaint, and obtained an *ex parte* temporary restraining order and asset freeze against the defendants within just 31 days of learning about the alleged scam. The lawsuit was recently resolved by entry of a stipulated permanent injunction against the main defendants named in the Commission's complaint and the issuance of a virtually identical administrative order against additional parties found to have played a role in the alleged scam. Under the two orders, the defendants and administrative

respondents are barred from engaging in the alleged unlawful practices, and over 38,000 consumers should receive full redress worth an estimated \$2.74 million.¹⁹

Consumer Education

The Commission has gone on-line to reach Internet users. Since April 1995, the Commission has used its web site at "www.ftc.gov" to make instantly available to consumers a rich and continuously updated body of advice and information. The Commission receives approximately 60,000 to 75,000 "hits" per day on this home page.²⁰ In September 1997 alone, FTC.GOV received almost 2 million hits from 114,000 visitors.

In constructing its web site, the Commission has put a premium on making it not only comprehensive, but also user-friendly. FTC.GOV contains a search engine that allows consumers to pull up information by typing in a few key words. The site also contains a special section called ConsumerLine that provides news releases, consumer alerts, and on-line versions of all of the Commission's consumer and business education publications.²¹

Building on the success of the FTC's home page, the Commission's staff conceived a plan to create a new site at "www.consumer.gov" and has developed the site in partnership with sister agencies -- the Securities and Exchange Commission ("SEC"), the U.S. Consumer Product Safety Commission ("CPSC") the Food and Drug Administration ("FDA"), and the National Highway

¹⁹ The Commission would like to acknowledge the assistance of AT&T and MCI in administering the redress program. AT&T and MCI will distribute refunds to most consumers in the form of telephone credits on their long-distance telephone bills.

²⁰ A "hit" occurs when someone accesses a web site.

²¹ After the home page for FTC.GOV, the search engine is the most popular area visited on the web site, followed by the ConsumerLine section. See Exhibit 2, excerpts from "www.ftc.gov".

Traffic Safety Administration ("NHTSA"). CONSUMER.GOV provides the public with "one-stop shopping" for federal information on a broad spectrum of consumer issues, ranging from auto recalls to drug safety to investor alerts.²²

Extending a hand to consumers at their most vulnerable point -- when they are surfing in areas of the Internet likely to be rife with fraud and deception -- the staff of the Commission has posted several "teaser" web sites. The "Ultimate Prosperity Page" is one example advertising a fake deceptive business opportunity. The "Ultimate Prosperity Page" uses "buzz words" and promises of easy money common to many such scams. When the consumer clicks from the "Ultimate Prosperity Page" to the next page in the series, he or she finds glowing testimonials from fictitious persons who purportedly have achieved fabulous success through the business opportunity -- again mirroring the typical get-rich-quick business opportunity scam. Clicking through to the third and final page in the series, however, brings the consumer to a sobering warning: "If you responded to an ad like [this], you could get scammed." The warning page gives advice on how to avoid fraudulent business opportunities and provides a hyper-text link back to FTC.GOV, where consumers can learn more about investing in franchises or business opportunities.²³

There are now other teaser sites, posted by the Commission's staff, that mimic pyramid schemes, scholarship scams, deceptive travel programs, false weight-loss claims, and fraudulent vending opportunities -- all perennial frauds that have been practiced on consumers for years

²² Exhibit 3, homepage of "www.consumer.gov".

²³ To alleviate any privacy concerns that consumers may have, the warning page makes it clear that the FTC has not gathered any personal information about individuals visiting this teaser site.

through direct mail, telemarketing, and other means, and are now enjoying new life on the Internet.²⁴ The Commission's staff has registered each "teaser" site with major search engines and indexing services on the Internet. Thus, consumers may encounter the site when they are perhaps most receptive, just when they may be about to become ensnared in a fraud by responding to a plausible but untrue come-on. Private on-line service companies have worked with the Commission's staff to highlight various teaser pages and have billed some as the "new" or "cool" site of the week.²⁵

In another effort to use new technology to reach the public, the staff of the Commission partnered with the North American Securities Administrators Association and held a real time on-line forum on the Internet in April 1997. Over 100 consumers participated, posing questions to, and receiving instantaneous responses from, state and federal experts about how to invest wisely in new business ventures or franchises. The Commission posted the transcript of this "chat" session on its web site so that other consumers could access it and benefit from the exchange.

The Commission has actively sought Internet companies and trade groups to join with us as partners in disseminating consumer protection information to consumers on-line. As a result, the Interactive Services Association, a leading on-line trade association, and companies such as AT&T, NetCom, and America Online have helped circulate public service announcements over the Internet, cautioning consumers to avoid particular scams and "hot linking" consumers to the

²⁴ Exhibit 4, examples of FTC teaser sites.

²⁵ Exhibit 5, example of FTC teaser site highlighted as "new" site of the week by Yahoo!, a large Internet search engine and indexing service.

Commission's web site where they can find "Cybershopping" guides, "Safe Surfing" tips, and other helpful information.

Business Education

At the forefront of its business education efforts, the Commission has conducted a number of "Surf Days" aimed at providing information to new entrepreneurs who may unwittingly violate the law. The first Surf Day was conducted in December 1996 and focused on pyramid schemes that had begun to proliferate on the Internet. Commission attorneys and investigators enlisted the assistance of the SEC, the U.S. Postal Inspection Service, the Federal Communications Commission, and 70 state and local law enforcement officials from 24 states. This nation wide *ad hoc* task force surfed the Internet one morning, and in three hours, found over 500 web sites or newsgroup messages promoting apparent pyramid schemes. The Commission's staff e-mailed a warning message to the individuals or companies that had posted these solicitations, explaining that pyramid schemes violate federal and state law and providing a link back to FTC.GOV for more information. In conjunction with the New York Attorney General's Office and the Interactive Service Association, the Commission announced the results of Internet Pyramid Surf Day at a televised press conference held during the Internet World '96 convention in New York City. A month later, the Commission's investigative staff checked on the status of web sites or newsgroups identified as likely pyramids during Surf Day and found that a substantial number had disappeared or been improved.²⁶ The Commission has employed this technique several times

²⁶ Apart from newsgroup messages that had terminated automatically, 66 (18%) of the notified web sites had been improved or taken down within a month. In the wake of a subsequent Surf Day that targeted a separate type of fraud, 24% of the notified web sites improved or removed their solicitations.

since, conducting additional Surf Days focused on Internet web sites or newsgroup messages that promoted potentially problematic business opportunities, credit repair schemes, and "miracle cure" health products.

The Commission has now taken its Surf Day concept to the private sector, the global law enforcement community, and sister agencies as well. In August 1997, the Coupon Information Center, a private trade association, and its members from the national merchandising community joined Commission staff in surfing for fraudulent opportunities that promoted coupon certificate booklets. Then on October 16, 1997, the Commission helped coordinate the first "International Internet Surf Day." Agencies from 24 countries joined this effort and targeted "get-rich-quick" schemes on the Internet.²⁷ Australia's Competition and Consumer Commission oversaw the world-wide effort while the FTC led the U.S. team consisting of the SEC, the Commodities Futures Trading Commission ("CFTC") and 23 state agencies.

In November 1997, the Commission used the Surf Day concept to help the Department of Housing and Urban Development ("HUD") target unscrupulous "HUD Tracers." These "tracers" track down consumers to whom HUD may owe a refund for FHA mortgage insurance.

Consumers can claim their refund for free by contacting HUD directly; however, unscrupulous "tracers" may falsely claim that refunds cannot be secured without their assistance (and they may charge up to 30 percent in commissions), may falsely claim an affiliation with the government, and may falsely represent to other entrepreneurs how much money they can make as "HUD tracers."

²⁷ International participants included Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Hungary, Ireland, Jamaica, Japan, Korea, Mexico, New Zealand, Norway, the Philippines, Poland, Portugal, South Africa, Spain, Sweden, Switzerland, and the United Kingdom.

The HUD Tracer Surf Day not only helped to generate publicity to inform consumers about HUD's refund program, but it also helped eliminate many potentially deceptive solicitations from the Internet. A month after sending out warning messages, the Commission's staff checked on suspect tracer sites and found that 70 percent had shut down entirely or removed questionable claims about earnings potential or their affiliation to HUD.

Earlier this month, the Commission announced yet another innovative use of the Surf Day concept, this time targeting deceptive UCE messages. Commission staff conducted a "fall harvest" by surfing the Commission's large database of UCE solicitations, topic by topic, and identifying over 1000 individuals or companies potentially responsible for misleading e-mail solicitations, for example, for pyramid or other get-rich-quick schemes. Ironically, most of these UCE messages did not allow any reply by e-mail, due to inaccurate or deceptive "sender" information, so in January through the U.S. Postal system the Commission sent out letters warning the sources of the UCE that their messages may be in violation of the law.

Our messages to businesses on the Internet are straightforward -- *e.g.*, don't lie or make misleading statements; don't make product or earnings claims that you can't support; don't mislead consumers with unrealistic testimonials. The difficulty lies in finding a way to get these basic messages to new entrepreneurs who may have no prior business or advertising experience. Surf Days help us overcome this hurdle, but in addition, we have put together a "road show" that our ten regional offices can use in their local communities to help explain how basic legal principles apply on the Internet. The Commission also is preparing a business guide for Internet entrepreneurs and a continuing legal education ("CLE") course for lawyers who counsel new Internet businesses. Finally, the Commission is going directly to the computer industry for help.

In July, Commission representatives met with Silicon Valley executives at Stanford University's Technology and Business Strategy Summit '97, and asked them to lend us their contacts and marketing expertise in order to reach new Internet entrepreneurs.

Looking Ahead

Currently, the Commission receives approximately 100 to 200 Internet-related complaints per month. Many of these complaints are forwarded to us by the National Fraud Information Center, with which the Commission works closely. The Commission has seen an increase in complaints over the last year, but fortunately on-line problems seem to be growing at a slower pace than the Internet marketplace itself. At the moment, complaints about Internet fraud remain a small fraction of the number of complaints the Commission receives about more traditional problems concerning credit cards or telemarketing. However, the Commission expects that as the Internet marketplace grows, reports about consumer fraud also will continue to grow.

The potential for fraud is likely to be fueled by easy on-line access that exists for legitimate and fraudulent businesses alike. Also, it is likely that many first-time entrepreneurs, because of their lack of marketing experience or knowledge of their obligations under basic consumer protection principles, will unwittingly engage in Internet practices that violate the law. Finally, keeping up with the introduction and application of new technologies will prove daunting. The growing problem of "spam" already threatens to outstrip our resources. The Commission currently receives approximately 500 pieces of UCE per day, forwarded by disgruntled consumers and others -- far more than we can read or analyze on an individual basis and a volume that strains the capacity of the agency's computers.

To combat on-line fraud, the Commission will continue to use the Internet itself as a tool to improve and enhance our investigations. The Commission's staff all have Internet access, and scores of attorneys, paralegals, and investigators in our Bureau of Consumer Protection have received intermediate or advanced training on use of the Internet to combat fraud.²⁸

Looking into the future, we anticipate that traditional types of deception -- including pyramid schemes, bogus business opportunities, and failures to deliver promised goods or services -- will continue to top our list of Internet problems. The Commission will continue to be vigilant in monitoring the Internet for new schemes that ingeniously exploit the new technology, like the "Trojan horse" software scheme challenged in the *Audiotex Connection* case. Fighting fraud over the Internet is clearly a formidable task for the FTC's limited available resources. The Commission will do all it can, however, to curb this threat to the continued growth of the Internet and the benefits the Internet can bring consumers through speed, efficiency, convenience, and information never before available.

Conclusion

The Commission recognizes that we stand at a critical juncture in the development of electronic commerce. Although we have seen an explosion in on-line shopping and advertising, fraud and deception may deter consumers from acquiring a greater confidence in the Internet as a place to transact business. The Commission will continue its efforts to fight fraud and deception on line by implementing a comprehensive strategy that combines traditional law enforcement with aggressive consumer and business education.

²⁸ The Bureau of Consumer Protection's internal Internet Training Committee provided comprehensive one or two-day Internet training sessions in both 1996 and 1997. Not only did Commission employees attend, but also officials from the FBI, the Department of Justice, U.S. Attorney's Offices, as well as state representatives from the National Association of Attorneys General. The training covered legal issues, on-line fraud, emerging technologies, and investigational techniques.

EXHIBIT 1

**Anticipating the 21st Century: Consumer Protection Policy
in the
New High-Tech, Global Marketplace**

Anticipating the 21st Century:

Consumer Protection Policy in the New High-Tech, Global Marketplace

Volume II



A Report by Federal Trade Commission Staff

May 1996

Anticipating the 21st Century:

Consumer Protection in the New High-Tech, Global Marketplace

May 1996

FOREWORD

Every report is of necessity the product of many hands. This one is no exception.

The Bureau of Consumer Protection is grateful to the experts outside the Commission who helped identify the issues and speakers for the hearings on which this report is based; and to the hearing participants, whose thoughtful, lively, and provocative presentations continue to give us much food for thought.

Special debts of gratitude to those inside the Commission as well: Greg Hales and his colleagues, whose technical expertise during the hearings helped bring many presentations to light; the staff of the Bureau of Consumer Protection — especially Tom Rowan and Robert Lippman — who contributed talent, time, and energy to the effort; and Dawne Holz, who patiently prepared this report for publication.

Finally, a word of appreciation to our colleagues in the public and private sectors who are working with us to prepare for the critical issues facing businesses and consumers in the 21st century.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
THE NEW MARKETPLACE — AN OVERVIEW	1
BENEFITS OF THE NEW TECHNOLOGY	1
An Information Explosion	1
Greater Choice	2
Convenience	2
Consumer Sovereignty	2
THE FLIP SIDE: CHALLENGES OF THE NEW TECHNOLOGY	3
Increased Fraud and Deception	3
Detection and Enforcement	4
Legal Issues	5
Limited Resources	5
Privacy	6
Information “Have Nots”	6
Anti-Competitive Behaviors	6
TOWARD A NEW CONSUMER PROTECTION AGENDA	7
Working Together	7
The Role for Law Enforcement Officials	7
Industry’s Part	7
Consumer and Business Education	8
Self-Help	9
NEXT STEPS	9
TECHNOLOGIES ON THE MOVE	11
THE TELEPHONE	11
Consumer Protection Issues	13
Tackling Telephone Fraud and Deception: A Game Plan	15
TELEVISION	19
Consumer Protection Issues	20
Blueprint for Protection	21
CYBERSPACE	22
Newest Technology	22
Fraud and Deception in Cyberspace	28
The Search for Solutions	30
Privacy Concerns	35
LOOKING AHEAD: CONVERGENCE	38

GLOBAL TRADE AND CONSUMER PROTECTION STANDARDS	41
TOWARD A SINGLE GLOBAL MARKETPLACE	41
The Global Trade Picture	41
Divergent National Consumer Protection Standards	41
ROLE FOR THE FTC	43
Regulatory Review	43
Leadership Role in International Forums	43
CONCLUSION	45
GETTING AHEAD OF PROBLEMS	45
APPLYING LESSONS LEARNED	46
FTC FOLLOW-UP	47
ENDNOTES	49
APPENDICES	
HEARING PARTICIPANTS	A
HEARING AGENDA	B

EXECUTIVE SUMMARY

For four days in November 1995, the Federal Trade Commission explored consumer protection issues in the emerging technology-based marketplace. The hearings focused on three rapidly evolving communications technologies — the telephone, television, and computer — and on the special challenges of globalization.

The Commission's goal was to look ahead: to learn more about how these technologies are developing and how they may be used to market goods and services; to identify significant consumer protection issues associated with the new technologies; and to consider how best to address those emerging issues.

The Commission took testimony from more than 70 experts in the fields of law, business, technology, economics, marketing, consumer behavior, and consumer education. Their comments and observations provoked discussions that produced an especially rich hearing record. That record is the basis for this report.

While the hearings did not produce consensus on every issue, a number of themes emerged. Among them:

- *Information technologies are developing at a dizzying pace.* Next generation technology is already off the drawing board: interactive “smart” TV that lets consumers use their remote controls to order merchandise from home and get news on demand; full-motion video over superfast telephone lines; television that appears in the corner of desktop computer monitors — and much more. The changes in technology and their impact on the marketplace offer challenges and opportunities for law enforcement officials, businesses, and consumers.

- *The technologies may change the marketplace significantly for consumers — giving them access to potentially unlimited amounts of information, a global marketplace, and more shopping convenience.* Already, the Internet enables consumers to pick and choose the information they want from sources around the world, and to receive it at the click of a mouse. The next wave of telephone and television technologies also promises to offer consumers new information, shopping, and entertainment services.
- *New technologies may provide fertile ground for old-fashioned scams.* The Internet may allow scam artists to set up shop easily and cheaply, anywhere in the world, and skip out on unwary consumers without leaving a trace. Recent experience with new technologies, such as pay-per-call telephone services, suggests that fraudulent operators are quick to take advantage of new marketing tools.
- *New technologies are pushing some consumer issues — such as privacy, security, and marketing to children — to the forefront of public debate.* Millions of consumers, including children, are encouraged to use the Internet, and the number of people going online is growing daily. Broad-based accessibility to the new, and still evolving, technologies raises fundamental questions for policy makers, law enforcement officials, businesses, and consumers.
- *The challenges for government consumer protection agencies will increase at a time when their resources — human and financial — are stretched tighter than ever.* There is no sign that low-tech scams will go away, and strong evidence that “next-tech” scams will increase and be more difficult to detect and track across international borders. Law enforcement agencies must work harder, smarter, and in concert to maximize the impact of their limited resources.

- *As the new marketplace develops, it is in the interest of both the private and public sectors to see that sound consumer protection principles are in place. Private sector initiatives to assure consumer protection are crucial. Without these assurances, consumers may avoid the new technologies.*
- *Consumer protection is most effective when businesses, government, and consumer groups all play a role. Meaningful consumer protection takes: (1) coordinated law enforcement against fraud and deception; (2) private initiatives and public/private partnerships; and (3) consumer education through the combined efforts of government, business, and consumer groups.*

The report that follows is based on the written and oral testimony offered during the hearings. It attempts to capture the dynamic flavor of the discussions and to present the various views of the participants; it does not try to reconcile differences or offer definitive answers to emerging consumer protection concerns. It provides much food for thought and a wide range of suggestions on how best to protect consumers in the rapidly changing marketplace, and will be used to help the Commission staff plan a consumer protection agenda. Indeed, it will be followed next year by a report of the actions taken to deal with many of the issues raised during the hearings.

The report that follows also may serve as a basis for future dialogue and collaborative efforts by all those with a stake in consumer protection issues as the new marketplace unfolds.

THE NEW MARKETPLACE — AN OVERVIEW

From Main Street to Wall Street, electronic consumers are plugging in and logging on — surfing and chatting in a community that is at once world-wide and intimate. With the click of a mouse, they can read newspapers, tour museums, buy groceries, or send flowers to Mom. In short, their computers give them nearly instant access to information, entertainment, and merchandise.

For years, the telephone and the television have been the stuff of everyday life. As the technology of these tools converges with that of the computer, consumers will be offered more choice, more convenience, and more control than most of them ever thought possible. Unfortunately, they also may encounter new consumer protection problems at a time when resources at all levels of government are shrinking.

To deal with the concerns emerging in the new high-tech global marketplace, consumer advocates, educators, the business community, and government must join forces to design and implement measures to protect consumers, promote competition, and encourage the development of still more technology.

BENEFITS OF THE NEW TECHNOLOGY

An Information Explosion

The flood of information available to consumers is arguably the most dramatic development in the marketplace of the '90s. In just a few minutes on the Internet, consumers can research their hobbies, read up-to-date news summaries, and shop for cars. Although still in its infancy as a marketing medium, the Internet itself promises to grow exponentially in the next few years. Many expect online marketing and commerce to follow suit.

Consumers will be able to use the storehouse of information on the Internet to make better informed decisions,¹ although the availability of information does not

necessarily assure its use. Indeed, as the amount of information in the marketplace grows, some observers predict that consumers will be overwhelmed and confused.² Others forecast that consumers will face obstacles as they try to take advantage of the available data: for example, some consumers may not have full access to the information technologies, while others simply may lack the sophistication to use them.³

Greater Choice

Thanks to the Internet, consumers soon will find themselves in a global marketplace with more avenues for shopping, more options in terms of price and services, and more access to a seemingly endless array of products.

The Internet probably will not replace more traditional marketing vehicles.⁴ Yet even these vehicles — the television and telephone — are expanding the amount of information and the products they are able to deliver. Since the 1960s, for example, the number of television stations has tripled and the number of channels per household has multiplied sixfold.⁵ Telephone services are offering a constantly expanding range of information, products, and entertainment. For example, consumers now can sample and purchase compact discs on the telephone and receive full motion video over their telephone lines.⁶

Convenience

Consumer transactions online soon may become routine. Increasingly, it will be possible for consumers to conduct entire transactions online, from selecting products and negotiating prices to ordering and paying for goods, filling out product registration cards, and even receiving the products, when — like software — they can be transmitted that way.⁷ In the future, interactive television and the Internet may offer face-to-face shopping in the consumer's own living room.⁸

Consumer Sovereignty

The new interactive media have been hailed as “the first intelligent media on

the consumer side.”⁹ That is because the technology has the potential to give consumers greater control over the information they receive. On the Internet, for example, they can seek out the information they are interested in and ignore the rest.¹⁰

For years, the remote control has played a similar role for television viewers, but emerging technologies promise even more opportunities for consumers to regulate what comes into their homes via the television, the Internet, and the telephone.¹¹ Telephone technologies soon may give consumers the ability to block calls they do not want to receive, specify calls they will receive, and identify businesses that are calling.¹²

To the extent that control shifts from the media to the consumer, advertisers will have to provide messages that are more useful and interesting — or run the risk of being tuned out.¹³

THE FLIP SIDE: CHALLENGES OF THE NEW TECHNOLOGY

Clearly, the new technologies create exciting and numerous benefits for consumers. Just as clearly, they create new risks for consumers and uncharted territory for industry and government. The emerging areas of concern suggest that successful solutions call for creative thinking and cooperation among all interested participants.

Increased Fraud and Deception

Modern technology is partly responsible for the fact that fraud has increased markedly in the last 30 years.¹⁴ While most fraud in the 1960s took place face-to-face, often in door-to-door sales, today it is perpetrated on a massive scale, often over telephone lines.¹⁵

Globalization also has facilitated the boom in fraud. It is easy for fraudulent telemarketers to move their operations out of the country to avoid U.S. law enforcement, yet continue to scam American consumers.¹⁶ Many pay-per-call

scams and fraudulent telemarketing operations, for example, are moving overseas as a result of aggressive law enforcement at home.¹⁷

Fraudulent marketers will continue to use the telephone, but they soon may gravitate to the Internet in large numbers.¹⁸ Some of the same features that made pay-per-call technology so ripe for fraud artists in the 1980s — low start-up costs and the potential for big profits — exist on the Internet as well.¹⁹ Indeed, for \$30 a month or less and the cost of a computer and modem, scam artists can be in business on the World Wide Web, taking orders from anywhere in the world.²⁰ There is nothing new about the kind of fraud. What is new — and mind-boggling — is the size of the potential market, and the relative ease and low cost of perpetrating a scam.²¹

Detection and Enforcement

For law enforcement agencies, the emerging technologies present serious challenges in detection, apprehension, and enforcement. With a telephone or an online link, fraudulent marketers can set up shop quickly and cheaply, and move on without a trace. The fraudulent telemarketer, for example, can use pay phones and obtain payment through wired funds or credit card cash advances — with no listed or traceable phone, no mailbox, and no office. For the cyber scam artist, it may be even easier to escape detection. Once transactions can be completed online routinely — with cyberscammers getting consumers' money in seconds — the challenges for law enforcement will be even greater.²²

As the number of media sources grows, so does the job for law enforcement and industry self-regulating groups. Monitoring television advertising has become more difficult with the surge in the number of channels and the number of infomercials.²³ Monitoring the Internet will be an even tougher job. Yet, it is crucial, because new entrants may have little knowledge of their legal obligations under consumer protection laws.²⁴

Legal Issues

In the new marketplace, law enforcement agencies will have to contend with a daunting array of legal issues. Interstate and international electronic communications raise new concerns about the choice of laws and jurisdiction. Any global consumer transaction may be subject to varying legal standards for advertising, including claim substantiation, the use of sweepstakes, and rights to privacy.²⁵ The increasingly blurry line between advertising and content on television and the Internet also presents potentially thorny legal problems.²⁶

Online transactions raise a host of issues about the relative legal responsibility of participants in the new marketplace, such as service providers, home-page sponsors, and bulletin board operators.²⁷ Legal issues also may arise over new types of activities, like Web sites that directly interact with children and solicit information from them.²⁸ It may be necessary to reassess the applicability of some consumer protection standards in a new environment where consumers have more access to detailed product information.²⁹

Limited Resources

While consumer protection problems are growing in number and complexity, government resources at all levels are shrinking.³⁰ Indeed, as one top law enforcement official put it: It's not the telemarketing scam artists at the card table anymore. "They tend to be in nice big area rooms with computer screens at their tables. I'll tell you who's at the card table. It's law enforcement."³¹

The challenge for law enforcement agencies is to get the job done with fewer resources. They need to work smarter and more efficiently, maximizing their impact by working collaboratively with other agencies and the private sector. They also need to make greater use of the new technologies to combat fraud and educate consumers.

Privacy

While the emerging technologies may enhance consumer sovereignty, they may rob consumers of control in other areas, such as the collection and use of personal information. Advances in computer know-how already have enabled the collection, storage, and retrieval of enormous amounts of data on individual consumers without their consent.³²

It is likely that data collection will expand. Surveillance on the Internet can be all-inclusive: every movement can be tracked, including sensitive information about where consumers are shopping, what they're looking at, what they eventually buy, who they talk to, and for how long.³³ While the parties to a transaction may have access to this data, so will Internet service providers, online services, and electronic payment providers.³⁴

Information "Have Nots"

It is predicted that the new technologies will become more affordable, and ultimately, more widely accessible.³⁵ The growth in the use of the Internet may signal this trend.³⁶ Certain segments of the population, however, may miss out, either because they do not have the money to buy high technology items,³⁷ or they lack basic skills to use them. Without access to the new technologies, the poor, the under-educated, and minority groups in rural areas and inner cities may become a class of information "have nots."³⁸

Anti-Competitive Behaviors

In the rapidly changing high-tech marketplace, concerns exist about concentrations of power by the mega communications companies;³⁹ non-competitive "cooperative pricing" on the Internet where rival sellers will have total access to their competitors' prices;⁴⁰ and the creation of online entry barriers through search engines designed to push competitors out of the way.⁴¹

On the other hand, the new technologies may push the door open even wider

to competition, lower prices and a proliferation of new products and services.⁴² The Internet, with almost no barriers to entry, may create the most highly competitive marketplace of all.⁴³

TOWARD A NEW CONSUMER PROTECTION AGENDA

Working Together

Emerging consumer protection issues call for creative law enforcement approaches that do not unnecessarily restrict legitimate business practices, that promote the free flow of information, and that encourage the development of new technologies.⁴⁴ To strike the right balance, it will be important to continue the kind of dialogue that took place at the FTC's fall hearings, and for all interested groups — industry, government, consumer groups, and academics — to work together to find solutions.⁴⁵ Recent cooperative efforts in tackling pay-per-call fraud and telemarketing fraud can serve as useful models for solving the new problems identified during the hearings.⁴⁶

The Role for Law Enforcement Officials

Law enforcement agencies at federal, state, and local levels must continue to focus on fraud and deception in all forums. Enforcement resources should not be too narrowly focused on the new technologies; rather, they must be spread broadly to catch and deter the most serious wrongdoers wherever they work.⁴⁷ The FTC must maintain an active enforcement presence in the area of deceptive advertising — in both the print and electronic media — to assure that current standards are maintained.⁴⁸ In addition to its role as a vigilant law enforcement agent, the government should encourage self-regulation by the private sector.⁴⁹

Industry's Part

The private sector can address many of the concerns consumers have about the new technologies. It has the "know how" to find solutions that work without unduly burdening their operations. For example, industry can continue to develop

technological solutions that allow consumers to block receipt of certain kinds of information and let them know who is calling.⁵⁰ Private groups may be able to develop pro-competitive certification standards that help assure consumers of a seller's adherence to consumer protection principles; they also may be able to devise ways to resolve disputes using the new technologies.⁵¹

Self-regulation offers flexibility in solving problems. It provides an opportunity to proceed slowly in difficult areas like privacy; to build a consensus about norms of behavior for an industry; and to experiment with different approaches.⁵²

Further, self-regulation is in the business community's best interest because consumers will use only the new technologies in which they have confidence.⁵³ Without self-regulation in the pay-per-call technology, for example, scam artists gained the upper hand early on and nearly ruined the medium for legitimate use.⁵⁴ In short, if consumers see cyberspace as "Dodge City," they will stay away from it.⁵⁵

Finally, self-regulation can ease the burdens on law enforcement agencies. If industry is effective in promoting general levels of consumer protection, government agencies can focus their resources on fraud and deception.⁵⁶

However, it must be remembered that self-regulation can be uneven.⁵⁷ It generally needs a strong law enforcement presence, and constant renewal and modification to meet the challenges of a rapidly changing marketplace.⁵⁸

Consumer and Business Education

Consumer education fuels enlightened decision-making. This critical, albeit expensive, element of the consumer protection agenda should come from a variety of sources — industry, consumer groups, schools, and government agencies — working independently but cooperatively.⁵⁹

For government, a good place to start is right at home. Government agencies

must become more savvy about the new technologies and the consumer protection problems associated with them. In addition, they must learn how to use the technologies to disseminate their messages more effectively.⁶⁰ On the Internet, for example, it is possible to deliver consumer education messages in real time — that is, just as a consumer is about to make a purchase. This could be a giant step forward from traditional printed brochures and public service announcements.⁶¹

At a time when consumers are being bombarded with information, getting messages through can be difficult.⁶² And in some areas, such as telemarketing fraud, consumer education messages must change how people behave⁶³ — a daunting task. In the end, even the best consumer education cannot be effective by itself.

Self-Help

The new interactive technologies will offer interesting opportunities for consumer self-help. But consumers need to be educated and encouraged — and the technologies need to be developed — before any self-help measures can flourish.⁶⁴

NEXT STEPS

What's ahead? Government, industry, educators, and consumer groups are not yet sure, but none of them wants to be left behind. They are entering the emerging marketplace with cautious optimism. They are looking forward to more and better information, bigger markets, increased competition, and new opportunities for partnerships. Yet they are fully aware of the risks: new versions of fraud and deception, a world-wide stage for scam artists, and less privacy — at a time when there are fewer human and financial resources to address them.

TECHNOLOGIES ON THE MOVE

Many experts predict that the telephone, the television, and the Internet will evolve, converge, and take on a new look. The familiar media still will be around, but may evolve into nearly unrecognizable tools that will energize the marketplace in new ways.

THE TELEPHONE

The expansion of the telephone from just a simple medium for personal conversation into a global platform for commerce is a key technological development in the new marketplace.

Now a medium for digital as well as verbal communication, the telephone is an important vehicle for buying and selling entertainment, information, and other products and services. For example, consumers now can listen to and order compact discs and other recorded music simply by calling an 800 number.⁶⁵

Indeed, the telephone infrastructure supports a large and still growing segment of the U.S. economy. The fact that it relies on the old-fashioned advantages of telephony — ease of use, affordability, security, and reliability — is particularly noteworthy.⁶⁶

It is no surprise that the telephone is nearly ubiquitous. Consumers like it because it is familiar, easy to use, convenient, inexpensive, reliable, secure, and private;⁶⁷ marketers like it because it offers one-to-one personal communication that can be tailored to consumer interests and concerns.⁶⁸

Since the 1970s, advances in telephone technology have spurred the use of the telephone as a marketing tool.⁶⁹ Digital technologies are reconfiguring old copper telephone lines to carry huge volumes of information at extremely high speeds.⁷⁰ Telephone wires already are carrying full motion video.⁷¹ Commercial transactions are taking place over these same wires using new “smart card” technology.⁷²

The Telemarketing Industry

Forty or 50 years ago, when telephone commerce was new, consumers generally were so pleased to hear from a telemarketer that he had to work to conclude the calls.⁷³ Today, however, many consumers regard the high volume of telephone solicitations as an irritation and an invasion of privacy.

Concurrent advances in database and telephone technology fostered the growth of an enormous telephone marketing industry.⁷⁴ Indeed, telemarketing is the lifeblood of many companies. At least one major long distance company says its sophisticated telemarketing sales program is responsible for its rapid expansion.⁷⁵

In addition to being a boon for business, telemarketing offers consumers convenience — the chance to buy a wide range of goods and services from their homes.⁷⁶ However, some telemarketers warn of a danger of “over fishing” their market.⁷⁷ If a negative image of telemarketing gets lodged in the public mind, consumers may stop responding to telemarketing solicitations. Support may grow for the same kinds of strict telemarketing laws and regulations that some foreign governments have.⁷⁸

The Pay-Per-Call Industry

The pay-per-call industry uses 900-number technology to market entertainment and information services.⁷⁹ Once considered a business with enormous potential, the pay-per-call industry has yet to meet expectations, largely because it was tainted early on by scam artists who adopted the technology in large numbers. Increasingly, however, the legitimate pay-per-call industry is offering business-to-business and business-to-consumer services, and major corporations are turning to pay-per-call services to replace toll-free 800 number operations.⁸⁰

Like their counterparts in the telemarketing business, pay-per-call industry representatives rank convenience as one of their industry's top benefits for

consumers. The 900 numbers offer consumers a quick and handy way to access information and entertainment services. In addition, pay-per-call service is available in virtually all homes, not just those with personal computer systems or those that subscribe to costly electronic information services.⁸¹

Consumer Protection Issues

Telemarketing Fraud

The elements of consumer fraud are the same today as they were in the days of face-to-face snake oil sales. Today, however, fraud is perpetrated on a massive scale over telephone lines. What is different about phone fraud is that the technology enables the con artist to scam many more consumers — and to hide the essence of the fraud because the consumer can't inspect the goods.

Many big telephone scams are low-tech;⁸² they use psychological tactics that play on the fears and hopes of the victims. Increased economic pressure, stagnant personal income growth, and a sense of powerlessness also make some consumers susceptible to fraud.⁸³ Sweepstakes, lotteries, and “get-rich-quick” schemes offer opportunities to ease financial strains,⁸⁴ and the techniques used by fast-talking scam artists are smooth enough to fool even savvy consumers.⁸⁵ Indeed, while older people are most often the victims of telemarketing fraud,⁸⁶ no demographic group is immune: doctors, lawyers, accountants, and corporate presidents of all ages are among those who have been scammed.⁸⁷

More sophisticated technology and a global marketplace will make it more efficient for con artists to defraud even more consumers.⁸⁸ Fraudulent telemarketers use new high-tech tools to develop sucker lists with names of people who have “bitten on” scams before.⁸⁹ Telemarketers also are expanding their operations into foreign countries. The new technologies make it as easy to telemarket from Canada as from any one of the states.⁹⁰

Pay-Per-Call Deception and Fraud

With low entry costs and the promise of big payoffs, the pay-per-call 900-number industry has been a powerful magnet for scammers. The typical deceptions include:

- advertisements that do not fully disclose the price of calls;
- useless introductory information designed to drive up the costs of calls; and
- failure to provide recourse for consumer complaints or inquiries.⁹¹

To escape U.S. law enforcement, 900-number crooks have re-routed their telephone calls to networks in foreign countries.⁹² Now, they can direct a call from Kansas through Sao Tome (a small country off the west coast of Africa) to New York "in the blink of an eye."⁹³ Newspaper ads for pay-per-call services may list local or toll-free telephone numbers. When consumers call, they are invited to make a second call to an 809 area code number. Unaware that they are now making an international call, consumers believe that they are being charged 15 cents a minute when, in fact, they are being charged \$15 a minute.⁹⁴ At the end of the month, consumers are surprised to receive thousand-dollar phone bills, which, if unpaid, could cost them their phone service.⁹⁵ The growth in international pay-per-call services has been staggering, with four to six million minutes of U.S.-based telephone calls a month being placed to services based in only five countries overseas.⁹⁶ The annual profits for international pay-per-call operations are now estimated at \$250 million.⁹⁷

Still Ahead: Challenges to Law Enforcement

The growth in telephone fraud poses many challenges for law enforcement agencies at a time when their budgets are especially tight. New technologies allow con artists to avoid physical locations that can be detected by law enforcement agents.⁹⁸ Working alone, the cons operate without a fixed address, office, or even telephone number by using pay phones and convincing victims to make instant wire transfers, ATM transfers, or credit card cash advances wired to

convenience store outlets.⁹⁹ This so-called “phantom phone fraud” is almost impossible to monitor¹⁰⁰ because scam artists can “cover their moves” by leaping — technologically — from place to place when they really are “around the corner.”¹⁰¹

Law enforcement agencies also are challenged by new payment systems that transfer funds instantaneously. While the technology — and its resulting efficiency — makes consumers’ lives easier, it also benefits scam artists by making it easier to collect consumers’ money before the consumers realize they have been scammed.¹⁰²

Detection, apprehension, and enforcement become even tougher when fraudulent telemarketers move abroad.¹⁰³ The global market may be a business reality; but for law enforcement agencies, the world marketplace remains fragmented, making it more difficult to stem — let alone prevent — consumer injury.¹⁰⁴

Tackling Telephone Fraud and Deception: A Game Plan

It is in the interest of legitimate business to see that telemarketing works fairly.¹⁰⁵ Government, too, seeks solutions that recognize the legitimate concerns of this industry, keep regulatory burdens to a minimum, and prevent consumer injury.¹⁰⁶ Recent examples include the Commission’s Telemarketing Sales Rule and its 900-Number Rule.¹⁰⁷

All stakeholders — government, industry, and consumer organizations — must work together to address the many consumer protection problems in the use of this technology.¹⁰⁸ Tackling telephone fraud, for example, requires a multi-pronged approach — government regulation and law enforcement, business self-regulation, and consumer education.¹⁰⁹ One part of this framework alone — for example, self-regulation without consumer education or enforcement — will not have much impact on the fight against fraud.¹¹⁰ The collaborative efforts involved

in the Commission's recent rulemakings to stop telephone fraud and abuse may provide models for addressing the next generation of consumer protection problems.¹¹¹

Law Enforcement — National and International Cooperation

A principal role of law enforcement agencies is to deal with the increasing volume of phone fraud.¹¹² To maximize limited resources, it is more important than ever that local, state, and federal agencies work together, as well as with foreign governments.¹¹³ They must continue to share expertise¹¹⁴ and data, and redouble their collaborative efforts in carrying out major law enforcement initiatives.¹¹⁵

With the increasing problem of cross-border telephone scams, there is a need to educate law enforcement agencies and judges around the world about the importance of this problem.¹¹⁶ U.S. agencies must work with other countries and develop better means of communication, to the extent possible, to facilitate cooperative relationships among law enforcement agencies.¹¹⁷ In addition, law enforcement entities throughout the world must address the transfer of property by con artists to foreign jurisdictions as a way to avoid asset seizures.¹¹⁸ In sum, law enforcement must become international to remain effective.¹¹⁹

Private Sector Initiatives — Early Self-Regulation

Industry has a responsibility and a strong interest in developing and adhering to self-regulatory regimes that reduce fraud.¹²⁰ Bank card companies, for example, bear much of the cost of telemarketing fraud¹²¹ and cannot wait for law enforcement agencies to solve the problem.¹²² Similarly, legitimate telemarketers, hurt by the crooks who make consumers skeptical of all telemarketers, want to help the public learn to tell the difference.¹²³

The history of the 900-number services industry should alert all industry members to the hazards of neglecting self-regulation. In the 1980s, the industry failed to crack down on bad actors. The result: consumer complaints, negative

media attention, and ultimately, comprehensive government regulation. The industry's failure to take an early and pro-active role in helping to solve the problem allowed the con artists to take over. Pay-per-call, which had grown quickly to a billion-dollar industry, lost \$400 million in one year.¹²⁴

Some self-regulatory programs already are in place:

- The Direct Marketing Association's (DMA) mail and telephone preference service allows consumers to write to a central address to remove their names from promotion lists; companies maintain their own do-not-call lists that they check regularly against DMA's.¹²⁵
- Notice and opt-out cards appear as inserts in magazines and bills, so that customers can indicate they do not want to be called.¹²⁶
- The bankcard industry contacts consumers under certain circumstances to verify a transaction.¹²⁷
- The bankcard industry supports careful merchant signing procedures, monitoring, and education to combat "laundering" of credit cards by con artists. In addition, the industry supports extension of deadlines for credit card holders to report fraud.¹²⁸
- Major U.S. long distance and local telephone carriers do not collect payment from consumers who have been deceived; some local telephone companies do not terminate phone service for non-payment of legitimately disputed charges.¹²⁹
- The American Telemarketing Association (ATA) is developing a certification process to hold member telemarketers to stringent standards.¹³⁰
- The DMA and the ATA have ongoing programs to educate and monitor their members and plan to institute a formal program to encourage the 11.1 million employees engaged in direct marketing to be vigilant about telemarketing fraud and active in reporting it.¹³¹

Companies that inadvertently assist fraudulent telemarketers, such as banks, credit card companies, shipping companies, mailbox companies, and wire transfer companies, also can play a part in these protection efforts. Once aware that con artists are using their services, they can cut them off.¹³²

Technological Solutions

Technology also must be part of the solution to consumer protection problems.

Among the possibilities:

- An automatic call back feature so consumers can verify who called them.¹³³
- An electronic filtration device to help consumers distinguish between legitimate telemarketers and crooks.¹³⁴
- Caller ID to allow consumers to manage a list of telephone numbers they will not accept calls from, or that they will only accept calls from.¹³⁵

Consumer Education

Consumer education can help stop the growth of telemarketing fraud — although it can be a daunting task to get an effective message through to those who are most susceptible.¹³⁶ A recent study by the American Association of Retired Persons revealed that older people — who are especially vulnerable to telemarketing fraud — need clear and concise triggers to help them recognize telephone scam artists and distinguish them from legitimate telemarketers. Mere awareness that scams occur is not enough: the study showed that many older victims already were skeptical of telephone solicitations when they were scammed.¹³⁷ Older consumers need help developing skills to deal with all telephone solicitors, and saying no to — or hanging up on — those they really do not want to do business with.¹³⁸

Consumer education can be expensive, and broad dissemination is difficult. Even so, it is important to keep consumers abreast of the risks they are facing in the changing marketplace.¹³⁹ Government and industry should be partners in these

education efforts. Industry knows how to reach its customers best. It also is in the best position to tell vast numbers of consumers how to separate the legitimate offers from the fraudulent ones.¹⁴⁰ Many industries already are involved in doing so.¹⁴¹ They need to continue, and others need to join in.

TELEVISION

Television has changed dramatically since the 1960s. Consider these statistics:

- Americans had access to almost 1900 local television stations in 1995, more than three times the number available in 1965;
- An estimated 63 percent of homes received cable television in 1995, up from five percent in 1965;
- The average household received 41 channels in 1995 — 34 more than in 1965;
- More than two-thirds of American households had more than one television in 1995; in 1965, only 28 percent had more than one TV; and
- Nine out of 10 households had remote controls for their televisions in 1995; more than eight out of 10 had video cassette recorders. In 1965, neither technology was available.¹⁴²

The television landscape has been forever changed. The number of local stations has skyrocketed, and technological innovations have given consumers more control over how and when they watch television. More outlets for programming and advertising are enhancing consumer and advertiser choice. In addition, audiences are becoming more fragmented as viewers time-shift, zip, zap, and graze at their multiple sets, video cassette recorders, and remote controls.

Changes in technology also have fueled advertising and marketing innovations. Television advertising dollars now are split among six broadcast networks, which share 33 percent of the ad dollars, and cable and syndication,

which share 14 percent.¹⁴³ Only 25 years ago, three networks — ABC, CBS, and NBC — shared 46 percent of total TV ad dollars.¹⁴⁴ The relationship between programming and advertising also has changed. In television's early days, advertisers produced both programs and ads. The line separating one from the other often was blurry. It became sharper as the networks produced the programs and advertisers the commercials. Recently, however, with the development of infomercials and shopping channels, the line is blurring again.¹⁴⁵ Indeed, soon there will be three cable television channels devoted entirely to paid programming.¹⁴⁶ The convergence of television and personal computers may further cloud the distinction between advertising and programming content.

Consumer Protection Issues

An Advertising Avalanche

The explosion in television outlets has meant an increase in both the number of new avenues for advertising and the number of ads for law enforcement agencies to monitor. In addition, ads may use new technology to portray products in a way that may deceive viewers. For example, advances in video technology, such as digital manipulation, raise particular concerns in the area of children's advertising.¹⁴⁷

Who will keep track of all of this new advertising? In an era of reduced human and financial resources, the federal government may not be able to adequately monitor this avalanche of new ads.¹⁴⁸ In any event, monitoring alone is not enough to protect consumers from deceptive ads.¹⁴⁹

Uneven Review Procedures

While networks and network owned-and-operated stations tend to have sophisticated procedures to screen for deceptive ads, independent and cable stations have varying levels of review.¹⁵⁰ In one recent survey of 30 cable networks, only four percent required advertisers to substantiate claims.¹⁵¹ With

more stations and networks available, consumers may not always know which outlet they can trust.¹⁵² While industry groups are becoming more active in the screening arena, it is clear that more efforts are needed.¹⁵³

Blueprint for Protection

Concerted Efforts

As more television outlets for advertising appear, old-fashioned types of deception will proliferate.¹⁵⁴ Simply finding all the ads that are being disseminated is challenging.¹⁵⁵ Surely, no one entity can monitor them all. All facets of the television industry — advertisers, advertising agencies, the media, trade associations, and self-regulatory organizations — must work alongside government to ensure that consumers are protected from deceptive ads.

Stepped-up screening

Self-regulation by all members of the television industry is crucial to reducing deceptive advertising. However, since the strength of these self-regulatory measures varies widely, a more uniform effort across the industry is needed.¹⁵⁶

Stronger screening efforts by new members of the television industry are especially important.¹⁵⁷ All members of the industry should work to ensure that the existing resources become better known — through challenges brought to the National Advertising Division and the Children's Advertising Review Unit of the BBB, to networks, and to individual stations.¹⁵⁸ Industry members should urge trade associations to establish review mechanisms and guidelines.¹⁵⁹ They also must lend financial support to self-regulatory efforts and related activities, including educating new businesses, media, and consumers.¹⁶⁰

Government Involvement

Effective industry self-regulation is not a substitute for government oversight.¹⁶¹ Indeed, self-regulation has inherent limitations, and certain issues simply are not suited to self-regulation. But government can encourage self-

regulation. Indeed, the power enjoyed by industry self-regulation groups ultimately comes from the existence of the FTC and its enforcement powers, which serve as a backstop to self-regulatory measures.¹⁶²

The FTC's primary consumer protection role is to stop the fraudulent and deceptive marketers who operate outside the legitimate field.¹⁶³ It also must address novel deception issues.¹⁶⁴ At the same time, it should do its job in a way that avoids unnecessary regulatory roadblocks.¹⁶⁵ This is an important goal under any circumstances, but may be particularly critical at a time when television is in transition.¹⁶⁶

CYBERSPACE

Newest Technology

A Brief History

By any measure — traffic, number of users, money spent — the growth of the Internet has been phenomenal.¹⁶⁷

Originally a military communications system, the Internet was expanded to include research institutions.¹⁶⁸ Private entities were permitted to offer commercial access to the Internet in 1992, and by 1995, the government's involvement was phased out.¹⁶⁹ World Wide Web technology, which made the Internet useful in an everyday way, appeared around 1992.¹⁷⁰

The Internet now is an interconnected web of 60,000-plus computer networks in over 90 countries that routes communications among users. The path of any individual Internet communication is not predetermined or controlled: indeed, the system automatically routes around system outages. Information posted in one location is accessible everywhere simultaneously.¹⁷¹

From the consumer perspective, 1995 was the year the Internet "arrived." More affordable high-speed multimedia home computers, faster modems, and more sophisticated software compressed the time needed to access information

and download files. As technology advances, Web sites will go beyond text, graphics, and photos to incorporate audio and video clips.¹⁷²

For Consumers The Internet provides consumers with unparalleled access to information. An online consumer in the market for a new car, for example, will find “virtual showrooms,” discount broker ads, classified ads, buying guides, consumer protection information, and “tips” from self-styled experts on the tricks of negotiating the purchase.¹⁷³

Ideally, interactive marketing puts consumers in control,¹⁷⁴ enabling them to determine what information they access.¹⁷⁵ This may lead advertisers to create communications that entice consumers to view their ads and to act more like door-to-door merchants, seeking a one-on-one dialogue with consumers and potential customers. Unless advertisers offer accurate information tailored to the consumer’s needs and desires, the consumer may not “invite” them in.¹⁷⁶

While the new consumer sovereignty may be liberating, information overload may make informed choice particularly difficult in the online marketplace.¹⁷⁷ Today’s electronic consumers have little control over unsolicited postings that flood electronic mail boxes, newsgroups, or other bulletin boards. If not addressed, such “spamming” practices could hinder the healthy growth of the Internet.¹⁷⁸

For Marketers Interactive technologies demand active, deliberate user participation and provide an opportunity for real-time, two-way communication between an advertiser and a consumer.¹⁷⁹ Cybercommunications fuse traditional marketing techniques, borrowing from advertising, promotional marketing, public relations, newspaper inserts, and catalogs.

Electronic marketers instantly may access customers from Vermont to Vietnam.¹⁸⁰ The interactive ad can become a “virtual” store, where an advertiser completes the sale — and sometimes even the delivery of its products or services — online, blurring the lines between communication, distribution, and sales, and

perhaps redefining advertising and marketing as we know them. Any product or information that can be digitized — software, databases, everything in print, sound, or pictures — can be delivered online.¹⁸¹

It doesn't take much to set up a base of operation on the World Wide Web: a personal computer, a modem, a little software — all of which can be bought new for under \$1000 — and an Internet connection, which costs \$30 or less a month.¹⁸² Indeed, cyberspace may be a better market for alternative voices or niche markets than either cable or broadcast, in part because there is no “cyber-gatekeeper” with the power to determine who can, or cannot, market online.¹⁸³

On the other hand, simply having an online presence does not assure success. Consumers must be made aware of the site, and enticed to visit.¹⁸⁴ Power-house brands and the leading sellers in traditional electronic markets may be able to dominate cyberspace — the former because they are in a better position to publicize their online sites in other media and attract more traffic,¹⁸⁵ the latter because of their greater entertainment-related resources.

Online technology enables marketers to track a consumer's behavior throughout an interaction¹⁸⁶ and, therefore, permits them to identify new customers at very little variable cost.¹⁸⁷ Although this raises privacy concerns, it allows marketers to better understand the user's needs and desires and to screen out irrelevant data.

Where Are We Now?

Most major advertisers have Web pages on the Internet, and many include their Web site addresses in their TV and print ads.¹⁸⁸ In turn, some advertising agencies have entered the world of interactive advertising, creating Web sites and CD-ROMs, programming for online service providers, and even advertising in “digitzines” (online or CD-ROM magazines).¹⁸⁹

Yet many current online advertisers are still in the dark about the return on their investment. Most investments in Internet-related activities are in research

and development, with the value of this new advertising and marketing channel still to be determined.¹⁹⁰ For some companies, an Internet site has more to do with creating a perception in the target market that the company is “cool” or “hip” than anything else.¹⁹¹

Where Are We Going?

While it seems certain that commerce on the Internet will grow dramatically in the next 10 years, few are willing to predict exactly how the new marketplace will develop. However, one witness at the hearings suggested that the market might take three different directions.

Under his “Yahoo Scenario,”¹⁹² the Internet would be dominated by mega-advertisers with fabulous Web sites designed to “catch” the consumer. These sites would be promotional playgrounds or sponsored worlds that would hold the consumer’s attention by changing constantly. Advertisers would enter into exclusive agreements with big-name celebrities to connect with their fans at the advertiser’s online site. Joint advertising promotions would proliferate; consumers would be pointed from one offer to the next; and the role of content providers, if they existed at all, would be to catch a particular demographic segment and then bounce them to an advertiser’s Web site.

Under his “Disney Scenario,”¹⁹³ mega-entertainment providers would dominate the Internet. Traditional media-advertiser relationships would be transferred to the new medium of cyberspace and content would be the magnet to attract users. Large, value-added media worlds would merge, often replacing the ones people know. While thousands of content providers might exist, only a few would dominate, offering elaborate multimedia sites where consumers gradually would spend more time. These sites would be creative empires, providing personalized entertainment and information value. Marketers would nest in these mega-brand sites, staking out territory like they do at the Olympics. Only the biggest brands would have the resources to buy this presence, and exclusive

relationships could arise between marketers and content providers. Here, marketing messages and entertainment content would blend into a seamless experience.¹⁹⁴

Finally, under his third scenario — “The Net as a Tool”¹⁹⁵ — consumers would not view the Internet as a source of entertainment or fun, but rather as a tool to accomplish mundane tasks more conveniently and cheaply than they might through conventional means. The dominant marketing application for the Internet would be customer service, similar to services now provided via 800 numbers. Consumers would go online to research products and prices, pay bills, register complaints, download a prospectus from a mutual fund provider, or check their bank balance.

Bumps in the Road

Some challenges must be addressed if the electronic marketplace is to realize its full potential.

Legal Uncertainties Because a message on the Internet is immediately accessible worldwide, it is potentially subject to a variety of laws governing advertising methods. Which country’s laws will prevail?¹⁹⁶ Enough areas of uncertainty exist to cause concern about conflicting liabilities among online players.

The appropriate treatment of intellectual property in cyberspace is another area of uncertainty. International laws in this area are inconsistent, and have caused conflicts in GATT and treaty negotiations for years. Some would say that intellectual property owners must be assured that their valuable property is not at risk, and that their credibility will be protected.¹⁹⁷ Others assert that overbroad intellectual property protection will stifle innovation on the global information infrastructure.¹⁹⁸

Other areas of uncertainty include the allocation of liability among advertisers and online service providers for copyright infringement, libel, and fraud,¹⁹⁹ and an

advertiser's liability when its messages are duplicated and re-worded on the Internet.²⁰⁰ The legal responsibilities of parties that sponsor Web sites or online bulletin boards also have yet to be clearly defined.²⁰¹

Payment Security Payment security issues continue to be a major concern for Internet marketers and users. In a recent survey, the vast majority of adult online users said that it is too easy for a credit card number to be stolen if it is used on the Internet, and that more Internet security is needed.²⁰²

There still is no widely used, secure way to pay for goods and services on the Internet, although such a system is under development.²⁰³ The conventional wisdom is that the Internet's potential as an electronic marketplace will explode when reliable payment mechanisms are established. This expansion of electronic commerce could parallel the growth in catalog sales during the last 10 years.²⁰⁴ Then other problems may arise, however, involving authorization, rights of rescission, charge backs, and cancellations.²⁰⁵

Consumer Confidence The commercial health of cyberspace will turn on consumer confidence.²⁰⁶ Doubts and insecurities could keep people away, capping the growth of the medium.²⁰⁷ Lawlessness, or even the threat of lawlessness, could dramatically limit the usefulness of the Internet to consumers.²⁰⁸

Businesses, too, want consumers to feel "safe" while doing business in cyberspace and are rooting for this electronic medium to realize its potential.²⁰⁹ It would be a disaster for advertising in the cyberworld to lose credibility because of the ease of disseminating false claims.²¹⁰ To assure consumer confidence, brand names — those that inspire credibility and trust — probably will continue to be important on the Internet.²¹¹

Access to the Technology According to the testimony, the new marketplace must be widely accessible to consumers. Some suggest that access to online services is expanding. The Internet now is open to anyone, not just those

associated with a university, research institute, or the government. Competition has pushed prices down, and commercial online services are moving into rural areas. More affordable Internet access may have to do with the fact that phone service — the way most users access the Internet — has been highly regulated.²¹²

In addition, advertising could speed the accessibility of the information highway, just as it supported the development of radio and television, and brought news and entertainment to a bigger audience.²¹³ The traditional advertiser subsidization of content may change, depending on how the Internet develops as a marketing tool.²¹⁴

However, the new information age may produce “haves” and “have nots”; information “have nots” are likely to be located in rural areas and the central cities, and to be less educated, members of a minority, and poor.²¹⁵ No one knows how the universal service question will play out in cyberspace, but one way or another, its resolution will have an important impact on electronic commerce.

Fraud and Deception in Cyberspace

Much of the fraud online will continue to be old hat. Scam artists are able to operate much as they have in the past, preying on greed, loneliness, naivete, and other human frailties.²¹⁶ The Internet offers crooks some powerful advantages, however. It enables them to identify potential victims more efficiently by tracking and profiling a consumer’s Internet activity.²¹⁷ It also offers low operating costs, anonymity, and instant access to consumers worldwide.²¹⁸

Ease of entry means that the Internet, like the telephone, is fertile ground for fraud. But consumer damage in cyberspace can be more significant and happen faster.²¹⁹ Entire transactions, from offer and acceptance to payment and perhaps delivery, can be accomplished with just a few clicks.²²⁰

Once a secure online payment system is in place, the sheer volume of transactions will present a real challenge to law enforcement.²²¹ Electronic

payment systems could reduce or eliminate delays or cooling-off periods available to consumers under conventional payment systems such as personal checks and credit cards.²²²

Cyberspace also makes it more difficult for law enforcement officials to identify and locate perpetrators of fraud. The technology helps scam artists escape detection, for example, by allowing them to change their name or persona in cyberspace.²²³

The ease of electronic communication often means that there are no boiler rooms to raid, no offices or warehouses to check, and no employees to pursue.²²⁴ And given the transitory nature of much online information, even the fraudulent come-ons may not exist long enough for officials to obtain copies.²²⁵ New payment systems may increase the difficulties associated with investigating fraud by eliminating the need for information such as postal addresses and telephone numbers — information now used by law enforcement officials to locate crooks.²²⁶

Cyberspace lacks physical boundaries, creating both practical and legal issues for law enforcement. What about the crook outside the U.S. who designs a Web page to peddle pirated U.S. software? Does the United States have jurisdiction over the foreign seller if a U.S. citizen accesses the Web page and places an order? How do U.S. authorities find the seller? Will the host country cooperate? If not, is there a technological way to block that seller from sending e-mail into the United States or to block U.S. citizens from accessing the seller's Web page?²²⁷

Cyberspace users constantly transform the medium. The combination of unstructured input and ever-evolving technology means that law enforcement officials may have to run to keep up.²²⁸

Digital technology offers new opportunities to mislead consumers by tampering with logos and trademarks online. Legitimate advertisers' credibility

can be harmed by the unauthorized use of forged or reformulated advertisements.²²⁹ Web site developers can manipulate data to ensure that a particular site is included on the "hit lists" produced by online search engines, even when the search topic is unrelated. This manipulation, similar to traditional bait-and-switch tactics, is designed to catch unsuspecting consumers.²³⁰ The popularity of a Web site can be inflated through software that quadruples the actual number of "hits," or access requests, received by a site.²³¹

Online advertising aimed at children is among the special problems posed by the Internet. Concerns focus on the solicitation of personal information from children, the blurring of advertising and entertainment, and the creation of sites that offer direct interaction with products or "spokescharacters" or encourage children to spend unlimited amounts of time.²³² Direct marketing of products to children through "electronic boutiques,"²³³ and children's access to sites advertising tobacco or alcohol also are areas of concern.²³⁴

The Search for Solutions

Law Enforcement Agencies The online marketplace cannot be the "Wild Web"; it must offer some measure of meaningful consumer protection to succeed.²³⁵ Enforcement agencies must adapt quickly to this new medium. They must become technically literate to identify problems and to understand the level of protection online users want and expect.²³⁶ Yet it is not clear how best to afford consumer protection to online users²³⁷ especially in light of the constantly changing nature of cyberspace.²³⁸

Preventing or dealing with online fraud requires monitoring and enforcement, and may even call for new legislation and rulemaking.²³⁹ While efforts by law enforcement agencies to focus on fraud are important to the success of the medium, substantially more resources may be needed to do the job right. Otherwise, agencies could be overwhelmed by the caseload.²⁴⁰

To deal with cross-border Internet fraud, the U.S. can, in appropriate cases, seek help from, or offer help to, foreign governments under existing or new legal assistance treaties.²⁴¹ It also may be necessary to create specialized investigatory and enforcement institutions, public or private, to seek relief for Internet victims or sanctions against wrongdoers.²⁴²

The role of law enforcement agencies regarding online advertising aimed at children raises particular concerns. Should a regulatory framework for such advertising be established to ban certain conduct like collecting personal information from children?²⁴³ Or is regulation premature because the advertising industry is moving to deal with this area itself?²⁴⁴ Are the principles that apply to children's advertising in other media suitable for online advertising?²⁴⁵ A comprehensive evaluation of children's advertising in the context of cyberspace may be needed.²⁴⁶

Business is not the only human activity conducted online. The Internet's potential for communication, research, entertainment, and education throughout the world — and the spirit of its users and its dynamic nature — should not be stifled by over-regulation.²⁴⁷

In addition to traditional enforcement, some have urged that the Commission encourage businesses to self-regulate by proposing enforcement or regulatory action, then soliciting industry response. The resulting dialogue between the Commission and industry may lead to innovative solutions and avoid unnecessary government action.²⁴⁸

Private Initiatives Self-regulation may offer some of the most promising avenues for consumer protection in this new medium, without inhibiting its development.²⁴⁹ A number of self-regulatory efforts are underway:

- The National Advertising Division of the Council of Better Business Bureaus currently applies its existing review process to cyberspace advertising and is considering an online certification program. Under this

program, companies that adhere to certain BBB standards and procedures would be authorized to display the BBB logo in their online ads.²⁵⁰

- Private businesses might develop to preview or vouch for online sites or goods. Examples include consumer subscription services that publish independently-conducted evaluations of products offered online and companies that sell “consumer insurance” to online marketers.²⁵¹
- The private market also can take on the arbitration of online disputes.²⁵² To accommodate the global nature of many disputes, hearings can be conducted through computer networks. Under existing treaties, enforcement of arbitration awards is more likely than enforcement of foreign court judgments.²⁵³ Online service providers and Web sites could state “terms of service” specifying the use of such mechanisms.²⁵⁴

One such system is the new Virtual Magistrate service, which is aimed at resolving disputes over messages or information posted in online forums or bulletin boards.²⁵⁵ A panel of neutral experts reviews disputed material and recommends within 48 hours whether it should be deleted by the forum or bulletin board operator.²⁵⁶

- Software filters can be programmed to block access to certain topics or categories of information, and software-based ratings systems are already available to advise consumers about visiting particular sites.²⁵⁷ Such tools could be crucial for consumers who want to make informed choices about the Internet sites they or their children access.²⁵⁸

One system — the Platform for Internet Content Selection (PICS) — is being developed by a group including online service providers and communications companies in conjunction with MIT’s World Wide Web Consortium. The technology standards produced by PICS will be available to any third party — consumer groups, children’s advocates, or religious organizations, for example — to design competing systems rating

World Wide Web sites.²⁵⁹ Consumers could then access or block Internet or Web sites based on the ratings service they choose.²⁶⁰

- The online industry may prevent scams by policing itself once key liability issues have been sorted out by the courts or by Congress. For example, service providers might develop a shared list of subscribers or advertisers expelled from one service in an effort to prevent them from jumping to another service.²⁶¹

Joint Private/Public Sector Actions Government, consumer protection advocates, and the private sector must work together to protect online consumers. State and federal regulators already are working with the online services to address current challenges.²⁶² Information sharing and education are central goals of these efforts. Given the speed with which issues in cyberspace change, law enforcers, online service providers, and consumer advocacy groups might do well to conduct regular conference calls to discuss the latest scams.²⁶³

Consumer protection organizations can help the Commission's enforcement efforts by serving as an early warning mechanism for scams.²⁶⁴ There also may be ways to combine the advantages of FTC oversight and private dispute resolution. Indeed, the development of formal mechanisms for deferring to private channels — similar to the federal government's reliance on the securities and commodities exchanges to self-regulate their markets, or the National Labor Relations Board's policy of deferring to collectively bargained arbitration — should be considered. The FTC could decline to consider matters that have not been presented to available private channels, choose to give effect to the decisions of private tribunals, or both.²⁶⁵

Consumer and Business Education Education will be crucial in battling the online scams of the future. This task must be undertaken by all the stakeholders — marketers, government agencies, the online industry, consumer advocates, journalists, and online users themselves. The need will grow as the number of

consumers online swells. Consumers will need information about online scams and about the operation of cyberspace itself.²⁶⁶

Cyberspace offers unique opportunities to provide more effective, "point-of-purchase" education to consumers. Because an online search for a product will list consumer information sites along with advertising or other sites relevant to the search topic, educators can deliver information when consumers are likely to be most receptive.²⁶⁷

The potential to disseminate consumer information when the consumer is interested could be expanded through advertisers' incorporation in their Web sites of cross-links to appropriate consumer information sites. Commercial online services can include pop-up screens or click choices that describe online consumer information resources next to relevant product areas of their networks.²⁶⁸

Finally, business education is important, too. Many legitimate advertisers, new to the electronic market, will need information about the norms and requirements already applicable to national advertisers, such as the need for substantiation and the operation of industry review programs.²⁶⁹

"Netizen" Self-help "Netizens" — experienced online users — also are an important part of the mix and can play a leading role in assuring greater protection for other online consumers. Knowledgeable netizens can help educate novice users about the operating norms of the online environment. In turn, online users can be a valuable resource for policymakers in determining how to protect consumers online.²⁷⁰

Privacy Concerns

Cyberspace may create a new level of consumer concern about privacy:

Imagine yourself in a "virtual" bookstore,²⁷¹ browsing through the books available for sale online. When you make a purchase, you expect that certain personal information — your name, address, and credit card number — will be collected to create a record of the transaction. So far, shopping at the virtual bookstore is no different from the bookstore at the mall, right? Wrong. The owner of the virtual bookstore has access to information about you that his traditional counterpart doesn't have, unless you provide it voluntarily.

Depending on the software, the owner of the virtual bookstore can track your identity and, by following your "clickstream,"²⁷² link you to the books you considered before deciding which one to buy.²⁷³ This gives the online bookstore owner access to information about your preferences, interests and lifestyle — even if you do not buy anything.

Concerns about privacy are not new,²⁷⁴ but they are mounting.²⁷⁵ In the online setting, consumers worry about both the amount and the type of information that can be collected,²⁷⁶ and about the number of different organizations that might have access to it.²⁷⁷ In addition to those directly involved in an online commercial transaction, many intermediaries may have access to the data exchanged in the course of the transaction, including an online service, Internet service provider, telecommunications company, and electronic payment service, to name a few.²⁷⁸ Who does have access to personal data? How might they use personal information?²⁷⁹ Will they misuse the information they obtain about consumers? Will it be possible for people to obtain unauthorized access to consumers' online communications?²⁸⁰ These concerns, if not addressed, can deter consumer participation in the developing online marketplace.²⁸¹

Potential Privacy Protections

There is much debate about consumer concerns over the secondary uses of information, *i.e.*, the use of personal information beyond the transaction initiated by the consumer. Various approaches have been suggested to address these concerns. One is to give consumers notice of the planned uses of non-sensitive information and an opportunity to request that their personal data not be used in particular ways. This practice, known as an "opt out," places the burden on consumers to prevent additional disclosures of information they have provided.²⁸² For some, the "opt out" approach is sufficiently protective.²⁸³

Another approach is to give consumers the chance to "opt in." Under this system, personal information is transferred only with the explicit permission of the data subject.²⁸⁴ This approach places the burden on business to obtain the consumer's okay prior to secondary uses of personal information.

Others suggest that the principles of contract law can be used to enforce both consumers' preferences about the use of their personal information and marketers' promises about such use.²⁸⁵ Under this system, consumers and marketers define privacy-related contract terms. The information collector's notice of intended uses of consumer information constitutes an "offer," and the consumer's agreement to the terms of the notice constitutes "acceptance."²⁸⁶ A business would be liable for breach of contract if it used consumer information in a way that was inconsistent with the privacy terms to which the parties agreed.²⁸⁷ Although the contract model would reduce the need for government in this area,²⁸⁸ there is concern that this model may not protect privacy sufficiently, given the inequality of bargaining power between consumers and information-gatherers.²⁸⁹ Thus, reliance on this approach would require the strengthening of the legal enforceability of privacy promises.²⁹⁰

Still another possibility is to use online technology itself to protect consumer privacy.²⁹¹ Some suggest, for example, that use of electronic privacy policy

screens would enable consumers to choose, at the beginning of any commercial online interaction, whether and to what extent they would allow the secondary use of their personal information.²⁹² The screen would inform consumers about an online business's information and privacy policies at the initial point of contact online,²⁹³ and would empower them to make privacy decisions based on the kind of transaction, the services offered in return for relinquishing personal information, and the uses to which such information would be put.²⁹⁴ In addition, technology standards, similar to PICS, might be developed for privacy.²⁹⁵

Nurturing Consumer Trust

Some advocates support government regulation or guidelines to protect consumer privacy online.²⁹⁶ Others believe it is too early to regulate privacy protection in cyberspace. They argue that there is still much to be learned from the experiences of consumers and industry as the online marketplace develops,²⁹⁷ and that the private sector should be allowed to experiment with a variety of technological solutions.²⁹⁸ Existing industry efforts to define ethical uses of consumer information in traditional marketing contexts may be transferable to the online context, in much the same way that mechanisms for business and consumer education, and dispute resolution and redress are transferable.²⁹⁹ Further, there is concern that government regulation cannot keep pace with the technological advances in this area.³⁰⁰

Some urge the Commission to play a role in this area by supporting industry self-regulation.³⁰¹ With the Commission's encouragement, a market in privacy protections might develop, with the best schemes emerging as the standards.³⁰²

LOOKING AHEAD: CONVERGENCE**Some Predictions**

Technology is changing so fast that it is difficult to see too far ahead. Even the most dedicated “techies” are cautious about predictions, and for good reasons.³⁰³ Consider these miscalculations:

- Western Union’s reaction to the telephone in 1876: “This telephone thing has too many shortcomings to be seriously considered as a means of communication.”³⁰⁴
- Tom Watson’s conclusion in 1943 that the worldwide market could handle “maybe five computers.”³⁰⁵
- Bill Gates’ estimate in 1981 that “640K [RAM] ought to be enough for everybody.”³⁰⁶

Still, the products now entering the marketplace offer glimpses into the future. They signal an unmistakable trend toward the convergence of communications technologies. Among the latest entrants:

- *Full motion video via super fast telephone lines.* Customers can order a video by phone and play the movie the same way they now use a VCR, with the ability to pause, rewind, and fast-forward. While the movie is being transmitted through the phone lines, customers also can talk on the phone.³⁰⁷
- *Internet via cable.* New cable technology can transmit audio, video, and text on the Internet at speeds 50 times faster than over conventional telephone lines. Next year, it may be 100 times faster and eventually, 1,000 times faster.³⁰⁸
- *PC-TV.* Employees working at their desktop computers can keep an eye on CNN news or C-SPAN on a small screen in the corner of their monitors and bring it up to a full screen picture at any time.³⁰⁹

- *Cable telephony.* Cable can deliver familiar telephone services and offer consumers a competitive alternative to the local telephone company.³¹⁰
- *Digital interactive television.* “Smart”³¹¹ television, delivered via cable, can provide consumers with immediate access to videos, shops, games, and news on demand.³¹² With a few clicks of the remote control, consumers can order stamps (which the mail carrier will deliver the next day), visit different stores in the shopping mall, “try on” clothes of varying colors to see how they look on a model, and print the information in color at home.³¹³
- *Video conferencing via the Internet.* The Internet will become a new medium for phone calls and provide video conferencing at every desk.³¹⁴
- *Fax and answering machines.* Like typewriters, they will begin to appear at yard sales for \$5.³¹⁵

Convergence will involve all aspects of the new technologies — information appliances, communications networks, and repositories of stored information.³¹⁶ In the future, it is likely that the networks for telecommunications, computing, and entertainment will be merged.³¹⁷

Implications of Convergence

These combined interactive media will give consumers greater opportunities to tailor news, sports, entertainment, and data to suit their own tastes and timetables.³¹⁸ The benefits of the current information technologies — access to information, convenience, choice, consumer sovereignty — will be magnified with the new, merged technologies.

Concerns about these technologies also may be magnified. In particular, convergence may raise new levels of concern about concentrated ownership of these new media³¹⁹ and about their availability and affordability to all segments of the society.³²⁰

The general view is that we are at the cusp of a major revolution³²¹ and that the technological landscape will remain volatile for years.³²² The changes may have a

Consumer Protection in the New High-Tech, Global Marketplace

profound impact on our lives, in much the same way that other significant technological developments — phones, television, radio, and cars — have affected our society.³²³

It is important to look ahead, even if the outlines of this revolution are not entirely clear, to be aware of its potential benefits and risks. If we keep at least one eye on the future, we can be better prepared to apply the lessons we learn from today's technologies to those that come along tomorrow.

GLOBAL TRADE AND CONSUMER PROTECTION STANDARDS

TOWARD A SINGLE GLOBAL MARKETPLACE

While all the economic trends point toward a single global market,³²⁴ it is still a market that is legally fragmented by national laws and jurisdictional boundaries.³²⁵ This patchwork of laws creates an array of problems. It seriously hinders law enforcement agencies worldwide in their efforts to address the growing problem of cross-border fraud.³²⁶ It also creates obstacles for legitimate businesses engaged in global trade that must incur the costs of complying with a variety of legal standards,³²⁷ and that often face uncertainties about the legal standards that apply to their transactions.³²⁸ These obstacles — which are discussed below — are likely to grow as the world increasingly moves toward a single global marketplace.

The Global Trade Picture

International trade is growing at a phenomenal pace, as trade barriers of all sorts — tariffs, transportation costs, and regulatory restrictions — come down.³²⁹ U.S. exports and imports more than doubled between 1970 and 1994.³³⁰ Since the mid-1980s, foreign investments into the U.S. and by U.S. investors also have more than doubled, exceeding \$1.7 trillion in 1993.³³¹ Worldwide, international trade rose by over 80 percent from 1980 to 1993.³³²

These developments benefit both consumers and businesses. Consumers enjoy broader selections of products and services from around the world, and businesses enjoy access to larger markets and more opportunities to compete. As more companies engage in international trade, however, they face the challenge of having to meet legal standards that vary from country to country.³³³

Divergent National Consumer Protection Standards

While there are broad areas of international agreement on consumer protection

standards,³³⁴ there continue to be significant differences as well — many of them involving the regulation of commercial communications. Areas of differences include:

- Comparative advertising³³⁵
- Telemarketing³³⁶
- Alcohol and tobacco advertising³³⁷
- Environmental claims³³⁸
- Premiums and discounts³³⁹
- Claim substantiation³⁴⁰
- Sweepstakes³⁴¹
- Food and pharmaceutical marketing³⁴²
- Energy labeling³⁴³
- Privacy protection for consumer data³⁴⁴

Businesses that market in countries with different legal standards must adjust their promotional material and tailor their sales practices to suit each country.³⁴⁵ The trade statistics suggest that for many companies, it is worth the trouble and expense. But other companies are discouraged by the costs and legal uncertainties.³⁴⁶

There are efforts on many fronts to reduce trade barriers and open markets to enhance the free flow of goods and services. Most important are the international trade agreements that establish frameworks for greater world trade.³⁴⁷ In addition, governments and international organizations are taking steps to harmonize regulatory standards around the world³⁴⁸ — a long term goal of the trade agreements.³⁴⁹ Global business groups also are engaged in “private sector harmonization” efforts.³⁵⁰

ROLE FOR THE FTC

The FTC can play a role on two fronts. First, it can be sure that its own regulations do not impose unnecessary burdens on companies that are in — or that want to get into — the global marketplace. Second, it can participate in international dialogues concerning more harmonious consumer protection standards worldwide.³⁵¹

Regulatory Review

Across the board, the FTC needs to review its regulations to assure that they are well suited to the new global marketplace, and adapt them where circumstances warrant.³⁵² Its initiative to revamp the Care Labeling Rule is an important first step in that direction.³⁵³ The FTC has proposed amending this rule to allow the use of care labeling symbols that would conform with symbols permitted by Canada and Mexico.³⁵⁴ The result would be a simplified label that would reduce manufacturers' costs and eliminate the need for country-specific inventory — an increasingly significant benefit as trade in apparel and textiles soars among the NAFTA countries.³⁵⁵

The proposed rule is designed to achieve two goals: a high level of consumer protection by conveying all necessary information to consumers, and the removal of undue burdens on businesses that can impede trade.³⁵⁶ The goals are consistent. High U.S. consumer protection standards help maintain high standards for American products and enhance their competitive position in the world marketplace.³⁵⁷

Other FTC labeling regulations that may be appropriate for harmonization include: appliance energy labeling,³⁵⁸ certification of origin requirements, textile and fiber labeling,³⁵⁹ and “eco-labeling.”³⁶⁰

Leadership Role in International Forums

The FTC has been encouraged to play a bigger role in the international debates

of both governments and private organizations about more uniform international consumer protection standards.³⁶¹ Given its small size and limited resources, however, the FTC may be somewhat constrained in its ability to participate in such efforts.³⁶²

Still, the FTC can participate by setting an example — as it is doing through its efforts to harmonize the Care Labeling Rule.³⁶³ It also can participate more fully in international discussions of consumer protection standards.³⁶⁴ Business and consumer groups have encouraged the Commission to be more pro-active on the international scene in promoting both its consumer protection standards and its market-based approach to regulation.³⁶⁵ In the future, as U.S. consumers and businesses rapidly expand their participation in the global marketplace, it will become even more important for the Commission to devote attention to consumer protection issues worldwide.

CONCLUSION

The new information technologies may change the marketplace in historic and revolutionary ways. By giving consumers access to more information, choice, control, and convenience, they can put consumers in the driver's seat and usher in a new era of consumer sovereignty.

At the same time, the new technologies raise consumer protection concerns about increased fraud and deception, greater invasion of privacy, and risks of anti-competitive behaviors. The challenge now is to address these concerns in ways that preserve the benefits of the new technologies.

There are reasons to be optimistic about finding solutions. First, some of these problems are just emerging and early actions may keep them manageable. Second, there is considerable expertise — in both the public and private sectors — on which to draw for solutions. Third, there are unique opportunities to use the new technologies to provide consumer protection, education, and self-help opportunities.

GETTING AHEAD OF PROBLEMS

Some problems, like fraud on the Internet, are still relatively small when compared, for example, with telemarketing fraud. Cross-border fraud — although especially vexatious — is still a relatively new phenomenon. Privacy concerns, too, may be addressed before they reach major proportions.

Given the rapid pace of change, the window of opportunity to prepare for these emerging challenges may be narrow. Government, consumer, and business leaders need to move quickly. If they do, there is some chance to get ahead of the problems.

Fortunately, both the public and private sectors are in a good position to anticipate the difficulties and to find solutions.

APPLYING LESSONS LEARNED

Although the new technologies raise some new consumer protection challenges, many of the issues are similar to those posed by more traditional marketing tools. Thus, the recent experiences of government, businesses, and consumer groups in dealing with telemarketing fraud, 900-number scams, and deceptive TV advertising are relevant to the emerging issues.

Those experiences show that the crucial elements of an effective and balanced consumer protection program are:

- coordinated law enforcement by state and federal agencies against fraud and deception;
- industry self-regulation and private initiatives to protect consumers; and
- consumer education through the combined efforts of government, business, and consumer groups.

The hearing record is replete with examples of private initiatives: industry self-regulation programs and plans to develop and expand such programs, technology-based consumer protections and self-help opportunities, and commitments to undertake new consumer education programs. These and other initiatives will be crucial in providing consumer protection in the new marketplace.

The Federal Trade Commission will continue to place a high priority on coordinating and participating in joint law enforcement efforts at home and abroad. It also will continue to actively support industry self-regulation and to work with a wide array of organizations in concerted education efforts.

FTC FOLLOW-UP

Next year, the Commission staff will issue a follow-up report on the steps taken to address many of the issues raised at the hearings. The hearings already have spurred a number of innovative consumer protection initiatives by both the private and public sectors, and there is every reason to be optimistic about progress on all fronts in the coming year.

ENDNOTES

1. Gallant 2724; Moore 2342; D. Goldstein 2391. Endnote citations are to the printed record on file at the Federal Trade Commission. The record is also available online at <http://www.ftc.gov>. A full list of the speakers referenced in the notes can be found in Appendix A.
2. White 2296; Jones 2845. While the costs of gathering and transmitting information are declining dramatically, the human costs of processing it may actually increase. Gertner 2870. Information overload may be partially addressed as sellers reduce their broad-based advertising and target their messages more narrowly to individuals who are interested in their product information. Huyard 2504-05; Nisenholtz 2757-58. This more targeted marketing, however, is possible in part because sellers can draw on vast data bases which, in turn, raise privacy concerns.
3. Barker 2705.
4. Michelotti 2789; Weitzner 2842; Burrington 2854.
5. Moore 2333-34.
6. Huyard 2512; Young 2252.
7. Nisenholtz 2754-55; Andreotta 2493-96; Humphrey 2794-95.
8. Cutler 2373-74.
9. Nisenholtz 2757.
10. Bell 2239-43; Zalewski 2849-50.
11. Levin 3038, 3064; Sackler 2727.
12. Gallant 2702-04.
13. Nisenholtz 2759; Bell 2239-43.
14. Doyle 2518. Also contributing to the growth in fraud are societal changes that may create opportunities for fraudulent practices, *e.g.*, increased economic pressures and lack of personal income growth that make consumers susceptible to get-rich-quick schemes and other frauds. Barker 2626-27; Zubrod 3092.
15. Doyle 2518-19.

Consumer Protection in the New High-Tech, Global Marketplace

16. Harris 3107; Zubrod 3091.
17. Barker 2633, 2636-37; E. Brown 2711.
18. Sloan 2574-85; Doyle 2518; Humphrey 2794-95.
19. Burrington 2553-54.
20. Cole 2803; Doyle 2523-24 (scam artists have been quick to adopt the new technologies, such as computer lists of people to target and computerized dialing systems).
21. Humphrey 2796-97; D. Goldstein 2391; Gertner 2771-73.
22. Barker 2628; Humphrey 2795; Doyle 2524-25.
23. Silbergeld 2366-67.
24. Cole 2804-05; D. Goldstein 2389.
25. Michelotti 2779-80; Goldman 2944; Hendricks 3008-09; Humphrey 2797; Post 2822.
26. Moore 2337-38; Cutler 2377; D. Goldstein 2387-88; Post 2850; Michelotti 2874.
27. An important question is whether this is a new type of market, or an extension of the traditional marketplace. Weitzner 2842 (new market); Nisenholtz 2846-47 (extension of existing market).
28. Center for Media Education, Comment (submitted for the record) 1-3.
29. Michelotti 2779.
30. Moore 2343; Silbergeld 2366-67; D. Goldstein 2388-89; Harris 3134. It is not just the emerging problems growing out of the new technologies that need attention; traditional scams continue and need to be addressed. Jones 2845.
31. Doyle 2529-30.
32. Goldman 3023-24.
33. Goldman 2929, 3023-24; Hendricks 2976-77; Kang 3010-11; Blanke 3014-15; Belair 2991.
34. Kang 2896-97; Plessner 3018.

35. Moore 2338-39. If advertising becomes an important source of funding for the Internet, it can make access to the Net more affordable to consumers. Michelotti 2789. Gallant 2724 (98% of households have telephones, 96% have televisions and 90% have VCRs); Gross 2742 (predicting that Internet will be firmly part of "everyday life" and that people will have computers like they have phones today).
36. Gross 2737-38; Burrington 2853-55; Weitzner 2881-82; White 2297-98.
37. Barker 2705. Consumers are concerned about whether they will be able to afford the new technologies, and whether they will select the right technologies, *i.e.*, those that will be successful in the marketplace. White 2295-98.
38. U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA), *Falling Through the Net: A Survey of the "Have Nots" in Rural and Urban America* (July, 1995) (submitted for the record) [hereinafter NTIA Study]. The study found telephone ownership is lowest among Native Americans in rural areas, followed by rural Hispanics and rural Blacks. Personal computer ownership is lowest for Black households in central cities and rural areas. The study found that "the less that one is educated, the lower the level of telephone, computer, and computer-household modem penetration." NTIA Study at 3.
39. Kimmelman 2312-13; Young 2261; Nisenholtz 2753.
40. Gertner 2763-67 (other factors, such as ease of entry into the market, may reduce the risk of non-competitive pricing).
41. Post 2851-52. Search engines enable consumers to find Internet sites. If they operate to push some sites to the head of the list of sites or to crowd competitors' addresses off the list, they could impede entry. *Id.* Also see Cole 2859-60 (whether information is provided fairly or unfairly on the Internet may be a major issue for consumers).
42. Levin 3037, 3056, 3078.
43. Berman 2839-40; Sherman 2841; Gertner 2767-69.
44. Young 2257; Moore 2344-45; Sherman 2864; Burrington 2555-56; Comments of J. Patrick Herold and John K. Lopker, Federal Transtel, Inc. (submitted for the record); Sackler 2645-46, 2650-51; Gertner 2770-74; Michelotti 2784; Humphrey 2799.
45. Burrington 2555-56; Doyle 2533-34; Michelotti 2873.
46. Doyle 2532-34; Humphrey 2800; Sackler 2640-41.
47. D. Goldstein 2392-93; Herold & Lopker *supra* note 44; Barker 2705.

48. Cutler 2422.
49. Burson 2319; Berman 2885-86; Barker 2633-34; Rotfeld 2408.
50. Sackler 2692-93.
51. Gertner 2771-73.
52. Gitlitz 2919; Belair 2955; Goldman 2929-31; Wellbery 2974; Strenio 2971.
53. Braasch 2684; Sackler 2641; Michelotti 2782; Andreotta 2496-99; Kang 3010-11; Young 2316; Alter 2395-96; Goldman 2927; Wellbery 2973.
54. Burrington 2545-56.
55. Cole 2806.
56. Gitlitz 2917; D. Goldstein 2392-93; Silbergeld 2419-21.
57. Silbergeld 2366; D. Goldstein 2385.
58. Rotfeld 2415-16; Moore 2344.
59. Sherman 2865; Burson 2270; Cutler 2379-81; Steel 2571-72; E. Brown 2696; Braasch 2690-91, 2698; Gregg 2698-99; Gitlitz 2910-11; Sloan 2574-85; Dowd 2699.
60. Cole 2858-59; Post 2877-78; Burson 2270.
61. Cole 2809-12 (demonstrating Better Business Bureau Web site program).
62. Gregg 2698-99; Dowd 2697.
63. Sloan 2574-85 (reporting on the recent study of telemarketing fraud by the American Association of Retired Persons that revealed that fraudulent marketers not only succeed with vulnerable groups, but with people who are affluent and well-educated).
64. Burrington 2830-32.
65. Huyard 2512.
66. Andreotta 2489-90.
67. Doyle 2519-2520; King 2602; Andreotta 2483.

68. According to one estimate, \$750 billion in U.S. commerce is based on the telephone. Huyard 2516.
69. These advances include 800-number and 900-number "pay-per-call" services, "intelligent call processing" that efficiently routes incoming calls, and "interactive voice processing" that allows consumers to communicate by entering numbers on a touch tone telephone. Andreotta 2484-2488. For telemarketers, automatic dialers can weed out busy signals and answering machines. When a consumer does answer, the call rolls over to a sales representative. Huyard 2503-2505.
70. Information is transmitted over ordinary telephone lines 2½ to 5 times faster using the new ISDN (Integrated System Digital Network) technology as compared with a standard computer modem. The experimental ADSL telephone system transmits information even more quickly. Young 2251-52.
71. Young 2252; Andreotta 2491.
72. The smart card is a small, credit-card sized device that functions both as an identification card and an electronic wallet. It is used in conjunction with TV- or phone-like appliances referred to as "readers." Andreotta 2494-95; Braasch 2683-84.
73. Mills 2589.
74. Over 11 million Americans are employed in some fashion in the direct marketing industry of which telemarketing is a major component. In 1994, \$600 billion in goods and services were sold through the direct marketing medium; by the year 2000 that figure is expected to grow by 30%. Gallant 2655.
75. Huyard 2501.
76. Huyard 2513-14.
77. Gallant 2655-57.
78. German law, for example, prohibits a company from telemarketing unless the marketer obtains prior written permission from the consumer. Gallant 2659-60.
79. William W. Burrington and Thaddeus J. Burns, Hung Up on the Pay-Per-Call Industry? Current Federal Legislative and Regulatory Developments, 17 *Seton Hall Legislative Journal* 359, 366 (1993) (submitted for the record). A company that develops and sells pay-per-call programming is an Information Provider (IP). An intermediary "Service Bureau" may assist the IP in developing its programming and arranging with the carrier for the IP's 900-number lines. The IP is paid for its services through an agreement with the carrier. *Id.* at 361.

80. Pay-per-call services include product information and support lines, stock market quotes, weather information, marketing, merchandising, consumer research, and customer services. *Id.* at 366-67.
81. *Id.* at 359-60.
82. Such scams rely on old tools such as sucker lists, ads, post cards, telephone pitches, and glib telemarketing. Zubrod 3092.
83. Barker 2626-27; Zubrod 3092.
84. Barker 2627; Doyle 2527.
85. Sloan 2574-85.
86. Sloan 2574-85; Barker 2629; Doyle 2523-24.
87. Zubrod 3092.
88. Harris 3107. Electronic transaction and voiceless communications systems, data processing and tracking systems, and computer-based commercial opportunities all provide means for new methods of consumer fraud. Barker 2625.
89. People on "sucker lists" may receive "as many as 10 to 20 calls a day soliciting them to buy things, to go on cruises, telling them they've won prizes and so on." Doyle 2523-24.
90. Larabie-LeSieur 3118. To a much lesser extent, there have been complaints about fraudulent operations in other countries such as Mexico and Bermuda. Barker 2637.
91. "In one celebrated example, a television Santa Claus urged children viewing the program to hold the telephone receiver up to the television, which emitted the dial tones necessary to automatically connect the child to a pay-per-call service." Burrington & Burns, *supra* note 79, at 370-72.
92. Harris 3108; Barker 2633, 2636; E. Brown 2711.
93. Harris 3107. Some countries solicit U.S.-based chat lines and pay-per-call schemes to supplement their postal and telephone earnings. Barker 2633, 2637.
94. Harris 3107. Consumers do not recognize the 809 area code as an international call because it does not begin with 011. Often there is a recording to keep people on the line. E. Brown 2712.
95. Harris 3110.

96. Harris 3109. The phone traffic to Sao Tome, for example, jumped from 40,000 minutes in 1992, to 13.2 million minutes in 1994; the traffic to Moldova jumped from 81,000 minutes in 1993 to 6 million in 1994. In part, the growth stems from efforts to circumvent U.S. law enforcement. *Id.*
97. Harris 3108.
98. Zubrod 3091.
99. Barker 2628-30.
100. Barker 2628.
101. Zubrod 3091.
102. Doyle 2524-25. Retrieving consumers' cash is much harder than preventing them from handing it over to fraudulent telemarketers in the first place. *Id.*
103. Barker 2633; Harris 3133.
104. Larabie-LeSieur 3118. Law enforcement agencies, operating with substantially reduced budgets, also face restrictions on cooperation and information sharing. *Id.*
105. Braasch 2684; Sackler 2641; Gallant 2659; L. Goldstein 2597-98; Steel 2562, 2604; Held 3097; Gregg 2673.
106. Burrington 2555-56; Sackler 2645-46, 2650-51; Braasch 2687; L. Goldstein 2600.
107. Doyle 2532-35; Burrington 2555-56; Mills 2595; L. Goldstein 2597-600.
108. Burrington 2555-56; Herold & Lopker, *supra* note 44, at 1-2; L. Goldstein 2597-98; Held 3148.
109. Sackler 2640.
110. Gallant 2662.
111. Sackler 2646, 2651; Braasch 2688. The Telemarketing Sales Rule, developed through broad consultation with the public and private sectors, provides consumer protection without overburdening legitimate telemarketers. Doyle 2532; Sackler 2643; L. Goldstein 2597-98; Mills 2595.
112. There is a need for more enforcement of consumer protection laws. Harris 3133-34; Herold & Lopker, *supra* note 44, at 1-2; Barker 2634.

113. Held 3148; Zubrod 3093; Harris 3113. One of the greatest challenges for law enforcement agencies is the task of coping with the increased volume of fraud and new scams at a time of diminished resources. Doyle 2529-30; Harris 3133.

114. Some of the most important collaborative efforts have been at an individual level, where investigators in various agencies or offices work together to solve problems. Zubrod 3138-39.

115. This includes the cross-designation of FTC and other agency attorneys in criminal investigations. While there is some institutional resistance to such overlap and the sharing of grand jury information, the resistance is gradually dissipating and, in the future, more FTC attorneys will be working as Special Assistant United States Attorneys in fraud prosecutions. Zubrod 3095.

116. Zubrod 3136; Larabie-LeSieur 3139. Although prosecutors are pursuing these crimes more aggressively, judges still are likely to give only probationary sentences to white collar criminals engaged in global telemarketing fraud. Zubrod 3136-37.

117. Zubrod 3093-94. A first step might be a network among agencies for obtaining public information in foreign jurisdictions. Larabie-LeSieur 3127-28. An international group of law enforcement agencies — the “International Marketing Supervision Network” — has been established to communicate about their respective countries and cross-border enforcement. Starek 3117. The establishment of “mutual legal assistance provisions” also may be useful and necessary to assist agencies in enforcement. Larabie-LeSieur 3128; Starek 3129. It will be necessary to overcome some institutional reluctance to share information, however, as well as some legal barriers that prevent exchanging confidential law enforcement information. Zubrod 3142; Larabie-LeSieur 3126.

118. Larabie-LeSieur 3124.

119. “[M]utual trust and sharing of a common vision are key elements to our success.” Larabie-LeSieur 3128. Working together and staying relevant to emerging problems, however, will “require an awful lot of work.” Held 3130.

120. Braasch 2684; Sackler 2640-41; Gallant 2659; L. Goldstein 2597-98.

121. Braasch 2684; Steel 2562; Held 3097.

122. Held 3131-32.

123. Steel 2603; Gregg 2673; L. Goldstein 2598-99. Consumers do not really know who is on the other end of the telephone line, and legitimate telemarketers must take responsibility for distinguishing themselves from fraudulent telemarketers. E. Brown 2676-77; Dowd 2697.

124. Burrington 2545-56; L. Goldstein 2598.
125. Sackler 2642-44.
126. Sackler 2644.
127. Braasch 2685.
128. Steel 2561-62; 2566-68.
129. Harris 3114-15. The Federal Communications Commission worked with industry to develop this voluntary agreement to protect consumers. The FCC also is working with foreign telephone companies and regulators to stop the fraud at the other end of the line. A few overseas carriers have agreed to provide the same consumer protections as their domestic counterparts. Harris 3115.
130. Gallant 2662-63. This certification may provide the means for legitimate companies to distinguish themselves from fraudulent ones. E. Brown 2677.
131. Gallant 2663.
132. Gregg 2670-72. Shipping companies could stop the use of CODs; mailbox companies could prevent use of the word "suite," which signals to consumers that they are dealing with a legitimate company at a real location, not just a mailbox address. Gregg 2673.
133. Sackler 2692. This would enable legitimate telemarketers to identify themselves to consumers and separate themselves from fraudulent telemarketers.
134. Sackler 2692-93. This device would be similar to the computer filtration devices that enable parents to screen out certain content for their children. Sackler 2693. However, given the clever "pitches" of con artists, it might be difficult to characterize a fraudulent telemarketing call so that a computer could recognize it. Further, scams change so rapidly that it would be hard to keep the device up-to-date. E. Brown 2693-94; Dowd 2696.
135. Gallant 2702-04, 2707 (the name of the business that calls will appear in the caller ID box).
136. Barker 2629; Dowd 2697, 2699; Gallant 2697; Sackler 2638-39; Braasch 2698; Gregg 2721-22; E. Brown 2695-96; King 2602.
137. Sloan 2583-85.
138. Sloan 2583-85; E. Brown 2695-96.

Consumer Protection in the New High-Tech, Global Marketplace

139. Gregg 2698-99, 2721-22; Barker 2629; Dowd 2699; Gallant 2697; E. Brown 2695-96; King 2602; Braasch 2690-91.

140. L. Goldstein 2599.

141. Steel 2572. Bankcard companies, for example, devote considerable resources to educating consumers about bankcard fraud.

142. Moore 2334-35.

143. Moore 2336-37. The remaining television advertising dollars are divided among national and local spot programming.

144. *Id.*

145. Moore 2337.

146. Silbergeld 2348. The three new infomercial networks are: the Direct Response Advertising Group Network, the Product Information Network, and the Access Television Network. *Id.*

147. Silbergeld 2355.

148. Moore 2343; Silbergeld 2353; D. Goldstein 2388.

149. D. Goldstein 2388-89.

150. D. Goldstein 2384-85; Rotfeld 2413-14; Cutler 2442-43. Various explanations were offered for the limitations and variations seen in television self-regulation, *e.g.*, a lack of enforcement mechanisms inherent in self-regulation, the fact that emerging television groups face greater economic pressure to fill the hours in a week than do well-established broadcast networks and thus may clear advertising that would not be cleared by the broadcast networks, and the possibility that self-regulation might only take place in response to government activism. Cutler 2442-43; Rotfeld 2408, 2444-45.

151. Rotfeld 2414.

152. Rotfeld 2415.

153. D. Goldstein 2384-85.

154. Silbergeld 2346; D. Goldstein 2391.

155. D. Goldstein 2388.

156. D. Goldstein 2384-85; Rotfeld 2414-15. For a discussion of the factors that impact the screening procedures in the cable industry, see Alter 2395-97.
157. D. Goldstein 2384-85.
158. D. Goldstein 2389.
159. *Id.*
160. Cutler 2379-81; D. Goldstein 2392.
161. Rotfeld 2407; D. Goldstein 2418.
162. Rotfeld 2408.
163. D. Goldstein 2392.
164. Silbergeld 2419-20.
165. Cutler 2376.
166. *Id.*
167. Gross 2737-38; Burrington 2853; Humphrey 2791.
168. Gross 2739-40.
169. Zalewski 2881; Weitzner 2881.
170. Gross 2740. Web technology enabled information to be presented in a highly graphical or pictorial manner, using illustrations and even photos. Screen displays created with the Web technology are called Web pages, or "sites," and are viewed by using a Web "browser." Web pages also contain cross-links to other sites or addresses on the Internet, such that by merely clicking on the cross-link, users can skip to the cross-linked site and access whatever information is available there. Alternatively, users can bounce between unrelated, unlinked sites by entering the Internet addresses of those sites in the Web browser.
171. Gross 2737-40; Post 2822.
172. Gross 2740-41.
173. Cole 2803-04.

174. Bell 2239-44; Nisenholtz 2757-59; Michelotti 2775-76; J. Walker Smith, *Civilizing Cyberspace* at 2 (submitted for the record) [hereinafter *Civilizing Cyberspace*]. This empowerment of the consumer also has ramifications for non-advertising communications. In a recent survey of online users, 75% of the users considered online services to be a better information source than traditional media because the information and news available online is “unedited” by a third-party provider. *Id.*

175. Consumer control over the information they choose to view will also provide some indication of whether consumers, in fact, find advertisements useful, as the economists have been asserting for years. Post 2850-51.

176. *Civilizing Cyberspace*, *supra* note 174, at 2; Michelotti 2776 (cyberspace advertising must be invitational rather than intrusive).

177. Cole 2803.

178. Bell 2323; Nisenholtz 2758; Professor Henry Perritt, Villanova University School of Law, Letter of November 7, 1995, at 5 (submitted for the record) (suggesting regulations to prohibit unsolicited commercial e-mail, similar to the FCC regulation prohibiting unsolicited commercial fax messages).

179. Michelotti 2775, 2777-78, 2789, 2849.

180. Humphrey 2796-97.

181. Michelotti 2777-78; Humphrey 2794.

182. Humphrey 2794; Cole 2803-04 (warning that the low cost of producing a “quality-appearing” Web site will make unresearched consumer choices more risky). See also Gertner 2767 (suggesting that new entrants can find customers without buying expensive customer lists or incurring the costs of telemarketing or direct mailings).

183. Berman 2839-40; Sherman 2841.

184. Nisenholtz 2847; Post 2851.

185. Berman 2838-39; Nisenholtz 2847. While consumer interest in viewing online ads may be low today, this ability to cross-advertise Internet addresses may become more valuable if the “Yahoo” entertainment model of the Internet develops. Nisenholtz 2860-61. See discussion in text accompanying notes 192-94 about the possible future domination of cyberspace by mega-advertisers or mega-entertainment providers.

186. Nisenholtz 2757.

187. Nisenholtz 2757-58; Michelotti 2775-76.
188. Nisenholtz 2847.
189. Michelotti 2775.
190. Nisenholtz 2749-50; Michelotti 2848. The situation today is like the days of television before the Milton Berle show, when advertising agencies were strenuously debating the level of resources that should be shifted to the "new" TV medium from the tried and true print advertising. Michelotti 2872.
191. Burrington 2853.
192. Nisenholtz 2750-52 (describing the elements of scenario one). Yahoo is an online guide to sites available on the Internet, whose young founder recently stated that the Yahoo guide exists because "people don't want to have to waste time wasting time." *Id.*
193. Nisenholtz 2752-54 (describing scenario two).
194. The few media super-sites would be surrounded by smaller, associated-content sites, each with an audience subset. Nisenholtz 2753.
195. Nisenholtz 2754-55 (describing scenario three).
196. Michelotti 2779-80; Post 2822.
197. Michelotti 2783-84. Intellectual property creates an indicia of authority and becomes the advertiser's "signature" on an ad. *Id.*
198. See Chapter 6, Volume I, of this report.
199. Even users, *i.e.*, consumers, of the interactive media might be viewed as publishers of information. Michelotti 2785.
200. Cyberspace provides the opportunity to "lift" or wholly create copyright- or trademark-infringing messages with great ease; such messages can dangerously appear to be "official," as if they were coming from the original advertiser. Michelotti 2786.
201. Michelotti 2784-86. Responsibility for Web site links to other sites is another unanswered issue. *Id.* At a minimum, Web pages should clearly disclose the identity of any sponsoring advertisers. *Id.*
202. Civilizing Cyberspace, *supra* note 174, at 1.

Consumer Protection in the New High-Tech, Global Marketplace

203. Humphrey 2795. Such system will either use new technology or implement currently available public key encryption to enable payment by digital cash or real-time credit card authorizations. Perritt, *supra* note 178, at 4-5.
204. Perritt, *supra* note 178, at 4-5; Gross 2742; Humphrey 2795.
205. Pollin 2289.
206. Michelotti 2780-81; Cole 2806; Burrington 2828; Gertner 2868-69; Weitzner 2878-80.
207. Civilizing Cyberspace, *supra* note 174, at 3. Online usage doubled throughout 1994, during a period of enthusiastic publicity about cyberspace, but then slowed, following publicity about problems that can arise online. *Id.*
208. *Id.*
209. Cole 2806; Weitzner 2880.
210. Michelotti 2780-81.
211. Bell 2242. However, due to the greater availability of information in online markets, new entrants can gain credibility, or lose it, very quickly. Cole 2844.
212. Weitzner 2881-82. (The market for Internet access might not be providing affordable service without this underpinning of a regulated phone service.)
213. Bell 2237-38; Michelotti 2789.
214. Nisenholtz 2860-61.
215. NTIA Study, *supra* note 38. The core of U.S. telecommunications policy has been "universal service," *i.e.*, affordable access to telephone service for all Americans. In today's world, "universal service" may include not only basic phone service, but also access to or ownership of computers and modems to participate in the new information age. *Id.* at 1. See also Jones 2846 (expressing concern that a different quality of information may be provided to network versus non-network consumers).
216. Burson 2266-67; Humphrey 2792; Burrington 2855.
217. Burson 2267-68.
218. Gertner 2771; Nisenholtz 2758; Cole 2804-05 (back-of-the-book marketers can operate online with minimum investment). The Internet's ability to support small, global transactions

may also increase the incidence of fraud, because victims are unlikely to pursue costly international legal remedies in such circumstances. Perritt, *supra* note 178, at 1-2.

219. Post 2824; Burrington 2833.

220. Humphrey 2792-93, 2795.

221. Humphrey 2795.

222. Perritt, *supra* note 178, at 5 (suggesting regulatory action to require a cooling-off period during which consumers would be able to rescind certain online transactions).

223. Humphrey 2793. Anonymity is a two-edged sword. While it is one of the most serious obstacles faced by law enforcers attempting to prosecute online fraud, it also enables consumers to preserve their privacy while "surfing the Net." *Id.*

224. Burson 2267. With a portable computer, anyone can be hooked up wherever there is a phone jack, and very soon they won't need a phone jack. Humphrey 2793.

225. Michelotti 2874.

226. Humphrey 2795-96.

227. Humphrey 2797-98.

228. Humphrey 2798-99.

229. Michelotti 2782-83.

230. Cole 2858-59.

231. Nisenholtz 2860.

232. Center for Media Education, *supra* note 28, at 1-3.

233. *Id.* at 4-5.

234. Michelotti 2875-76.

235. Burrington 2835; Humphrey 2799; Cole 2806. A recent survey showed that online users believe that government regulation ultimately will be needed, but that regulation, as well as self-policing efforts, will fail. If so, there could be a crisis in consumer confidence that chokes off growth of the online market. Civilizing Cyberspace, *supra* note 174, at 3.

236. Burson 2271-74; Cole 2858-59; Jones 2863-64; Post 2877-78.
237. Michelotti 2872; Perritt, *supra* note 178, at 3 (urging government agencies to monitor and gain experience with problems online); Gertner 2770 (arguing that regulation can create new entry barriers). See also Michelotti 2784, Burrington 2885, Berman 2884 (all expressing concern that online censorship legislation might establish a framework for addressing other issues and therefore limit the Internet's potential).
238. Nisenholtz 2749. "Attempts to set inflexible policies around something ephemeral at best would be a waste of effort and at worst, could stifle the evolution of the thing that, from a marketing perspective, is not yet real." *Id.*
239. Burson 2268-70; Cole 2805 (the necessary monitoring levels will be much higher than with traditional media outlets); Nisenholtz 2861 (the pace of Internet innovation will necessitate constant vigilance).
240. Cole 2805-06; Post 2822; Perritt, *supra* note 178, at 3.
241. Perritt, *supra* note 178, at 5-6. Governments should also be meeting to resolve the conflict of law issues posed by online advertising. Michelotti 2780.
242. Perritt, *supra* note 178, at 1-4. If international, this institution could be established under the auspices of the UN. *Id.*
243. Center for Media Education, *supra* note 28, at 7. One approach would be to ban such activities as tracking children's online activities, linking children's Web sites to advertiser sites, providing interaction with product "spokescharacters," and aiming direct marketing to children. In addition, there could be requirements for demarcation between advertising and programming content, restriction of online purchases to those over 18, and computer coding of advertising sites to permit automatic screening out of such sites by parents. *Id.*
244. Michelotti 2872, 2874. The Children's Advertising Review Unit (CARU), a division of the Council of BBB, is now at work on children's advertising issues. Cole 2805. Market solutions, such as software filters, already are available for parents to block their children's access to alcohol or tobacco advertising. Michelotti 2784, 2871.
245. Michelotti 2874 (limiting online children's advertising to certain hours of the day, as it is with television advertising, may not be effective online).
246. *Id.*
247. Humphrey 2799-2800; Burrington 2835-36; Civilizing Cyberspace, *supra* note 174, at 3.

248. Burson 2319; Berman 2885-86; Michelotti 2787 (urging government and industry to move forward in addressing issues of consumer privacy and advertising liability).

249. Burson 2269-70, 2273; 2319-20; Michelotti 2780-81; Cole 2806; Burrington 2832-36; Weitzner 2879-80. Regulators should allow the private market to test its ability to fulfill consumers' needs for information and protection. Gertner 2868-69, 2773-74.

250. Cole 2805, 2811-12. Such a program might include "e-mediation" and arbitration, *i.e.*, resolution of consumer complaints via e-mail or other online communications, regarding goods or services offered online. Other possible requirements for company participation are keeping on file with the BBB basic business information, such as the company's physical address, and maintaining a satisfactory complaint-handling record for both online and off-line business. Various industry groups, such as the Advertising Standards Alliance organizations in the UK and Europe and the International Chamber of Commerce in Paris, have also begun to address self-regulation from an international perspective. Michelotti 2781.

251. Gertner 2771-72. Online stores or shopping malls may also serve a certification function, just as department stores do now. *Id.*

252. Perritt, *supra* note 178, at 6. Areas suitable for private arbitration include intellectual property, personal privacy, consumer protection, and possibly defamation, intentional infliction of emotional distress, or intentional interference with contract. *Id.*

253. *Id.* at 6-7. Most developed countries are signatories to the New York Convention treaty on enforcement of international arbitration awards. *Id.*

254. *Id.* at 7.

255. Post 2823-24. The system was initially developed for copyright infringement claims, but could also be extended to complaints involving defamation or marketing fraud. Post 2826.

256. Post 2824-25. Such mechanisms may lead to development of a "cyberspace common law" to help address the emerging legal issues inherent in the evolving technology and multi-jurisdictional nature of cyberspace. Because the decisions of the Virtual Magistrate system will be publicly available, the online users themselves can participate in the development of this "common law." Post 2825-27.

257. Michelotti 2784, 2871; Pollin 2326-29. It may also be possible, in effect, to compartmentalize the Internet as to content type, or into regulated and unregulated areas, thus allowing consumers to judge for themselves which areas to visit. Pollin 2326.

258. Weitzner 2814-16, 2820. Such tools balance the responsibility of content providers with that of individuals accessing the information while still allowing the broadest possible diversity

of information online. *Id.* Michelotti 2784.

259. Weitzner 2814-17. PICS is a joint effort of industry and non-profit entities to formulate the underlying technical standards for the system.

260. Weitzner 2816-19. The third-party ratings systems would reside on PICS-compliant Internet servers and be offered as a service available for use on the Internet and with Web browsers, including those used by the commercial online services. Because the ratings lists would not be permanently attached to the underlying content being rated, any given Internet site might be included in numerous ratings systems. *Id.*

261. Burrington 2835. In addition, in the United States, legal avenues exist, such as Section 43(a) of the Lanham Act, by which competitors can, in effect, police each other. Sherman 2865. Marketing organizations could also police consumer fraud through actions similar to those used by ASCAP and BMI to fight copyright infringement. Perritt, *supra* note 178, at 3.

262. Humphrey 2800. As part of this effort, the major commercial online services have provided the FTC and state Attorneys General with resource manuals incorporating their terms of service and other policies. Burrington 2833-34.

263. Burrington 2834.

264. Cole 2806.

265. Perritt, *supra* note 178, at 8. The FTC could certify private dispute resolution institutions to handle the actual case load, working in a general way from the Magnuson-Moss dispute resolution requirements (16 C.F.R. Part 703). Perritt, *supra* note 178, at 3.

266. Burrington 2831-32; Cole 2804-06; Burson 2269-70; Sherman 2865; Humphrey 2800. This education must start with the basics, such as don't provide credit card information in response to an e-mail solicitation or disclose your password for a commercial online service, and continue through explaining the rules, or lack thereof, extant in cyberspace. Burrington 2830.

267. Burrington 2830; Cole 2806-07.

268. Cole 2807-08. Government and consumer education organizations could develop more extensive online cross-links to each others' Web sites as well. *Id.*

269. Cole 2804-06. Given this influx of new marketers, regulators and self-regulators may have to deal with a higher percentage of non-complying advertisers than in the past. *Id.*

270. Burrington 2832; Burson 2273-74 (suggesting that regulators should create an on-going dialogue with "netizens").

271. Kang 3010.
272. The clickstream is the sequence of electronic markers left by online users as they browse through various sites on the Internet.
273. Kang 3010.
274. Kang 2946.
275. Burson 2266-67; Belair 2955; Andreotta 2496.
276. Wellbery 2973; Goldman 3023; White 2320-21; Hendricks 2976.
277. Gitlitz 2941.
278. Kang 2896-97; Plesser 3018.
279. Gitlitz 2941.
280. Goldman 2927.
281. Gitlitz 2941; Goldman 2927-28; Wellbery 2973; Kang 3010-11.
282. Goldman 2928.
283. Gitlitz 2912; Plesser 2987-88.
284. An "opt in" system might apply to the use of sensitive information, such as medical or financial data. Kang 3012; Plesser 2987; Wellbery 2972-73; U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA) Privacy and the NII: Safeguarding Telecommunications-Related Personal Information (1995) at 8-9 (submitted for the record). Or "opt in" could apply to any secondary use of non-sensitive personal information. Baker 3016. Yet another approach is to refrain from the use of medical information for marketing purposes. Plesser 2987.
285. Kang 2897-2900.
286. Kang 2899.
287. Kang 2939-40, 2980.
288. Kang 2978-80.
289. Goldman 2984-85.

Consumer Protection in the New High-Tech, Global Marketplace

290. Perritt, *supra* note 178, at 4-5.
291. Goldman 2925-26.
292. Goldman 2925-28, 3025; Goldman, Privacy and Individual Empowerment in the Interactive Age at 13-16 (submitted for the record) [hereinafter Privacy and Individual Empowerment]; Kang 2946-48, 3012.
293. Privacy and Individual Empowerment, *supra* note 292, at 14; Varney 2933-34.
294. Privacy and Individual Empowerment, *supra* note 292, at 14-15.
295. Goldman 2948-49. For a description of PICS, see note 259 *supra*, and accompanying text.
296. Hendricks 2957-59; Plessner 2968.
297. Gitlitz 2915; Strenio 3003-06.
298. Kang 2931; Strenio 2969-71; Wellbery 2974.
299. Gitlitz 2910-11, 2917.
300. Wellbery 2974; Goldman 2931.
301. Gitlitz 2919.
302. Strenio 2970; Belair 2955; Baker 2964.
303. Nisenholtz 2748. In 1967, the leading slide rule manufacturer commissioned a study of the future of technology that predicted video phones and bed-making machines but missed the development of electronic calculators. Ten years later, it was out of business.
304. Gross 2856.
305. Gross 2856.
306. Gross 2856-57.
307. Young 2253.
308. Levin 3040.
309. Levin 3054.

310. Levin 3056.
311. Moore 2341-42.
312. Levin 3064-77 (demonstrating the first digital interactive cable network now operating in Orlando, Florida).
313. Sackler 2727.
314. Gross 2742.
315. Gross 2742-43.
316. Andreotta 2493.
317. Andreotta.
318. Levin 3043; Michelotti 2775-76.
319. Kimmelman 2312; see also the discussion of Commissioner Varney and Mr. Levin 3087-3088.
320. See discussion of Chairman Pitofsky and Mr. Levin 3081-82.
321. Young 2249.
322. Gross 2855.
323. Gross 2856-57.
324. See Chapter I, Volume I of this report.
325. Larabie-LeSieur 3118.
326. Michelotti 2779-80; Barker 2632-33; Zubrod 3091; Larabie-LeSieur 3124; Harris 3107, 3113; Held 3130.
327. Blatch 3252; Guarino 3254-55.
328. Michelotti 2779-80; Post 2822.
329. Chapter I, Volume 1 of this report, at 2.

Consumer Protection in the New High-Tech, Global Marketplace

330. *Id.* at 5-6. Exports grew from 5.5% to 12% of the gross national product, while imports grew from less than 7% to more than 14%.
331. *Id.* at 7-8.
332. *Id.* at 6.
333. Blatch 3250-51. The Canadian experience in harmonizing standards internally revealed that the business community is often more concerned about having to meet differing standards than it is about having to meet high consumer protection standards. Hoffman 3225; Thompson 3239-41.
334. MacLeod 3175.
335. Starek 3172; MacLeod 3175, 3179. Germany, for example, prohibits comparative advertising; its concern is unfair competition, not consumer protection. A recent EU directive would allow more comparative advertising, however. MacLeod 3179; Blatch 3191-94.
336. Germany, for example, prohibits calls unless consumers give written permission in advance. Gallant 2659-60.
337. The U.S. imposes fewer regulations on the advertising of these products than many other countries. Silverglade 3188.
338. MacLeod 3180, 3265-66; Guarino 3245, 3254; Spivak 3207-08; Hall 3167.
339. Germany limits discount and premium offers. Blatch 3191-94, 3251. See also MacLeod 3175-76.
340. Michelotti 2779-80.
341. Michelotti 2780.
342. Steiger 3250; Blatch 3250-51; Silverglade 3183-84; MacLeod 3252-53; Guarino 3246.
343. Spivak 3208; Thompson 3239-42.
344. Hendricks 3008-09.
345. Blatch 3192-93; Guarino 3254-55.
346. Meier 3153-54, 3157-58. Not all obstacles are legal, of course; some are based on national differences in culture, consumer preferences, infrastructure, and payment systems. Hall 3162-65, 3164-70.

347. Among the agreements to lower barriers is The Agreement on Technical Barriers to Trade (TBT) which prohibits the discriminatory use of standards, and encourages the use of international standards to harmonize government regulations across borders. Similar principles are at the heart of NAFTA, the Asian and Pacific Economic Cooperation Agreement (APEC), and the nascent Free Trade Agreement of the Americas. Meier 3153-57.

348. The International Organization for Standardization (ISO) plays an important role in developing international voluntary standards, and its Consumer Policy Committee (COPOLCO) promotes national and international standardization from the consumer protection point of view. Spivak 3204-05, 3207-11.

349. Meier 3155.

350. The International Chamber of Commerce, for example, is working to establish codes for advertising practices. Blatch 3195. U.S. and European toy manufacturers, along with the Council of Better Business Bureaus, are developing guides for children's advertising. Spivak 3210-11. The direct marketing companies also have international self-regulatory programs underway. Gitlitz 2916.

351. Meier 3157.

352. Agencies need to be sensitive to the implications of their regulations. An example of rules with enormous ramifications for international companies were FDA's regulations under the Nutrition Labeling and Education Act. Guarino 3246-47.

353. Lord 3214-19; Priestland 3248-49.

354. Lord 3216.

355. Lord 3215. Apparel and textile trade grew among the NAFTA countries by 30% — to \$5.4 billion — in the first year of the trade agreement. *Id.* at 3217.

356. Lord 3215; Priestland 3249.

357. Silverglade 3183-84, 3247. International harmonization gives rise to some concern that consumer protection regulations may be harmonized downward to a low level of consumer protection. Silverglade 3186; Starek 3189. This need not be the case, however. Canada's experience with its internal harmonization effort, for example, proved just the opposite and produced uniformly high standards. Hoffman 3225-26.

358. Thompson 3237-42.

359. Lord 3214.

Consumer Protection in the New High-Tech, Global Marketplace

360. Hall 3167; MacLeod 3180-81.

361. Meier 3157; Silverglade 3185; Blatch 3190-91; Sackler 2650.

362. Spivak 3261.

363. Lord 3218.

364. The Commission can both learn and contribute in these settings. Thompson 3263; Spivak 3258.

365. To be effective, the Commission needs to present not just its views, but studies and evidence to support its policies. MacLeod 3181-82.

APPENDIX A**HEARING PARTICIPANTS**

Robert H. Alter
Cabletelevision Advertising Bureau

Ralph Andreotta
AT&T

Stewart Baker
Steptoe & Johnson

John Barker
National Fraud Information Center

Robert R. Belair
Privacy & American Business

David Bell
Bozell, Inc.

Jerry Berman
Center for Democracy & Technology

D. Douglas Blanke
Office of the Minnesota Attorney General

Mari Ann Blatch
Reader's Digest Association, Inc.

George Braasch
Spiegel, Inc.

Eric Brown
Assistant Attorney General of Ohio

M. Zane Brown
Consumer Products Directorate

J. Beckwith Burr
Federal Trade Commission

William Burrington
America Online, Inc.

Charles Burson
Attorney General of Tennessee

Steven J. Cole
Council of Better Business Bureaus, Inc.

Scott Cooper
Intel Corporation

Barry Cutler
McCutchen, Doyle, Brown & Enersen

Nora Dowd
American Association of Retired Persons

James Doyle
Attorney General of Wisconsin

Harvey Dzodin
Capital Cities/ABC

James Gallant
NYNEX

Robert Gertner
University of Chicago, Graduate School of Business

Jonah Gitlitz
Direct Marketing Association

Janlori Goldman
Center for Democracy & Technology

Linda A. Goldstein
Hall, Dickler, Kent, Friedman & Wood

Debra Goldstein
Council of Better Business Bureaus

Dean Graybill
Federal Trade Commission

Barbara Gregg
Montgomery County (MD) Office of Consumer Affairs

Phill Gross
MCI Communications, Inc.

Elizabeth Toni Guarino
Buc, Levitt & Beardsley

Robert P. Hall III
National Retail Federation

Eileen Harrington
Federal Trade Commission

Scott Blake Harris
Federal Communications Commission

Richard D. Held
Visa International

Evan Hendricks
Privacy Times

Joseph Hoffman
Ontario Ministry of Consumer & Commercial Relations

Hubert H. Humphrey III
Attorney General of Minnesota

Wayne E. Huyard
MCI Communications, Inc.

Helene D. Jaffe
Weil, Gotshal & Manges
Mary Gardiner Jones
Consumer Interest Research Institute
Gene Kimmelman
Consumers Union, Washington Office
Jerry Kang
UCLA School of Law
Jane King
MCI Communications
Elaine D. Kolish
Federal Trade Commission
Rachel Larabie-LeSieur
Industry Canada
Gerald M. Levin
Time Warner Building
Susan Lord
American Textile Manufacturers Institute
William MacLeod
Collier, Shannon & Scott
Anne V. Maher
Federal Trade Commission
David Medine
Federal Trade Commission
Richard G. Meier
Office of the U.S. Trade Representative
Carla Michelotti
Leo Burnett Company
Olan Mills II
Olan Mills, Inc.
Michael Moore
D'Arcy, Masius, Benton & Bowles, Inc.
Lucy Morris
Federal Trade Commission
Martin Nisenholtz
The New York Times Electronic Media Company
C. Lee Peeler
Federal Trade Commission
Robert Pitofsky
Federal Trade Commission Chairman
Ronald Plesser
Piper & Marbury

Robert Pollin
AutoScribe, Inc.

Mary Ponder
Consumer Federation of America

David Post
Georgetown Cyberspace Law Institute

Carl Priestland
American Apparel Manufacturers Association

Herbert Rotfeld
Auburn University, Department of Marketing

Arthur B. Sackler
Time Warner Inc.

Jorge Reina Schement
Pennsylvania State University, College of Communications

Teresa Schwartz
Federal Trade Commission

Robert Sherman
Paul, Hastings, Janofsky & Walker

Mark Silbergeld
Consumers Union, Washington Office

Bruce Silverglade
Center for Science in the Public Interest

Katrinka Smith Sloan
American Association of Retired Persons

Steven Spivak
Chairman, University of Maryland

Roscoe B. Starek, III
Federal Trade Commissioner

James Steel
Master Card International

Janet P. Steiger
Federal Trade Commissioner

Andrew Strenio
Hunton & Williams

Michael Thompson
Whirlpool Corporation

Christine A. Varney
Federal Trade Commissioner

Daniel J. Weitzner
Platform for Internet Content Selection

Barbara S. Wellbery
National Telecommunications & Information Administration

Arthur White
Yankelovich Partners, Inc.
William Wilkie
University of Notre Dame, Department of Marketing
James Young
Bell Atlantic
Mark Zalewski
Cybercash, Inc.
Gordon Zubrod
Assistant U.S. Attorney, Middle District of Pennsylvania

APPENDIX B

HEARING AGENDA

Thursday, November 16, 1995

Presiding for Opening Session — Chairman Robert Pitofsky

Welcome and opening remarks.

Panel 1: The Changing Marketplace

- A. The Changing Face of Marketing
David Bell, Chairman, Bozell, Inc.
- B. The Evolution of Payment Systems
Robert Pollin, President, AutoScribe, Inc.
- C. The Year 2000: The Communications Technologies
James Young, Vice President and General Counsel, Bell Atlantic
- D. The Year 2000: Technologies & The Consumer
Arthur White, Vice Chairman, Yankelovich Partners, Inc.
- E. Consumer Protection Issues in the High-Tech, Global Marketplace
Charles Burson, Attorney General of Tennessee
Gene Kimmelman, Co-Director, Consumers Union (Washington Office)

Thursday, November 16, 1995

Presiding for the Afternoon Session — Commissioner Janet D. Steiger

Panel 2: The Changing Role of Television in Marketing

- A. The Evolution of Television Advertising
Michael Moore, Corporate Executive Vice President, D'Arcy, Masius, Benton & Bowles
- B. Consumer Protection Issues for Television Advertising & the FTC
Mark Silbergeld, Co-Director, Consumers Union (Washington Office)
Barry Cutler, McCutchen, Doyle, Brown & Enersen
- C. Self-Regulation and the Future of Television Advertising
Debra Goldstein, Director, National Advertising Division, Council of Better Business Bureaus

Herbert Rotfeld, Professor of Marketing, Auburn University College of Business

Robert Alter, Vice-Chairman, Cabletelevision Advertising Bureau

Round Table Discussion with Panelists and Commentators:

Harvey Dzodin, Vice President, Commercial Standards, Capital Cities/ABC

Helene D. Jaffe, Chair, Consumer Protection Committee, ABA Antitrust Section; Weil, Gotshal & Manges

Mary Ponder, Senior Projects Director, Consumer Federation of America

William Wilkie, Professor of Marketing, University of Notre Dame

Friday, November 17, 1995

Presiding for the Morning Session — Commissioner Janet D. Steiger

Panel 3: the Changing Role of the Telephone in Marketing

A. An Overview of Telephone Technologies

Ralph Andreotta, Director, Technology and Infrastructure, AT&T

B. Marketing by Telephone: An Overview and Demonstration

Wayne Huyard, President, MCI Mass Market, Sales & Service

C. Consumer Protection & Telemarketing Fraud

James Doyle, Attorney General of Wisconsin

James Steel, Vice President, Security & Risk Management, MasterCard

Katie S. Sloan, Manager, Consumer Affairs, American Association of Retired Persons

D. Consumer Protection & Pay-Per-Call Services

Scott Cooper, Manager, Government Affairs, Intel Corporation

William Burrington, Assistant General Counsel & Director of Policy, America Online

Round Table Discussion with Panelists and Commentators:

Linda Goldstein, Hall, Dickler, Kent, Friedman & Wood

Jane King, Senior Manager, Law & Public Policy, MCI

Olan Mills II, Chairman, Olan Mills, Inc.

Friday, November 17, 1995*Presiding for the Afternoon Session — Chairman Robert Pitofsky***Panel 4: Telephone Technologies: Emerging Issues****A. The Next Generation of Consumer Protection Issues****Jorge Reina Schement**, Dean, Graduate Studies & Research, College of Communications, Pennsylvania State University**John Barker**, Director, National Fraud Information Center; Vice President, National Consumers League**B. Consumer Education & Self-Regulation****Arthur B. Sackler**, Vice President for Law and Policy, Time Warner Inc.**James Gallant**, Director of Marketing, NYNEX**Round Table Discussion with Panelists and Commentators:****George Braasch**, Corporate Credit Counsel, Spiegel, Inc.**Eric Brown**, Assistant Attorney General of Ohio**Nora Dowd**, Deputy Attorney General, Office of the Pennsylvania Attorney General (on leave with AARP Telemarketing Fraud Project)**Barbara Gregg**, Director, Montgomery County (MD) Office of Consumer Affairs**Monday, November 20, 1995***Presiding for the Morning Session — Commissioner Christine A. Varney***Panel 5: The Newest Medium for Marketing: Cyberspace****A. Demonstration and Overview of the Technology****Phill Gross**, Director, Internet Marketing, MCI Telecommunications Division**B. Marketing in Cyberspace****Martin Nisenholtz**, President, New York Times Electronic Media Company**Carla Michelotti**, Senior Vice President, Leo Burnett Co.**Robert Gertner**, Professor of Economics & Strategy, University of Chicago Graduate School of Business

C. Consumer Protection Issues in Cyberspace

Hubert H. Humphrey III, Attorney General of Minnesota

D. Alternative Approaches to Protecting Consumers in Cyberspace

Steve Cole, Senior Vice President, Council of Better Business Bureaus

Daniel Weitzner, Co-Chair, Platform for Internet Content Selection (PICS)

David Post, Professor of Law, Georgetown University Cyberspace Law Institute

William Burrington, Assistant General Counsel & Director of Policy, America Online

Round Table Discussion with Panelists and Commentators:

Jerry Berman, Executive Director, Center for Democracy & Technology

Mary Gardiner Jones, President, Consumer Interest Research Institute

Robert Sherman, Paul, Hastings, Janofsky & Walker

Mark Zalewski, Director, Business Development, Cybercash, Inc.

Monday, November 20, 1995

Presiding for the Afternoon Session — Commissioner Christine A. Varney

Panel 6: Privacy in Cyberspace

Jerry Kang, Professor of Law, UCLA School of Law

Jonah Giltitz, President, Direct Marketing Association

Janlori Goldman, Deputy Director, Center for Democracy & Technology

Round Table Discussion with Panelists and Commentators:

Stewart Baker, Steptoe & Johnson

Robert R. Belair, Editor, Privacy and American Business

D. Douglas Blanke, Director of Consumer Policy, Office of the Minnesota Attorney General

Evan Hendricks, Publisher/Editor, Privacy Times

Ronald Plessner, Piper & Marbury

Andrew J. Strenio, Hunton & Williams

Barbara S. Wellbery, Chief Counsel, National Telecommunications & Information Administration, U.S. Department of Commerce

Tuesday, November 21, 1995*Presiding for the First Presentation — Chairman Robert Pitofsky***Convergence of Technologies and Globalization****Gerald Levin**, Chairman and Chief Executive Officer, Time Warner Inc.*Presiding for the Morning Session — Commissioner Roscoe B. Starek, III***Panel 7: Globalization and Cross Border Fraud****A. An Overview****Gordon Zubrod**, Assistant U.S. Attorney, Middle District of Pennsylvania**B. Cross Border Consumer Fraud****Scott Blake Harris**, Chief, International Bureau, Federal Communications Commission**Richard D. Held**, Senior Vice President, Risk Management and Security, Visa International**Rachel Larabie-LeSieur**, Director, Marketing Practices, Industry Canada**Tuesday, November 21, 1995***Presiding for the Afternoon Session — Commissioner Roscoe B. Starek, III***Panel 8: International Trade and Consumer Protection Issues —****A. Overview of International Trade Developments****Richard G. Meier**, Deputy Associate Trade Representative, Office of U.S. Trade Representative**Robert P. Hall III**, Vice President, Government Affairs Counsel, National Retail Federation**B. Differing National Laws and Implications for the FTC****William MacLeod**, Collier, Shannon & Scott**Mari Ann Blatch**, Vice President, Government Affairs, Readers Digest**Steven Spivak**, Professor, University of Maryland, Chairman, Consumer Policy Committee, International Organization for Standardization**Susan Lord**, Vice President, Government Relations, Springs Industries, Inc.; Chairman, Export Subcommittee, American Textile Manufacturers Institute

Appendix B

Bruce Silverglade, Director, Legal Affairs, Center for Science in the Public Interest

Zane Brown, Director General, Consumer Products Directorate, Industry Canada

Joseph Hoffman, Director of Policy, Ontario Ministry of Consumer & Commercial Relations

Round Table Discussion with Panelists and Commentators:

E. Toni Guarino, Buc, Levitt & Beardsley, International Bar Association Council

Carl Priestland, Chief Economist, American Apparel Manufacturers Association

Michael Thompson, Director, Government Relations, Whirlpool Corporation

EXHIBIT 2

WWW.FTC.GOV

**Excerpts from the Web Site
of the
Federal Trade Commission**



WORKING FOR CONSUMER PROTECTION
AND A COMPETITIVE MARKETPLACE

Current News Releases

[California U.S. Postal Service
Planned to Merge in
Consumer Market](#)



**Who We Are &
How We Serve You**



**Legal
Framework**



**Consumer
Protection**



**Antitrust/
Competition**



**Business
Guidance**



**Economic
Issues**



**Formal Actions,
Opinions & Activities**



**News Releases,
Publications & Speeches**



**Regional
Offices**

**Privacy
Statement**

- [Contact Us](#)
- [Search](#)
- [Site Directory](#)
- [Glossary](#)
- [New Additions](#)
- [Related Sites](#)

Last Update: Thursday, January 22, 1998



Enter words describing a concept or keywords you wish to find information about:

Start Search

Documentation about [making speeches](#) is available.

Contact Us

Search

Site Directory

Glossary

Home



ConsumerLine is the online service of the Office of Consumer and Business Education of the Bureau of Consumer Protection. It offers the full text of consumer publications on a wide range of categories. In addition, it offers **Education Campaigns** -- a collection of on-going consumer information initiatives -- and **Consumer Alerts!** -- brief publications with concise information about current issues.

[Publications](#)[Consumer Alerts](#)[Searching Consumer Alerts](#)[Education Campaigns](#)[1997 Consumer's Resource Handbook](#)[Publications in Spanish](#)

[Contact Us](#)[Search](#)[Site Directory](#)[Glossary](#)[Home](#)

Last Revised: Tuesday, September 16, 1997



Consumer Alerts!

- [Just When You Thought It Was Safe... Advance Fee Loan "Sharks" \(1/98\)](#)
- [Federal and Postal Job Scams: Tip-offs to Rip-offs \(1/98\)](#)
- [Look Before You Lease \(12/97\)](#)
- [FCC License Auctions \(11/97\)](#)
- [Virtual "Treatments" Can Be Real-World Deceptions \(11/97\)](#)
- [Is There a Bandit in Your Mailbox? \(10/97\)](#)
- [How to Dodge a Display Rack Scam \(08/97\)](#)
- [Green Card Lottery Scams \(08/97\)](#)
- [Spotting Sweet-Sounding Promises of Fraudulent Invention Promotion Firms \(07/97\)](#)
- [How to Avoid Losing Your Money to Investment Frauds \(07/97\)](#)
- [Avoiding the Muscle Hustle: **Tips for Buying Exercise Equipment** \(06/97\)](#)
- [D.C. Residents: Thinking About a Home Improvement? Don't Get Nailed](#)
- [Public Safety Fund-Raising Appeals: Make Your Donations Count \(04/97\)](#)
- [Paunch Lines: Weight Loss Claims Are No Joke For Dieters \(03/97\)](#)
- [Advertisements Promising Debt Relief May Be Offering Bankruptcy \(03/97\)](#)
- [Traveler's Advisory: Get What You Pay For \(03/97\)](#)
- [Beloved...Bejeweled...Be Careful: What to Know Before You Buy Jewelry \(02/97\)](#)
- [International Telephone Numbers Scams \(12/96\)](#)
- [Phone, E-Mail, and Pager Messages May Signal Costly Scams \(12/96\)](#)
- [Kitchen Gadgets Offer Food for "Thaw-t" \(12/96\)](#)
- [Profits in Pyramid Schemes? Don't Bank on It \(11/96\)](#)
- [When Opportunity Knocks... See Who's There \(11/96\)](#)
- [OUCH...Students Getting Stung Trying to Find \\$\\$\\$ for College \(09/96\)](#)
- [Getting Purse-onal \(08/96\)](#)
- [Border-Line Scams Are the Real Thing \(06/96\)](#)
- [Penny Wise or Pump Foolish? \(05/96\)](#)

[Contact Us](#)
[Search](#)
[Site Directory](#)
[Glossary](#)
[Home](#)

Last Revised: Thursday, January 22, 1998

EXHIBIT 3

WWW.CONSUMER.GOV



U.S. CONSUMER GATEWAY

Your Link to Federal Consumer Information

www.consumer.gov

About This Site



This federal guidebook is divided into two sections: the first, on buying and selling products and services, and the second, a directory of federal, state, municipal, and corporate consumer contacts.

CPSC, Headstrom Announce Recall of Glide Rides

About 1.5 million Glide Rides, sold with backyard gym sets, are being recalled for in-home repair.

CPSC & Graco Announce Recall to Repair Carriers & Carrier/Swing Seats

About 564,000 Graco carriers and carrier/swing seats recalled for repair. The handle on the seats can unlock unexpectedly.

Grandparent's Guide

The CPSC and Pampers Parenting Institute offer important safety & child nurturing tips to grandparents.

Holiday Shopping Tips

The Federal Trade Commission has prepared a few tips to remind consumers of their rights when ordering and paying for gifts.

FDA Approves Irradiation of Meat for Pathogen Control

The Food and Drug administration today approved irradiation of meat products for controlling disease-causing micro-organisms.

healthfinder

Healthfinder is a gateway to consumer health and human services information from the United States Government.

Of Special Interest

Scam Alert

Project Mousetrap

A warning about "invention-promotion" scams.

Stock Market Phone Fraud

SEC warning about stock market fraud.

[Food](#) | [Health](#) | [Your Home](#) | [Transportation](#) | [Children](#) | [Buying Smart](#) | [Product Safety](#)
[Your Money](#) | [Education](#) | [Other](#) | [Site Map](#) | [About this Site](#)
[Consumer's Handbook](#)
[Privacy Policy](#)
[Talk to Us](#)

Last Updated: Wednesday, January 21, 1998



U.S. CONSUMER GATEWAY

About This Site

The *U.S. Consumer Gateway* -- "consumer.gov" -- is a "one-stop" link to a broad range of federal information resources available online. It is designed so that you can locate information by category -- such as *Food, Health, Product Safety, Your Money, and Transportation*. Each category has subcategories to direct you to areas within individual federal web sites containing related information.

The *U.S. Consumer Gateway* is a "work-in-progress." Be on the lookout for more federal information sites added and a refined navigation mechanism.

ScamAlert! provides current information on fraudulent and deceptive practices in the marketplace. This feature appears on each page, as necessary, and contains important law-enforcement information and tips to avoid scams.

Of Special Interest showcases new education and consumer awareness campaigns and other items of significant interest.

The *U.S. Consumer Gateway* web site has been optimized for [Netscape](#) version 2.0 or higher and [Internet Explorer](#) version 3.0 or higher. Download these browsers by clicking on one of the links above.

Participating Agencies and their protection responsibilities:

The Federal Trade Commission (FTC)

The Federal Trade Commission works to eliminate unfair or deceptive practices in the marketplace. The FTC's efforts are primarily directed toward stopping actions that threaten consumers' opportunities to exercise informed choice.

The Securities and Exchange Commission (SEC)

The Securities and Exchange Commission enforces the laws that ensure the fairness of the securities markets and that guarantee that investors have access to all material information concerning publicly traded securities.

The U.S. Consumer Product Safety Commission (CPSC)

The U.S. Consumer Product Safety Commission is charged with reducing unreasonable risks of injury from consumer products. The CPSC has jurisdiction over approximately 15,000 products in the home, in schools, and in recreation.

The Food and Drug Administration (FDA)

The Food and Drug Administration scrutinizes food, cosmetics, medicines, medical devices, and radiation-emitting products, such as microwave ovens, to ensure that they are safe, wholesome, and will not cause human injury or harm. The FDA has similar responsibility for

feed and drugs for farm animals and pets.

The National Highway Traffic Safety Administration (NHTSA)

The National Highway Traffic Safety Administration is responsible for reducing deaths, injuries, and economic loss caused by motor vehicle crashes. NHTSA establishes and enforces safety performance standards for motor vehicles and items of motor vehicle equipment and conducts public safety programs.

The U.S. Office of Consumer Affairs (USOCA)

The U.S. Office of Consumer Affairs helps shape and advance federal consumer policies. USOCA provides leadership and coordination to Federal consumer programs and serves as an advocate in the federal policy development process.

[Food](#) | [Health](#) | [Your Home](#) | [Transportation](#) | [Children](#) | [Buying Smart](#) | [Product Safety](#)
[Your Money](#) | [Education](#) | [Other](#) | [Site Map](#) | [About this Site](#) | [HOME](#)
[Talk to Us](#)

Last Updated: Thursday, October 09, 1997

EXHIBIT 4

FTC "Teaser" Sites

Business Opportunity "Teaser"

The Ultimate Prosperity Page

THE ULTIMATE HOME BASED BUSINESS IN AMERICA!!!



Earn \$60,000 to \$100,000 YOUR VERY FIRST MONTH!!!


Hundreds of people have earned over \$50,000 in their first 30 days -- and you can too!

Start your own outrageously profitable part-time business!

Use your telephone and computer modem to make money, even if you are not home.

- No paper work
- No full-time effort required
- No capital investment
- No franchise fee
- No employees
- NO RISK!

Tell me more!

 for more information

\$\$\$ MAKE \$2,000 A DAY \$\$\$ USING YOUR TELEPHONE AND MODEM!

How would you like to be your own boss and earn up to \$2000 a day or more just for turning on your computer? It can be yours for just loading our **FREE** modem software onto your computer and turning it on. It's really that simple! Honest!

UPP spent a year researching home businesses and our computer modem package ranked far above the rest. It has tested to be the nation's #1 money making opportunity. We guarantee that our start-up kit along with our **FREE** software will make you money the first day that you load it and turn on your computer.

See what other entrepreneurs are saying:

"I live a Life of Freedom. This is a total **TURNKEY** Business with a Low Start-Up Cost...but Quick Profits."

-- E. Doe, Milwaukee, WI

"This is the business of the '90s. As a marketing consultant, I've investigated many programs in the last 5 years. UPP's modem program is one of the best opportunities I've seen."

-- Allen Hancock, *President of Hancock Consulting.*

"I turned on my computer modem on New Year's Day and grossed \$49,442 by Easter. Best of all, I did it all from my den. No more 9 to 5, every day of the week for me."

-- J. Klondike, MN

How do I sign up and begin making money?



for more information



If you responded to an ad like The Ultimate Prosperity Page...

YOU COULD GET SCAMMED!

The Ultimate Prosperity Page does not advertise a real business opportunity. The ad is a fake, posted by the Federal Trade Commission to raise awareness about the hazard of business opportunity fraud on the Net. *No information about you has been transmitted to or collected by the FTC.*

DON'T BE A VICTIM OF CYBERFRAUD

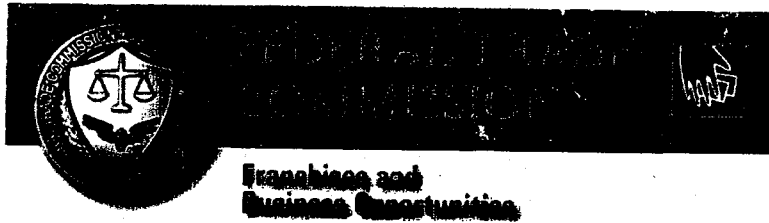
- Beware of online business opportunity advertisements that make exaggerated earnings claims and ads that offer little product information but lots of glowing promises.
- Use *extreme* caution before sending bank account or credit card information online. The Net is NOT a secure environment for financial transactions yet.
- Also use caution when transmitting your address and other personal information. This information is used by scam artists to compile "sucker" lists.

BEFORE YOU INVEST...

- Get disclosure documents and review them carefully. In most cases, the law requires business opportunity and franchise promoters to give potential buyers detailed information about the business and about company finances.
- Check to make sure the business opportunity is in compliance with applicable state registration laws.
- Research the business and the market, and talk to current investors.

Additional information about [Franchises and Business Opportunities](#) is available from the Federal Trade Commission.

Send comments on The Ultimate Prosperity Page to opr@ftc.gov.



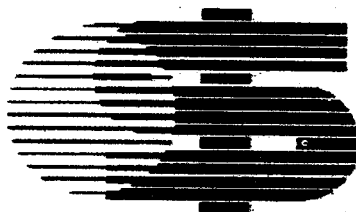
- **Regulatory Reform:** [Franchise Rulemaking](#) **NEW**
- **Regulatory Reform:** [Franchise Rule Review](#)
- **Before You Buy:** [Franchise and Business Opportunity Pamphlets](#)
- **Consumer Alert:** [Enforcement "Sweeps" Target Business Opportunity Fraud](#)
- **Your Legal Rights:** [Guide To The FTC Franchise Rule](#)
- **Franchise Rule Text:** [Ls CFR Part 436](#)
- **State Disclosure Requirements:** [Franchises and Business Opportunities](#)
- **Know The Risks:** [Summary of Recent Enforcement Cases](#)
- **How To Comply:** [Recent Staff Advisory Opinions](#)
- **Franchise and Business Opportunity** [FAQS](#)

[Contact Us](#) [Search](#) [Site Directory](#) [Glossary](#) [Home](#)

Last Updated: Wednesday, September 17, 1997



Pyramid Program "Teaser"



LOOKING FOR FINANCIAL FREEDOM?

- **Most people only dream about financial independence.**
- **Only a few unique individuals have those qualities that *ensure success*.**
- **Our revolutionary, no-risk networking system guarantees lucrative commissions and bonuses!**

GET IN ON THE GROUND FLOOR!

[NEXT]



**EARN AS MUCH AS \$50,000 IN 90 DAYS!
MAKE BIG MONEY FROM YOUR HOME COMPUTER.**

Are you looking for an MLM opportunity that requires:

- No prior experience
- No product knowledge

Are you interested in:

- Setting your own hours or working at home
- Excellent support and training
- Low-cost sponsorship kits
- Outstanding profits from your growing downline distribution

**GET IN EARLY TO TAKE ADVANTAGE
OF THIS UNIQUE GROUND-LEVEL OPPORTUNITY!!**

Look how quickly your earnings can multiply with our easy, proven "forced binary matrix" system:

Just recruiting a few people -- friends, neighbors, co-workers -- quickly adds up to **BIG** profits:

LEVEL	# PEOPLE	\$ VOLUME	\$ BONUSES
1	5	\$ 500	\$ 25
2	25	\$ 2,500	\$ 125
3	125	\$ 12,500	\$ 625
4	625	\$ 62,500	\$ 3,125

[NEXT]



**IF YOU RESPOND
TO AN AD LIKE THIS ONE
YOU COULD GET SCAMMED!**

This ad is a *fake*, posted by the Federal Trade Commission to increase awareness of potentially fraudulent multi-level marketing plans that are nothing more than "pyramid" scams.

THERE ARE NO PROFITS BURIED IN PYRAMIDS!!

To learn more about how to avoid fraudulent multi-level marketing or pyramid schemes and other online scams, visit the [FTC's website](#).

No information about you has been transmitted to or collected by the Federal Trade Commission.

Comments: pyramid@ftc.gov



TIPS TO AVOID PYRAMID SCHEMES

- 1 Avoid any plan that offers commissions to recruit new distributors.
- 2 Beware of plans that ask you to spend money on costly inventory.
- 3 Be cautious of claims that you will make money by recruiting new members instead of on sales you make yourself.
- 4 Beware of promises about high profits or claims about "miracle" products.
- 5 Be cautious about references; they could be "shills" by the promoter.
- 6 Don't pay money or sign contracts in a high-pressure situation.
- 7 Check out all offers with your local Better Business Bureau and state Attorney General.

- [Consumer Alert](#)

- [Public Service Messages](#)

- [Educa Alliance](#)

An actual case brought by the FTC against an alleged pyramid scheme

Comments: [1](#)

Scholarship "Teaser"

NEED MONEY FOR TUITION ????

A+ FAST CASHH



YOUR ONLY SOURCE FOR COLLEGE AID !!

**YOU'RE SMART ENOUGH TO GET INTO COLLEGE,
NOW BE SMART ENOUGH TO LET SOMEONE ELSE PAY**

**A+ FAST CASHH IS AN AAA RATED SCHOLARSHIP
SERVICE**

We search Public and Private Databases with our Proprietary
Software. This gives us access to THOUSANDS of Grants and
Scholarships just waiting for

*******YOU*******

**WE DO ALL THE WORK !!
Using our service, you are GUARANTEED
free money for all or part of your tuition.**



We get information directly from financial aid officers, corporate executives, and foundation heads about money returned to them by students who do not need assistance. We pass this inside information to our clients for no extra charge.



Because we provide personal attention to all our clients, we do not advertise in magazines or by direct mail. AND, you can get all your money back if you aren't satisfied.

TO START YOUR FAST CASH COMING COMPLETE THE APPLICATION FORM ON THE NEXT PAGE AND SEND IT TO US WITH YOUR CHECK FOR \$119.00. FOR FASTER RESULTS, CALL US WITH A CREDIT CARD NUMBER AND WE'LL START FINDING YOUR FAST CASH TODAY.



**IF YOU RESPOND TO AN AD LIKE THIS
ONE**

**YOU COULD GET
SCAMMED!**

**A+ FAST CASH is not a real company. The ad is a fake, posted by
the Federal Trade Commission to increase awareness of potentially
fraudulent scholarship services.**

**No information about you has been transmitted
to or collected by the FTC.**

**[Click here](#) to learn more about how to avoid fraudulent scholarship services and
other online scams, and for recommendations on where to find information on
obtaining legitimate scholarship information.**

SIX SIGNS THAT YOUR SCHOLARSHIP IS \$UNK

1 "THE SCHOLARSHIP IS GUARANTEED OR YOUR MONEY BACK."

No one can guarantee that they'll get you a grant or a scholarship. Refund guarantees often have conditions or strings attached. Get refund policies in writing before you pay.

2 "YOU CAN'T GET THIS INFORMATION ANYWHERE ELSE."

There are many free list of scholarships. Check with your school or library before you decide to pay someone to do the work for you.

3 "MAY I HAVE YOUR CREDIT CARD OR BANK ACCOUNT NUMBER TO HOLD THIS SCHOLARSHIP?"

Don't give out your credit card or bank account number on the phone without getting information in writing first. It may be a set-up for an unauthorized withdrawal.



4 "WE'LL DO ALL THE WORK"

Don't be fooled. There's no way around it. You must apply for scholarships or grants yourself.

5 THE SCHOLARSHIP WILL COST YOU SOME MONEY.

Don't pay anyone who claims to be holding a scholarship or grant for you. Free money shouldn't cost a thing

6 "YOU'VE BEEN SELECTED" BY A 'NATIONAL FOUNDATION' TO RECEIVE A SCHOLARSHIP, OR "YOU'RE A FINALIST" IN A CONTEST YOU'VE NEVER ENTERED.

Before you send money to apply for a scholarship, check it out. Make sure the foundation or program is legitimate.

NEED MONEY FOR COLLEGE? Check with your school guidance counselor or local librarian for free information about current scholarships before you pay someone for the same-or similar-scholarship lists. To find out how to spot, stop and report a scam, contact the Federal Trade Commission at <http://www.ftc.gov>, or call the National Fraud Information Center at, 1.800.876.7060

Consumer Alert

Federal Trade Commission • Bureau of Consumer Protection • Office of Consumer and Business Education

OUCH...Students Getting Stung Trying to Find \$\$\$ for College

Washington, D.C. -- Need money for college? Doesn't everybody?

With tuition bills skyrocketing, and room and board going through the roof, students and their families are looking for creative ways to finance a college education. Unfortunately, in their efforts to pay the bills, many of them are falling prey to scholarship scams.

According to the Federal Trade Commission, unscrupulous companies *guarantee or promise* scholarships or grants. Some guarantee that they can get scholarships on behalf of students or award them "scholarships" in exchange for an advance fee. Most offer a "money back guarantee"— but attach conditions that make it impossible to get the refund. Others provide nothing for the student's advance fee — not even a list of potential sources; and still others tell students they've been selected as "finalists" for awards that require an up-front fee. Sometimes, these companies ask for a student's checking account to "confirm eligibility," then debit the account without the student's consent.

The FTC cautions students to look and listen for these tell-tale lines:

- "The scholarship is guaranteed or your money back."
- "You can't get this information anywhere else."
- "I just need your credit card or bank account number to hold this scholarship."
- "We'll do all the work."
- "The scholarship will cost some money."
- "You've been selected" by a 'national foundation' to receive a scholarship — or "You're a finalist" in a contest you never entered.

The FTC says many legitimate companies advertise that they can get students access to lists of scholarships in exchange for an advance fee. Others charge an advance fee to compare a student's profile with a database of scholarship opportunities and provide a list of awards for which a student may qualify. And, there are scholarship search engines on the World Wide Web. The difference: Legitimate companies never guarantee or promise scholarships or grants.

For more information on scholarship fraud, contact the FTC at www.ftc.gov. To find out how to finance a college education, contact Sallie Mae at www.salliemae.com. For information about spotting, stopping, or reporting a scam, contact the National Fraud Information Center at 1.800.876.7060 or at www.nfic.org.

##

September 1996

Travel Agent Opportunity "Teaser"

Want to make money? Love to travel?




BE AN INDEPENDENT TRAVEL AGENT!!!

EZ Travels

**PRESENTS A UNIQUE OPPORTUNITY
FOR ENTREPRENEURS WHO LOVE TO TRAVEL...**

Now you can earn **THOUSANDS OF DOLLARS** operating an *EZ Travels* independent travel agency from your home or office. With **NO PRIOR EXPERIENCE**, you can start earning **HUGE COMMISSIONS** from the first day you receive your deluxe *EZ Travels* Independent Travel Agent Kit. *EZ Travels* independent agents enjoy **FABULOUS DISCOUNTS** on luxury travel. Join our family of happy independent travel agents and **CHANGE YOUR LIFESTYLE FOREVER!!!**

Click on 
for more information

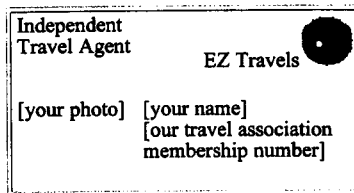


HOW IT WORKS

Yes, it's true. With *EZ Travels* you can operate your own independent travel agency. *EZ Travels* provides all the support you need. You just follow a few simple steps:

- Find out where and when your client wishes to travel
- Call *EZ Travels'* toll free number with your client's travel information
- Wait for *EZ Travels* to issue the tickets or other travel documents
- Deliver the travel documents you receive from *EZ Travels* to your client

IT'S THAT EASY! And with each travel sale you collect a **50% commission!!!**



BENEFITS FOR *EZ TRAVELS* INDEPENDENT AGENTS

Your deluxe *EZ Travels* Independent Travel Agent Kit includes an ID card (pictured above) with the *EZ Travels* logo, your photograph, and our travel association membership number. This card entitles you to all the discounts and benefits available to travel agents. Travel suppliers offer a wide variety of discounts and privileges to encourage travel agents to use their facilities, including:

- **HUGE DISCOUNTS** – 40, **50, 75%**
on vacation packages, car rentals and theme park admissions
- **MAJOR UPGRADES** on airline flights, cruises and hotel rooms

Click on 
for more information



TESTIMONIALS FROM EZ TRAVELS INDEPENDENT AGENTS

"I've saved thousands of dollars on hotels and airfares for myself and others with EZ Travels. My wife and I went on a fabulous week-long Carribean cruise for \$395 each when it would have normally cost \$1,695 each. I've also made in excess of \$6,000 in commissions."

-- Allen H., EZ Travels Independent Agent, South Carolina

"With no prior experience as a travel agent, I earned \$11,449 on my first two EZ Travels group tours of 43 people to Saipan, and 20 to Guam."

-- Thomas R., EZ Travels Independent Agent, California

"I'm a secretary at an ad agency in New York. Since I started booking travel for my work friends, I've made \$15,000 in commissions! With my EZ Travels ID card, my family and I have also gotten nearly free admission to Florida theme parks."

-- Carolyn S., EZ Travels Independent Agent, New York

TO PURSUE THE EZ TRAVELS OPPORTUNITY Click on





If you pursue the *EZ Travels* opportunity...

YOU COULD GET SCAMMED!

EZ Travels is not a real company. The *EZ Travels* opportunity to which you responded is a fake, posted by the Federal Trade Commission to highlight the hazards of travel agent credential fraud on the Net. *No information about you has been transmitted to or collected by the FTC.*

DON'T FALL FOR TRAVEL AGENT CREDENTIAL FRAUD

- Travel business opportunities like *EZ Travels'* are neither easy to operate nor generally profitable.
- Fraudulent travel agent identification cards generally don't qualify users for discounts and upgrades. They pump up the cost of travel for the public-at-large, and they deprive legitimate travel agents of limited available incentives and rewards.

BEFORE YOU INVEST...

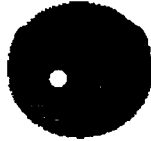
- Check to make sure the business opportunity is in compliance with applicable state registration laws
- Research the industry and the market, and talk to current investors

The FTC provides consumer information on **Franchises and Business Opportunities** and **Travel Fraud**. Additional information on Travel Fraud is available from the **American Society of Travel Agents**.

Send comments on the *EZ Travels* page to travelscams@ftc.gov.

Travel Award "Teaser"

Certificate of Notification



You are hereby notified you will receive a
**FABULOUS FLORIDA/CARIBBEAN VACATION
OFFER, INCLUDING ALL ACCOMMODATIONS!**

MUST BE 21 YEARS OF AGE OR OLDER TO PARTICIPATE

EZ Travels is delighted to advise you of this offer via The
Internet.

The offer includes their **FUN-FILLED 4-DAY THEME PARK
ROMP**
for the whole family! In celebration! you will receive their
SPECTACULAR 8-DAY LUXURY DREAM VACATION offer for
two!

- 4 fun-filled days and 3 exciting nights in **MAGICAL ORLANDO**, home of Walt Disney World, Universal Studios, and Sea World!
- 7 days exploring **GRAND BAHAMA ISLAND!** Stay at a World Famous Resort with two 18-hole golf courses, 12 tennis courts, 9 restaurants, a luxury spa, and magnificent pools. Plus, shopping at the adjacent International Bazaar, or just relax on one of their sandy, white beaches!

***A toll free hotline has been established
for your immediate confirmation!***

Who is authorized to use this toll free claim line?

Individuals who receive notification from *EZ Travels* via The Internet are authorized to use this claim line.

In what capacity does *EZ Travels* function?

EZ Travels regulates and administers the disbursement of promotional vacation packages to promote Florida/Caribbean tourism. All accommodations provided at nationally recognized hotels. *EZ Travels* is registered with major professional travel associations.

Consumer Disclosure

This offer is not available to the general public. Vacations include hotel lodging plus round-trip airfare to Florida and are offered to recipients of this certificate at a discounted rate. Vacations do not include taxes, service fees, gratuities or meals. This is the only notification you will receive. Please call the toll free hotline within 72-hours of receipt. This is not a contest, giveaway, sweepstakes or lottery. This offer is designed to promote Florida and Caribbean hotels and resorts. Only one call per recipient.

To call the toll free EZ Travels hotline... click here





If you call the *EZ Travels* toll free hotline...

YOU COULD GET SCAMMED!

EZ Travels is not a real company. The *EZ Travels* offer to which you responded is a fake, posted by the Federal Trade Commission to highlight the hazards of travel fraud on the Net. *No information about you has been transmitted to or collected by the FTC.*

DON'T BE A VICTIM OF TRAVEL FRAUD

- A "SPECTACULAR LUXURY DREAM VACATION offer" isn't a free vacation. It's an *offer to sell* you a trip that may be luxurious -- or not.
- Taxes and service fees can substantially inflate the cost of a vacation.

BEFORE YOU BUY TRAVEL...

- Research the travel seller. Make sure the seller is a member of a professional travel association such as the American Society of Travel Agents, the National Tour Association or the United States Tour Operators Association.
- Verify arrangements before you pay. Get the details of your vacation in writing and a copy of the cancellation and refund policies. Ask if the business has insurance and whether you should buy cancellation insurance.

The FTC provides consumer information on Travel Fraud. Additional information on Travel Fraud is available from the American Society of Travel Agents.

Send comments on the *EZ Travels* page to travelscams@ftc.gov.



Planning a vacation? Be sure you get what you pay for.

- Be wary of "bargain" vacation offers on postcards and certificates. Hidden charges can add up.
- Adopt a "no-surprise" travel policy. Get the total cost in writing and know what it includes before you pay.
- Walk away from high-pressure sales pitches that don't give you time to think or plan.
- Give bank or credit card information only to businesses you know and trust. Never give unsolicited callers your bank account or credit card number, and never send money by overnight express.

Want more information?

Check out these FTC Publications:

- [Consumer Alert! Traveler's Advisory: Get What You Pay For](#)
- [Telemarketing Travel Fraud](#)
- [Timeshare Tips](#)
- [Timeshare Resales](#)

Or visit these travel sites:

- [American Society of Travel Agents](#)

- National Tour Association
 - US Tour Operators Association
-

Display Rack "Teaser"

EZ Toyz

presents an exciting investment opportunity for
the entrepreneur who insists on earning at least

\$100,000 PER YEAR

Distribute Licensed Products!!!

**Disney ● Warner Bros.
Coca-Cola ● Pepsi
NCAA ● NFL ● NBA ● NHL**

**EZ Toyz is seeking qualified investors to
distribute
these and other brand name, licensed products.**

- NO EXPERIENCE NECESSARY
- RESTOCK PROFITABLE
ACCOUNTS
- PART-TIME OR FULL-TIME
- WORK FROM HOME
- NO OVERHEAD

**Want more information on this exciting
opportunity?**





If you pursue the EZ Toyz opportunity...

You could get scammed!

EZ Toyz is not a real company. The EZ Toyz opportunity to which you responded is a fake, posted by the Federal Trade Commission to highlight the hazards of "licensed product" fraud on the Net. *No information about you has been transmitted to or collected by the FTC.*

Licensed product fraud typically involves the purchase of brand name products from a business opportunity promoter. The promoter claims the investor can make large profits by marketing the products on display racks.

DON'T FALL FOR LICENSED PRODUCT FRAUD

- **Check-out the promoter.** Call the legal department of the consumer products company. Ask if they've heard of the business opportunity promoter and whether the promoter is a "licensed distributor" of the company's products.
- **Get earnings claims in writing.** Insist that the promoter give you written information to support any earnings claims, including the number and percent of others who have earned as much as the promoter claims. Also, ask the promoter for the disclosure document required by law. If the promoter hesitates or refuses, walk away.

BEFORE YOU INVEST

- Check to make sure the business opportunity complies with applicable state registration laws
- Research the industry and the market and talk to current investors in person.

The FTC provides consumer information on [Franchises and Business Opportunities and Licensed Product Fraud \(Display Rack & Ruin\)](#).

Send comments on the EZ Toyz page to EZToyz@ftc.gov

Going to Display Rack and Ruin...

August 1997

Ever hear the phrase "all that glitters is not gold"? It applies to fraudulent display rack business opportunities.

Fraudulent promoters across the country are offering entrepreneurs like you the chance to make \$100,000 or more a year selling licensed products from well-known companies. Their pitches include some great claims: *No selling. You won't have to quit your job. You can work from home. You can make your own hours.* Indeed, they say that for an investment of as little as \$15,000, all you have to do is restock profitable high-traffic display rack locations like malls, shopping centers, gift shops, convenience stores, supermarkets, and chain drug stores.

Sounds like a dream opportunity, right? Wrong!

Entrepreneurs who invest in business opportunities like these rarely make the big money they're promised. Promoters often supply undesirable merchandise—for example, outdated products that may never have captured the public's attention—and unprofitable locations. In fact, would-be business owners generally lose their entire investment.

If you're thinking about investing in a display rack opportunity, the Federal Trade Commission has a message for you: Check out their claims to avoid going to display "rack and ruin."

Business Opportunity Checklist

- **Check out the promoter:**
 - Call the legal department of the company whose merchandise is being promoted.
 - Find out whether the promoter is affiliated with the company.
 - Ask if the company has ever threatened trademark action against the promoter.
- **Question promises that your entire investment will go for "display racks and initial inventory."** The promoter's sales commissions on your purchase of products may eat up as much as 30 to 40 percent of your investment.
- **Ask the promoter if you'll be charged wholesale or retail prices for your initial inventory.** If you pay retail, you'll have to mark up the price to make a profit. That means you probably won't move much inventory. Even if the promoter agrees to sell you inventory at wholesale prices, you may get out-of-date merchandise that never sold in the first place. Either way, you lose.
- **Check out locator companies.** These are third-party firms, usually recommended by the promoter, that you hire to locate display rack sites. The firms may claim they've done market surveys in your area. Ask for copies. Typically, a firm charges you \$200 per site; the locator gets half the fee. Since high-traffic stores could sell popular consumer products on their own, locators may be able to secure low traffic locations only.
- **Get a list of previous investors, as well as their addresses and phone numbers.** The FTC's Franchise Rule requires it, and any legitimate business should be happy to provide it. If possible, visit one or two investors—and their locations—in

person. If you call, you may talk to a "singer" or a "shill"—a person hired by the promoter to give a favorable report on the business.

- **Get earnings claims in writing as well as substantiation.** Insist that the promoter give you written substantiation in the disclosure document required by the Franchise Rule. Be sure this includes the number and percent of others who have earned at least as much as the promoter claims. If the promoter hesitates or refuses, walk away. Don't believe what they say about sales, profits, or income.
- **Consult an attorney, accountant, or other trusted financial or business advisor** before you sign any agreement or make any upfront payments. Ask your attorney to review the company's contract and advise you on how best to proceed.
- **Call your state Attorney General** or local consumer protection agency, and the Better Business Bureau where you live and where the promoter's business is headquartered. Ask if there are any unresolved consumer complaints on file. This is a prudent and practical way to proceed, but not foolproof.

For More Information and Help

If you think you've been defrauded by a display rack business opportunity promoter, contact the company and ask for a refund. Let the company know that you plan to contact law enforcement officials about your experience. Keep a record of your conversations and correspondence. If you send documents to the company, make sure you send copies, not originals. Send correspondence by certified mail, return receipt requested, so you have a record of what the company received.

If you can't resolve the dispute with the company, several organizations may be able to help you. Your phone book will have the names, addresses, and phone numbers for these organizations:

- **Your state Attorney General.** Most of these offices have divisions that deal with consumer protection issues.
- **The advertising manager of the publication that ran the business opportunity ad.**
- **The Federal Trade Commission.** To file a complaint with the FTC, write: Consumer Response Center, Federal Trade Commission, Washington, DC 20580. While the FTC cannot intervene in individual disputes, the information you provide may indicate a pattern of possible law violations requiring action by the Commission.
- **The National Fraud Information Center (NFIC)** at 1-800-876-7060, 9 a.m. - 5 p.m. EST, Monday through Friday. NFIC, a project of the National Consumers League, is a nonprofit organization that operates a hotline to provide services and help for consumers who may want to file complaints. NFIC also sends appropriate information to the Federal Trade Commission/National Association of Attorneys General Fraud Database.

For a free copy of **Best Sellers**, a list of the FTC's consumer and business publications, contact: Consumer Response Center, Federal Trade Commission, Washington, D.C. 20580; 202-326-2222; TDD: 202-326-2502.

Weight Loss "Teaser"

Shed Pounds *and* Enjoy Your Favorite Foods!

NordiCalite

~~the safe and natural way to lose weight...~~

***New Scandinavian herbal formula
shrinks fat cells!***



Have you tried starvation diets with little or no success?

Is your schedule too busy for daily trips to the gym?

Have you lost 5-10 pounds only to put the weight right back on?

Do you have trouble slimming down your hips, thighs, buttocks, and waistline?

Do you get hungry late in the afternoon or in the evening?

Do you suffer from cellulite?

Regular weight loss programs work for some people, but if you answered **YES** to three or more of these questions, then you **already** know that they may not work for **your** special metabolism. But there's good news! If other diets have failed you, we have a product that may be the secret to a **SLIMMER, TRIMMER YOU!**

New formula!

- NO dangerous pills to jangle your nerves!
- NO special "diet meals" to buy!
- NO expensive doctor visits!
- NO more rabbit food!

Tradition Meets the 21st Century:

From the Forests of the Northern Lights comes the Scandinavian weight loss breakthrough **guaranteed** to work for you. What's the secret? It's Essence of Malmös--a unique blend of all-natural herbs derived from the evergreen forests of Scandinavia.

After nearly three decades of scientific research, Dr. Pers Johannsen, Direktor of the Center for Weight Loss at the Göttenberg Institute, has identified the **molecular isomers** in natural Essence of Malmös. This concentrated extract burns fat by encouraging **isotonic thermogenesis**--the process of transforming fat reserves to produce energy.

For the first time, this special Essence of Malmös is available in gelcap form as ...

NordiCaLite

~~the safe and natural way to lose weight...~~

"You know how the camera add at least 10 pounds. A week of NordiCaLite before meals and I'm ready for the skimpiest bathing suit. It takes the weight off--especially those pockets of cellulite that exercise can't budge."

— Swimsuit issue cover model Vamishke

"On regular diets, I'd starve and starve and hardly lose a pound. But NordiCaLite gave my problem metabolism the jump start it needed. I lost 27 pounds in 5 weeks and went from a size 16 to a size 8 -- while enjoying all my favorites foods."

— Astrid S.

To enjoy the benefits of this slimming secret, you could spend thousands of dollars for a month at one of Scandinavia's most fashionable spas. But why bother when NOW you can pamper yourself with the very same delicious pre-meal beverage that fashionable Europeans drink to maintain their sleek, willowy shape. Relax with NordiCaLite before lunch and dinner and then enjoy all your favorite foods -- pasta, potatoes, even snack foods and sweets! You'll have that sleek Scandinavian silhouette in no time at all. A 30-day supply is \$29.95. Or save even more by getting a 60-day supply for only \$39.95!

CAUTION! If you begin losing weight too fast, switch to *one* delicious cup of NordiCaLite a day.

NordiCaLite...

- Clinically tested in Scandinavia
 - Recommended by doctors and pharmacists
 - Proven effective for men and women of all ages
-

Thirty-day supply...
only **\$29.95!**

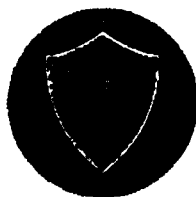
Special Introductory Offer!

NordiCaLite

Just dissolve one NordiCaLite in a glass of hot water at least 30 minutes before each meal. While you relax with this delicious, all-natural soothing beverage, the secret ingredient in NordiCaLite has already started to release the toxins trapped in your subcutaneous fat cells – those lumpy bulges that keep you from having the slim, trim silhouette you deserve.

We can thank the holistic practitioners of Scandinavia for the miracle we call NordiCaLite. The exclusive spas of Scandinavia are known for indulging their jet-set clients while helping them lose 10, 15, as much as 30 pounds in only 30 days! They know that all the calorie-counting and exercise in the world can't budge those lumpy, jiggly pouches of fat. To attack fat, you've got to break up those deposits from the inside out and release the toxins trapped inside.

[more]



If you responded to an ad like NordiCaLite...

**YOU COULD GET
SCAMMED!**

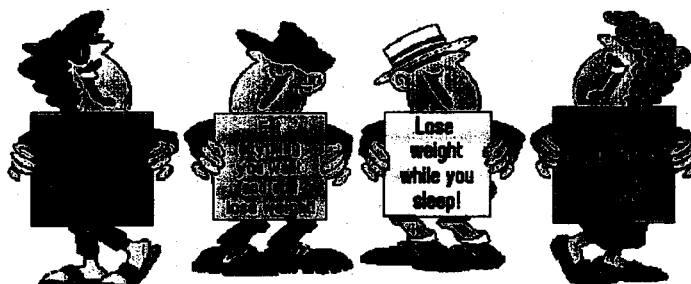
NordiCaLite *is not* a real weight-loss product.

The ad is a fake, posted by the Federal Trade Commission to raise awareness about the false and deceptive advertising claims made by many so-called "weight-loss" products.

**DON'T BE A VICTIM OF
WEIGHT-LOSS SCAMS!**

For more information, visit the FTC's "[Operation Waistline](#)" page.

Should You Believe These Amazing Claims?



You've Seen the Claims... Now Get the Facts!

- Claims for diet products and programs that promise effortless weight loss are false.
- To lose weight, you have to lower your intake of calories and increase your physical activity.
- As a rule, the faster you lose weight, the more likely you'll gain it back. Unless you're under a physician's care, don't go for programs that promise quick weight loss.
- Claims that you'll keep weight off permanently or for a long time usually are baloney. To maintain weight loss, change how you eat and how much you exercise.

For more information:

- Consumer Alert! Paunch Lines
- The Skinny on Dieting

HUD Tracer "Teaser"

UNITED STATES GOVERNMENT
HUD TRACER ASSOCIATION


WORK FOR THE GOVERNMENT -- FROM YOUR VERY OWN HOME

How can you make up to \$1500
by helping someone get money from HUD?

The federal government owes hundreds of millions of dollars to people just like you. You can become a Tracer for the Department of Housing and Urban Development (HUD) and earn as much as \$12,000 a month by helping others get the money owed to them by HUD. You'll work on behalf of HUD locating and contacting people that are owed money because they've paid off their home loans. Hundreds of thousands of people don't know this money's owed to them! Help them! Help HUD! Help yourself at the same time! It's fun and easy, and you can do it from the privacy and comfort of your very own home.

For only \$29.99, we'll send you:

- A list of the people due mortgage refunds from HUD with recent addresses;
- Tips on ways to locate these people;
- Tips on what to say once you've located them;
- Official government forms to use when processing their refunds;
- Tips on how to keep good records to keep the money coming in.

 for more information ...



If you responded to an ad like
The Tracer Association Page...

YOU COULD GET SCAMMED!

The Tracer Association Page does not advertise a real business opportunity. The ad is a fake, posted by the Federal Trade Commission to raise awareness about the hazard of business opportunity fraud on the Net. *No information about you has been transmitted to or collected by the FTC.*

DON'T BE A VICTIM OF CYBERFRAUD

- Beware of online business opportunity advertisements that make exaggerated earnings claims and ads that offer little product information but lots of glowing promises.
- Use *extreme* caution before sending bank account or credit card information online. The Net is NOT a secure environment for financial transactions yet.
- Also use caution when transmitting address and other personal information. This information is used by scam artists to compile "sucker" lists.

BEFORE YOU INVEST...

- Get disclosure documents and review them carefully. In most cases, the law requires business opportunity and franchise promoters to give potential buyers detailed information about the business and about company finances.
- Check to make sure the business opportunity is in compliance with applicable state registration laws.
- Research the business and the market, and talk to current investors.

Additional information about Franchises and Business Opportunities is available from the Federal Trade Commission. Real information is also available about the HUD/FHA mortgage insurance refund program. Send comments on The Tracer Association Page to tracer@ftc.gov.

EXHIBIT 5

**FTC "Teaser" Site
featured as
"New" Site of the Week**



Like a little more green in your life?

www.amway.com

[click here](#)

Like a little more green in your life?

Top: Business and Economy: Products and Services: Business Opportunities

Search Options

Search all of Yahoo Search only in Business Opportunities

• [Directories \(27\)](#)

- | | |
|--|--|
| • Classifieds@ | • Marketing@ |
| • Franchising@ | • Multi-Level Marketing (1536) |
| • Get Rich Quick!@ | • Restaurants (7) |
| • Health (60) | • Telecommunications (29) |
| • Insurance (2) | • Travel Agencies (12) |
| • Investment Opportunities (135) | • Vending Machines (30) |
| • Magazines@ | • Usenet (3) |

- • [EZ Toys Investment Opportunity](#) - distribute licensed products! EZ Toyz presents an exciting investment opportunity for the entrepreneur who insists on earning at least \$100K per year!
- [Virtual Technologies](#) - offers business plan for starting a company with little money down.
- [SurfPay](#) - get paid to surf the Net!
- [101 Jobs You Can Do at Home](#) - Opportunities for 'at home' employment. Additional income without 'traditional' outside work. Hundreds of jobs you can do at home, no experience required.
- [21st Century Marketing Systems, Inc](#) - own a marketing consulting practice.
- [3 Goddesses Gourmet Tea](#) - Seeking national and international distributors for its gourmet Indian Nilgiri tea offers excellent product, attractive packaging and easy financial arrangements
- [A&M Wholesale Distributors](#) - hot business links for the entrepreneur.
- [A+ Learning Success Institute](#) - innovative learning strategies and business opportunity.
- [ABC Marketing Group](#)
- [About Business in Australia](#) - Australian stock exchange information, Australian employment opportunities, products and services available via the internet.
- [Abuse the IRS Right Back!](#)
- [Abyss Scuba Center](#) - dive shop for sale including inventory.
- [Access to Home Based Business](#) - ten unusual home computer business opportunities including medical billing, paralegal, financial broker, scholarships, advertising, scor, small business services and travel agency.
- [Access to Success](#) - providing access to information that will aid in furthering your success.
- [Action Computer](#) - distributor of computer components.
- [AdMaxNets](#) - unique software which allows you to write an ad for you business opportunity.
- [Advantage Financial Services](#)
- [Agents Needed for U.S. Mortgage](#)
- [Agnm.Com](#) - credit card, mortgage reduction, and many business opportunities.

United States Senate
Permanent Subcommittee on Investigations
Committee on Governmental Affairs
February 10, 1998

Tatiana Gau
Integrity Assurance
America Online, Inc.

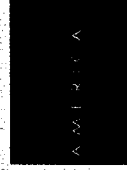
Senate Permanent Subcommitt
on Investigations

EXHIBIT #

A M I R A

Password Scams

- **Password Solicitation:**
 - Password Phishing via Instant Message
 - Password Phishing via Email
- **Concealed Password Solicitation:**
 - Diag.dat Password Phishing
 - Trojan Horses



Password Phishing via IM

Windows-style window titled "Password 'Phishing'" with a globe icon and standard window controls.

ScreenName: Dear User, Due to a complicated problem in our program we have lost contact with your account information. The problem occurred earlier today when one of employees released a virus onto one of our main system. Please respond back with your password in order to keep your account from termination.

ScreenName: Greetings CyberSurfer! I Am A Representative For the Online Banking System on AOL. As You May Have Read Credit Card Fraud is Huge on the 'Net'. Would You Like To Safe Guard Your Credit Card Info With AOL? Just Reply With Your Credit Card Number And Full Information So That We may Logg Your Card Into Our Computers So Noone Else But You May Access It Online! We Are Offering This Safety Measure At No-Cost to You At All!



Password Solicitation via Email

Password Info

Subj: Password Info
Date: 8/6/97 3:20:04 PM Eastern Daylight Time
From: JohnDoe
To: BetHeRiB
Sent on: AOL 4.0 for Windows 95 sub 56

Dear Member:

When you upgraded to unlimited usage earlier this year, we failed to update your records with the appropriate Screen Name information.

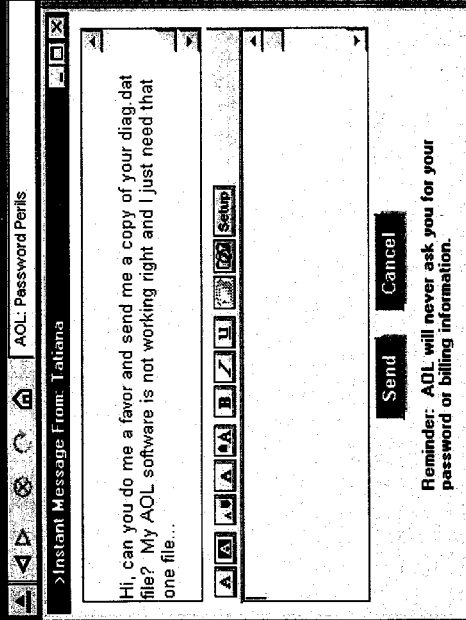
Please hit the "Reply" button and send us your Screen Name and Password as soon as possible.

Reply Forward Reply All Add Address Help

269 of 270 Prev Next Delete



Diag.dat Phishing via IM



Trojan Horses

AOL Computer Protection Center



Computer Protection Center



Fact: Attached files can contain viruses! *If you don't know who sent the e-mail, don't download the attached file!* Attached files may also contain Trojan Horse programs that may compromise the security of your AOL account, contain objectionable graphics, or damage computer files. No matter how enticing the file may appear, you put yourself and your computer at risk when you download a file from an unknown source, even if it appears to be an official AOL communication. **If you receive any suspicious files, forward them immediately to screen name TOSFiles.**



What are computer viruses and Trojan Horse programs?

Get the latest Dr. Solomon's virus protection tools today!

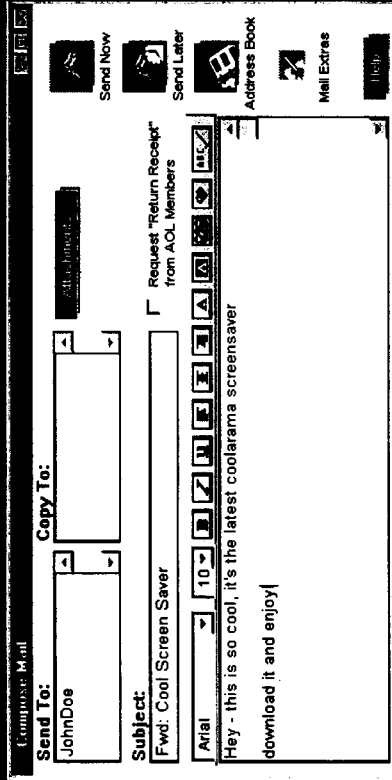
Essential Virus Protection Tips. Protect your computer today.

Think you've been infected? Don't panic! We're here to help!

Keyword: Virus Info



Trojans - Screen Saver



Trojan - Software Update

The screenshot shows the AOL Compose Mail interface. The window title is "Compose Mail". The "Send To:" field contains "SUZ12@we". The "Copy To:" field is empty. The "Subject:" field contains "Fwd: Software Upgrade v2.0". The "Request 'Return Receipt' from AOL Members" checkbox is unchecked. The font is set to "Arial" and the size is "10". The message content is as follows:

Forwarded Message:
Subj: Software Upgrade v2.0
Attached is the latest upgrade to your software by Ventronics. Please download and install promptly.

At the bottom of the window, there are several icons: "Send Now", "Send Later", "Address Book", "Mail Extras", and "Help".



Other Password Vulnerabilities

- **Web Sites**
 - Login Required
 - Scam For Personal Information
- **Password Guessing**
- **Password Cracking**

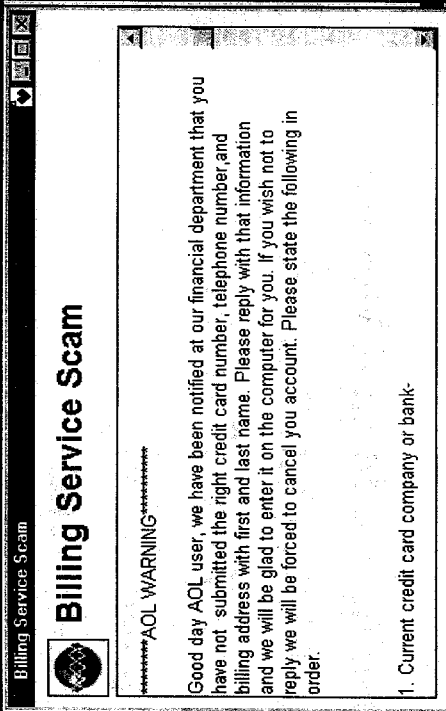


Credit Card & Billing Scams

- **CC Phishing via Instant Message**
- **“Update Billing Info” Email**
- **“You Have Won...” via Email**
- **Subscription Fraud**
- **Transaction Fraud**



Billing Scam via Email



Billing Scam - Email/Web

Important AOL Information! Please Read: :)

Date: 8/5/97 3:22:43 PM Eastern Daylight Time
From: BillyVgh
To: Kollinc23
Sent on: AOL 4.0 for Windows 95 sub 56

Special News Bulletin:

As you know, the number one priority for all of us at America Online continues to be meeting our obligation to provide you with the best possible service.

Let me update you on what we're doing to meet our commitments to you, including the development of a new server which offers a higher system capacity.

Just complete the required update of your information by [Clicking Here to continue.](#)

Reply Forward Reply All Add Address Help

Delete Prev 270 of 270



Subscription Fraud

Billing Information

By providing the following account information, I hereby authorize America Online to debit my account for any charges I incur in excess of my free trial period hours. Enter your information for VISA

Card Number: 0123-4567-9001-2345 Expiration Date: 08-99
Bank Name: First Virginia Bank

Card Number:

Expir. Date:

Bank Name:

Enter the name exactly as it appears on the credit card:

First Name:

Last Name:

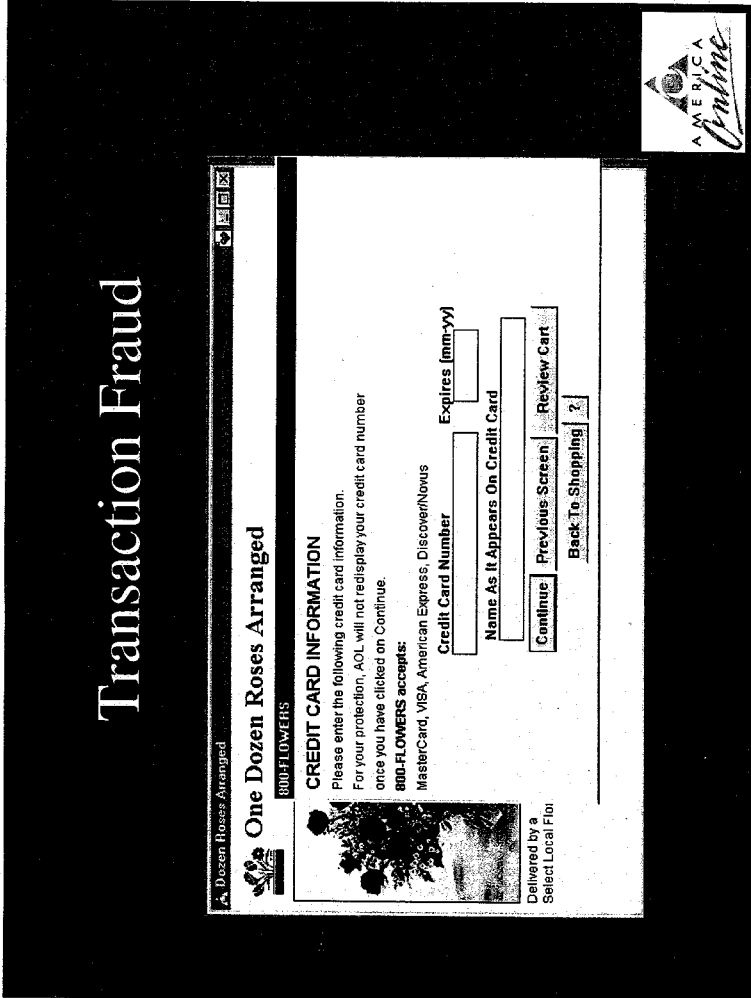
Please select:
 Credit Card
 Debit Card

Exit Other Billing Methods Next

- Credit Card Number
 - Mod10 Check
 - Prefix Crosscheck
- CC Type Check
- Valid Expiration
- Electronic Signature



Transaction Fraud



Other Web Frauds

- Fake Store Fronts
- Virulent Active Content
- Trojan Horses
- Impersonation/Hoax Sites



Spam

- **Fraud in Content**
 - Marketing Spam
 - Get-Rich-Quick Spam
- **Technological Fraud**
 - Forged Header Spam



Marketing Scam



Subj: The Break Through!
Date: 97-08-07 03:54:43 EDT
From: 10700856@ldd.net
To: members@aol.com

Now we know why it is harder for some than others
You have nothing to lose, but that unwanted weight.

A Phenomenal Break through in healthy weight control
Click on line below:
EatGoals




If you are having trouble loading the website through AOL
Please be patient it will be worth your wait.
Or you can try another browser just cut and paste
to location, this line <http://ogdent1.com>

----- Headers -----
From: mar440067@acme.actwin.com, Fri, Jun 13 08:51:48 1997
Return-Path: <mar@acme.actwin.com>
Received: from acme700062.actwin.com (acme.actwin.com [204.96.36.78])
by emi689623.mail.amt.com (8.8.5/8.5/AMT-4.0.0
with ESMTP) id IAAJ1071 for <yob6778097@amt.com>
Fri, 13 Jun 1997 08:51:47 -0400 (EDT)



Get-Rich-Quick Scam

**** Secret Password ****



 Reply
 Forward
 Reply to All

Subj: ** Secret Password **
Date: 97-08-07 16:14:51 EDT
From: Fun4u@aol.com
Reply-to: jdclark@juno.com
To: freind12321@aol.com

Dear Friend,




**** Print This Now For Future Reference ****

HOW TO MAKE \$800,000.00 CASH IN FOUR WEEKS!
 Ok, maybe not that much, but still easy money.
 Ask yourself...How much can I possibly lose here??? Then ask yourself...
 How much can I make??? The answers should tell you it's worth a try.
 All you can lose is 5 bucks (SO WHAT!!!) Yet you may make a nice profit.





Forged Headers

Headers
 From: Fun4u@aol.com Thu Aug 7 14:47:49 1997
 Return-Path: <Fun4u@aol.com>
 Received: from denmark.it.earthlink.net (denmark-c.it.earthlink.net [204.119.177.221])
 by emin60.mail.aol.com (8.8.5/8.5/AOL-4.0.0)
 with ESMTP id OAA06621;
 Thu, 7 Aug 1997 14:47:44 -0400 (EDT)
 Received: from mail.earthlink.net (1.Cust214.tn6.dn6.da.uu.net [165.36.201.214])
 by denmark.it.earthlink.net (8.8.5/8.5) with SMTP id LAA05977;
 Thu, 7 Aug 1997 11:47:12 -0700 (PDT)
 From: Fun4u@aol.com
 Received: from mailhost.aol.com (alt1.aol.com [208.9.77.65]) by aol.com (8.8.5/8.5) with
 SMTP id GAA07848 for <friend12321@aol.com>; Thu, 07 Aug 1997 13:18:53 -0600 (EST)
 To: friend12321@aol.com
 Message-ID: <199702170025.GAA08066@aol.com>
 Date: Thu, 07 Aug 97 13:18:53 EST
 Subject: ** Secret Password **
 Reply-To: jdclark@juno.com
 X-PMFLAGS: 34078648 0
 X-JIDL: 2610431056a78aeb1b28ida426c9e5a
 Comments: Authenticated sender is <friend12321@aol.com>

Secret Password



AOL Tools

- **Mail Controls**
- **Download Sentry**
- **AOL Neighborhood Watch**
- **Notify AOL**
- **Parental Controls**

Mail Controls



Mail Controls:

Mail Controls
Use Mail Controls below to decide who can exchange mail with

Choose a setting:

- Allow all mail
- Allow mail from AOL Members and addresses listed
- Allow mail from AOL Members only
- Allow mail from the addresses listed only
- Block mail from the addresses listed
- Block all mail

Result: You will not be able to send or receive mail.

Attachments:

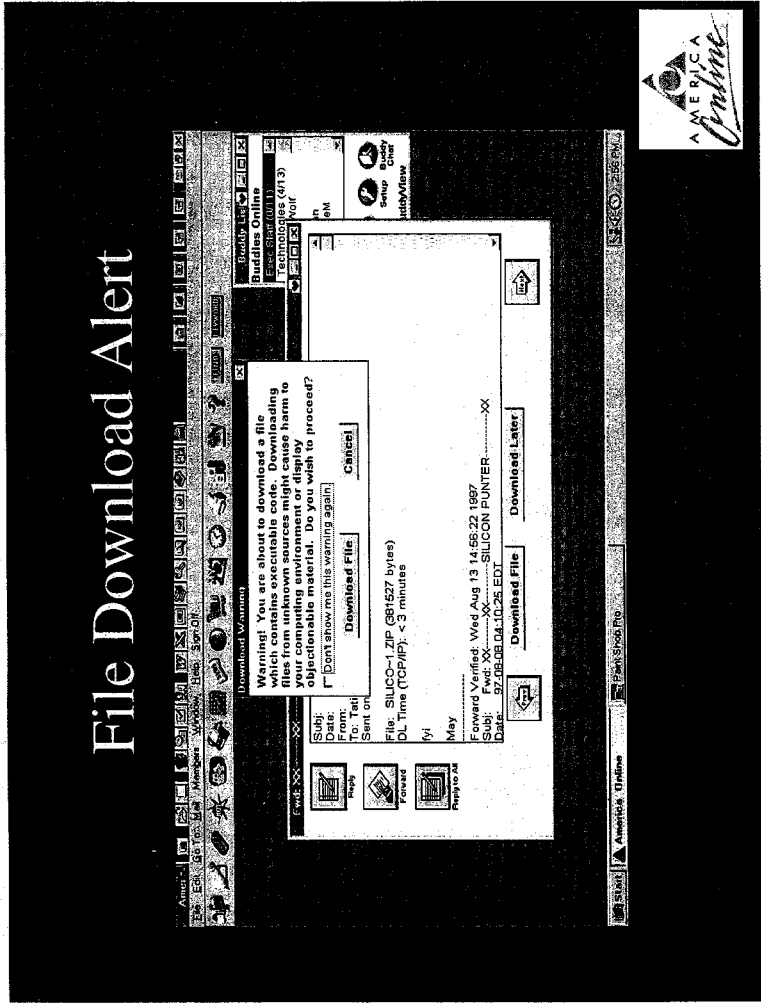
- Block file attachments and pictures in mail (You cannot send or receive files in mail)

OK Cancel

Type mail address here: Add

Remove Remove All

File Download Alert



Neighborhood Watch

AOL Neighborhood Watch

AOL Neighborhood Watch

Keeping the AOL Community safe

AOL Neighborhood Watch gives you the tools and tips you need to ensure a safe and fun online experience for you and your family. Here are some ways AOL's Neighborhood Watch can help you customize AOL to fit your needs:

* Set **Parental Controls** for your children. Parental Controls help parents make sure their children have a fun and enriching experience online, while limiting access to



PARENTAL CONTROLS:
Take charge of your kids' online experience.



E-MAIL SAFETY: Find out what you can do about junk mail and more.



COMPUTER VIRUSES:
Protect your computer against damaging viruses.

Notify AOL

Shopping & Banking

Suggested Safeguards

Keyword: Neighborhood Watch



Notify AOL

Keyword: Notify AOL

AOL Notify AOL

Type of Violation

- Chat
- E-mail & Attachments
- Instant Message™ Notes
- Message Boards
- Web Pages
- Screen Names & Profiles

● How to Copy & Paste
 ● Ask the Staff
 ● Member Services
 ● About Notify AOL

If you witness any inappropriate activity on AOL, please report it here at Notify AOL.

- * Click on **Chat** to report vulgar language and disruptive behavior in chat rooms.
- * Click **E-mail & Attachments** to report e-mail from strangers that contains attached files or requests for your password, credit card number, or other personal information.
- * Click **Instant Message™ Notes** if you receive requests for your password or observe disruptive

Keyword: Notify AOL



Spam Tools

Junk Mail | MAIL CENTER | FIND | Keyword: Junk Mail

Junk Mail: What you can do about it.

A Community Update from Steve Case

Dear Members:

I'd like to welcome you to AOL's updated member information area, "Junk Mail," designed to provide you with all the information you need to know about unsolicited or junk e-mail. Through this area, we'll answer your questions about junk e-mail, and provide information about the tools we make available, as well as the steps you can take, to fight unsolicited e-mail. We will also use this area to keep you updated on the steps we're taking to combat this Internet-wide problem.

AOL's latest legal efforts against junk e-mail.

Take control of your mail with Mail Controls.

Need help? Meg helps you combat junk mail.

AMERICA Online

Parental Controls

Parental Controls

Parental Controls - Putting Parents in Control

Since children of all ages use AOL, we've created easy-to-use features to help parents make sure their children have a fun and enriching experience online, while limiting access to some features of AOL and the Internet. These Parental Controls allow parents to designate different levels of access for each child.

Parents of children ages 12 and under, for example, should assign the **KIDS ONLY** category to their children's accounts. This restricts young children to the Kids Only channel. A Kids Only account cannot send or receive Instant Messages (private real-time communications), cannot enter member-created chat rooms, cannot use premium services, and can only send and receive text-only

[Set Parental Controls Now](#)

Online Safety for Kids

Learn how to keep your kids' online experience fun, educational and safe and visit the Kids Only Channel.

Premium Services

Limit your kids' access to services and games for which a special fee is charged.

Create a New Screen Name

The first step to child safety online - give your children their own screen names.

Fine-tune with Custom Controls



Safety Tips

- **1) Choose a safe password, e.g., six alpha numeric characters**
- **2) Do not give out your password or billing information to anyone**
- **3) Do not give out personal information such as home address, tel. number or SSN**
- **4) Do not download files from strangers**
- **5) If a Web site is unfamiliar, look into the company's background before you do business with them**
- **6) Don't believe everything you read; if it sounds too good to be true, it probably is**



**90 DAY, NO QUESTIONS ASKED, MONEY BACK
GUARANTEE!!**

FORTUNA ALLIANCE®

**A World-Wide Cooperative Profit-Sharing Association
Designed for people with NO TIME AND NO MONEY
for traditional Business Opportunities**

What if you could simply hire a Marketing Expert to help you be successful in your own business, to handle all the headaches and just make you money?

What if you paid this Marketing Expert \$250 a month which produced a minimum of \$5,250 income each month for you, While you simply watched?

Would you want to continue this arrangement while you kept earning \$5000 a month profit?

Well that's exactly what would happen if you hired Fortuna Alliance as you personal Marketing Expert!

Fortuna Alliance systematically builds your business for you. We've eliminated all the negatives!

- No recruiting necessary.
- No investment in inventory.
- No product selling or collections.
- No phone work or mailouts.
- No monthly paper work.
- No costly advertising.
- No personal shipping or delivering.
- No product return handling.
- No sales tax (in most cases).
- No baby-sitting customers or reps.
- No minimum volume requirement.
- No forced break-aways.
- No need to balance "legs".
- No runaway leg.
- No giving away recruits to upline.
- No cross-lining.
- No people retention problems.

144	12	11	
89	11	13	
55	10	12	
34	9	11	
21	8	10	
13	7	9	
8	6	8	
5	5	7	
3	4	6	
2	3	5	
1	2	3	
1	1	2	

- NO HEADACHES!

The absolute highest residual income in the industry is locked in through our unique mathematical formula: The Fibonacci Sequence!

The most powerful marketing concept to come along in many years! Fortuna Alliance generates more than 30 times the income of any other program, with 1/10th the number of people.

If you are not completely satisfied with your earnings at the end of 90 days, you keep your earnings AND get your money back ... No Questions Asked!

Where else could you start your own business for only \$250 with No Headaches and that kind of guarantee?

Multiple Income Centers available for unlimited income potential.

Shop and buy through the Internet.

Available countries:

Fortuna Alliance is free association of individuals. Any country that follows the path of free enterprise and allows free association of its individual citizens should be open for individuals to join.

To Learn More About FORTUNA ALLIANCE...

- Call 800-766-4810 24 hr. msg. (outside US...)
- Fax on Demand: (512) 703-6188
- Call 800-610-1958, x3056 (outside U.S. 612-707-0570)
- <http://www.pacificrim.net/~fortuna>
- E-mail: fortuna@pacificrim.net
- Your Sponsor: Williams Enterprises 502-456-5345
- Visit the products page at <http://shoppers.com/fortuna/>



Go To Select your destination: ▼

FOR RELEASE: FEBRUARY 24, 1997

**INTERNET PYRAMID OPERATORS, FORTUNA ALLIANCE,
COULD RETURN OVER \$5 MILLION TO CONSUMERS**

Consumers who lost money investing in an illegal pyramid scheme on the Internet will recover their funds, under a settlement obtained by the Federal Trade Commission and the scheme's promoters, and Fortuna Alliance. Under the settlement, every Fortuna member is entitled to receive a refund in full for their membership fees.

In the complaint detailing the charges, the FTC charged that Fortuna Alliance, L.L.C., and four officers, marketed the pyramid scheme through a home page on the World Wide Web and with printed promotional materials. Using fabulous earnings claims, they induced tens of thousands of consumers in over 60 countries around the world to pay between \$250 and \$1750 to join their pyramid scheme, claiming that members would receive over \$5000 per month in "profits" as others were induced to "enroll." In addition, Fortuna and its officers provided advice and promotional materials for members to recruit others to join the pyramid, both through direct contact and by setting up their own web sites. The FTC's complaint asked the court to order a permanent halt to the alleged deceptive practices and to order redress for the people Fortuna signed up to the scheme.

The redress program will offer consumers who invested in the scheme, including foreign nationals, full refunds for membership fees they paid. The money will come from a fund initially using money frozen in the U.S. and \$2.8 million transferred from Antigua, W.I. If this is insufficient to meet refund requests, defendants will pay additional money to ensure full refunds for all who seek them. Consumers who received refunds from the \$2 million already distributed will not receive further payments. The FTC expects refund notices to be sent out by the end of March.

"Our expert calculated that over 95% of the people who invested in Fortuna would have lost money if we had not shut this pyramid down," said Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection. "Under this settlement, any investor who lost funds will be able to recover them. But big losses are the bottom line in all pyramid schemes. We closed down Fortuna's web site quickly and the settlement will provide consumer redress in this case. But we hope that all consumers get the message: pyramid schemes are illegal and in the end they all fail."

Under the agreement to settle the FTC charges, Fortuna will set aside \$2.8 million to fund a consumer redress program. Earlier, a federal district court directed the return of \$2 million and an additional \$350,000 remains frozen in U.S. banks. When the FTC's case

against the firm was filed last May, a federal district court issued a temporary restraining order and froze the company's assets pending trial. At the same time, the FTC, with the assistance of the U.S. Department of Justice's Office of Foreign Litigation, also obtained a court order in Antigua, freezing Fortuna funds that had been transferred to an offshore bank there. As part of its case, the FTC sought a permanent injunction against the pyramid scheme, repatriation of funds transferred offshore, and redress for consumers.

To settle the FTC charges, Fortuna Alliance and its principals also will be barred from "engaging, participating, or assisting in any manner or capacity . . . the advertising, promoting, offering for sale, or sale, of any chain or pyramid marketing program. . . ." In addition, the defendants will be barred from making deceptive earnings claims in conjunction with any marketing or investment program they offer. Bookkeeping and monitoring provisions are included to allow the FTC to track compliance with the terms of the settlement.

The Commission vote to accept the proposed consent judgment was 5-0. The FTC's Seattle Regional Office handled the case, with invaluable early assistance from the Washington State Division of Financial Institutions' Securities Division; the Bellingham, WA police dept.; the Nevada and Washington State Attorneys' General offices; and the Florida Comptroller's Office, Department of Banking and Finance's Division. of Financial Investigations. The FTC used counsel in London, Belize, and Antigua for the foreign litigation. The Department of Justice, Office of Foreign Litigation was instrumental in reaching settlement of the foreign actions.

NOTE: This consent judgement is for settlement purposes only and does not constitute an admission by the defendant of a law violation. Consent judgments have the force of law when signed by the judge.

Overview Fortuna Alliance

Background for Existing Members of Fortuna Alliance While this document is not intended to be exhaustive on the subject, it is intended to present enough information for a prior member of Fortuna Alliance to choose one of the three options now available to them *prior* to the start-up of the new Fortuna Alliance II.

Fortuna Alliance is the company, policies and format which existed world-wide prior to May 29, 1996, when Fortuna Alliance offices in the United States were "raided" by *armed* members of a U.S. regulatory and enforcement agency known as the "Federal Trade Commission" (FTC).

Fortuna Alliance was forced into "receivership" by order of Federal Judge McGovern, at the request of the FTC. All assets were seized; offices, phones, computers, software, business records, and cash. All bank accounts in the U.S. and Antigua were frozen.

Defendants were deprived of all existing funds to defend themselves by the Judge through the application of laws intended for *convicted* criminals and the like. Fortuna Alliance was forced to stop doing business and the court appointed "Receiver" began a systematic dismantling of the company including spending membership money at a rate of approximately USD\$3,000 per day.

According to U.S. Government documents, the FTC traditionally returns only 3.6% of the money it seizes to its original owners in the name of "protecting U.S. Citizens".

After a lengthy battle, which included a 300 million counter-suit, Fortuna Alliance secured a major victory on behalf of its members. Judge McGovern instructed the Receiver to return all application fees not yet processed by Fortuna, or that were received after the "raid", to the rightful owners. Fortuna Alliance has not yet been allowed to speak; Judge McGovern denied our request for an evidentiary hearing.

Founder Augie Delgado and many of Fortuna Alliance's world-wide staff have continued working to defend Fortuna and reorganize it into an organization with improved programs for the membership and built in protection from any country's arbitrary abuse of power over its citizens. Especially from the jurisdiction of U.S. agencies which are striving to curtail the increasing participation in "off-shore" activities by U.S. Citizens *and* who also wish to gain jurisdiction over the "Internet", thereby adding to their current control of information available to U.S. Citizens. *To emphasis this point:* Last year, 33 Trillion Dollars were held offshore by financial centers world-wide.

As a result of this 8 month "Baptism of Fire" there has been severe devaluation of the member income centers as well as devastating losses to Fortuna Alliance itself. *The vision* has survived and is going forward, as Fortuna Alliance II. Please Note, existing Fortuna Alliance members are *automatically* members in Fortuna Alliance II.

OVERVIEW OF FORTUNA ALLIANCE II (TM)

The new Fortuna Alliance II will be similar to the "original" Fortuna Alliance in most ways. It was very good as it was and the primary reasons to change any part of it are:

1. to protect it from interference by governmental agencies of any country and,

2. to take advantage of all that the founder, Augie Delgado, and the Executive Team have learned from this most devastating experience at the hands of a brutal U.S. regulatory agency, the Federal Trade Commission.

A primary and fundamental change from the structure of the other company will be a fourth category of membership called the "Basic Membership". This category of membership will now be the first level of membership and a prerequisite to the Elite Membership level. This prerequisite will not apply to existing Elite members. It will carry with it the privilege of shopping at our on-line *virtual mall* using the Internet, as will all higher categories of membership.

Prior to completion of the Fortuna mall, the members will be able to "shop" from our new portfolio (catalogue) with its new and exciting products and services. A few of the new products/services will be worth joining Fortuna Alliance II on their merit alone.

In addition to our current international portfolio of over 275,000 products and many *unique* services, we are continuing to add providers specifically within each local region.

Another change in the new Fortuna Alliance II will be the restructuring of the company's popular charitable contribution program from 15% to 10% of *gross* revenues. The 5% change will be reapplied to set up and maintain Regional Offices and Member Service Centers (MAGNETS) in various countries as well as support ongoing legal defense and an assertive public relations campaign.

From your monthly membership fees paid to Fortuna of the gross, 10% is used for donations to Non-profit organisations, with the remainder going to Fortuna Alliance as a Consultancy Fee. It is the intention that any profit remaining after running expenses and promotion of members co-ops and from investment returns will be paid out by the Company to the members as company shared profits according to the Fibonacci Sequence, on a first come first service basis. At first, there will be three Regional Offices: Canada for North America, Holland for Europe and New Zealand for Australasia.

This will better support the opportunity to have more regional providers in the local area, and provide members telephone access to "the company" where the local language is spoken and business is not hindered by time zone differences.

The number and size of these Regional Offices will grow based on the needs of our expanding world-wide membership base.

One of the most important changes in Fortuna Alliance II will be that the company will maintain its operations *off-shore* from each and every country where it will do business.

This means that a "raid" by a governmental agency which put Fortuna Alliance out of business without a warning or a trial to prove guilt of any kind, will never happen again.

Few of the new changes will be more financially rewarding to the new members of Fortuna Alliance II than the innovative concept that every Basic or Elite Member may now own profit-sharing certificates in the new company.

This will bring profit-sharing to a whole new level - the "Holding Company" level. This international holding company will control various subsidiaries offering members Off-Shore Banking, Insurance, IBC's, Trusts, Debit/Credit cards, Travel, Resort Ownership, Asset Management/Protection, Real Estate, Financial Planning and

Investments.

Will members of the previous company, Fortuna Alliance, be left out of these innovative and exciting changes?

No, definitely not! A brief description of the opportunities available to members of the original company will be presented following the Basic Membership information.

Basic Membership

Prospective members pay US\$250 for:

- The privilege of belonging to the F.A. II Co-Op for one year,
- The right to purchase portfolio items,
- The opportunity to receive a 30% profit-share on *personal* purchases,
- The opportunity to purchase Profit Sharing Certificates in the amount of USD\$100 each, with a guaranteed 20% minimum return the first year.

Basic Members will be sponsored by a current F.A. II member.

Basic Memberships are not commissionable.

Basic Members participate in 30% profit-sharing from their personal purchases only.

Basic Members will be placed in the 376 member Fibonacci Tree of their Sponsor if and when they upgrade to Elite Membership.

Basic Members must pay an annual renewal fee of \$199 to remain members in good standing *only* if he/she has not chosen to upgrade to Elite Membership status during the year.

Basic Membership is not refundable after the initial 14 day rescission period.

Basic Members are allowed to upgrade to profit-sharing Elite status at any time *after* 14 days and up to one year.

Basic Members who choose to upgrade to Elite Membership within 90 days of becoming a Basic Member, will have a portion of that fee *paid by Fortuna Alliance II* according to the following schedule:

If a Basic Member becomes an Elite Member within 30 days, Fortuna Alliance II will contribute \$175 to the purchase of the first "profit center".

If a Basic Member becomes an Elite Member after 30 days, but within 60 days, Fortuna Alliance II will contribute \$125 to the purchase of the first "profit center".

If a Basic Member becomes an Elite Member after 60 days, but within 90 days, Fortuna Alliance II will contribute \$75 to the purchase of the first "profit center".

Elite Membership

Each Elite Membership may be purchased for a *one-time* out-of-pocket amount of USD\$250.

At the Elite level of membership the Elite Member will be entitled to:

- Acquire one or more Elite level "profit centers",
- Distribution of Company shared profits according to the Fibonacci sequence determined by the placement of Elite Members in their co-op tree,
- *Full* profit-sharing from the purchases of others in his/her tree,
- The option to purchase an off-shore trust from his/her profit center earnings or advanced by Fortuna Alliance II against future earnings for a nominal service fee. All future profits earned may be paid directly into the Elite member's

- private trust,
- Opportunity, subject to availability, to purchase Profit-Sharing Certificates in the amount of USD\$100 each with a guaranteed 20% minimum return the first year,
- Indefinite money-back guarantee *after* 90 days, of the amount actually paid by member for Elite "profit centers" minus any income or benefit derived from them. Any refund request must be for all "profit centers" owned by the requesting member,
- Access to higher levels of membership such as Premier and Ambassador, which will be described in the new Fortuna Alliance II marketing materials.

The Options Available to Those Who Were Members Prior to May 29th are:

Option I

Elite Members of Fortuna Alliance prior to May 29, 1996, will have their family tree positions converted to similar positions in Fortuna Alliance II, providing they have not previously indicated an unwillingness to continue their membership. Also they may participate in the "ownership" of Fortuna Alliance II through the purchase of one or more "Profit-Sharing Certificates" for USD\$100 each. Of the three options, this is the *only* option which has an acceptance deadline attached to it. Option I will be available to prior Fortuna Alliance members only until the 250,000 certificates are gone. They are currently going fast!

Option II

Every Elite Member of the old Fortuna Alliance is offered the opportunity to convert his/her family tree positions to similar positions in Fortuna Alliance II and NOT participate in the "ownership" of Fortuna Alliance II. Option II requires the member to do nothing except be patient as the company goes through this re-inception phase and sends out the F.A. II program information. Any member choosing to accept this "default" option, does not give up his/her right to choose Option III at any time in the future. Although Fortuna Alliance is currently unable to pay-out the "profit center" earnings due to the FTC action, the computer records which were prepared for submission to the court show that many prior members had earned several thousand dollars in consecutive months from a single profit center.

Option III

Every Elite Member of Fortuna Alliance prior to May 29, 1996, may receive a refund of his/her original Elite Membership fees, minus any cash advance or funds distribution already received. This will require filling out a form which will soon be mailed to you by a third party assigned in part by the FTC. While there will be a closing date for the FTC offer, there will be no closing date for acceptance of refund requests by Fortuna Alliance II. This option will be honored by Fortuna Alliance II indefinitely, as it always has, after it is able to resume business. In fact, due to the predicted success of Fortuna Alliance II, if this option is not exercised prematurely, few if any members will want to exercise this option *at all* due to the already achieved and *possible* earnings per profit center through Fortuna's profit-sharing concepts. For the benefit of existing members, any available refunded centers from these "early positions" will be made available for purchase on a "net worth" basis consistent with their demand value in the *Fibonacci* system. This will be on a lottery basis for fairness.

FOR RELEASE: May 29, 1996

FTC HALTS INTERNET PYRAMID SCHEME

In its 12th and largest law enforcement action against fraud on the Internet, the Federal Trade Commission has obtained a federal court order temporarily halting a pyramid scheme advertised on the Internet. The FTC estimates that the scheme has already taken in over \$6 million. The court's temporary restraining order freezes the defendants' assets and appoints a receiver to manage the company, called Fortuna Alliance. The FTC has asked the court to issue a permanent injunction that will provide redress for the consumers who were victims of the scam.

"This brand new, high-tech scam is as old as Methuselah," said Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection. "Behind all the techno-jargon and the mathematical mumbo jumbo, this is just an elaborate, electronic version of a chain letter. People are told that if they sign up and send money, they'll eventually end up at the top of the pyramid, collecting from those at the bottom. But most people never make it to the top. Early entrants may make some money, but eventually, the pyramids collapse and most of the "members" are left holding the bag," she said.

The FTC has charged that Fortuna Alliance, L.L.C., and five officers marketed the pyramid scheme through a home page on the World Wide Web. Using claims such as "*What if you paid...\$250 a month which produced a minimum of \$5,250 income each month for you, While you simply watched?*", and "*Would you want to continue this arrangement while you kept earning \$5,000 a month,*" they induced thousands of consumers to pay between \$250 and \$1750 to join their pyramid scheme by claiming that members would receive over \$5000 per month in "profits" as others were induced to "enroll." In addition, Fortuna and its officers provided advice and promotional materials for members to set up their own web sites to recruit others to join the pyramid.

According to the complaint detailing the charges, most participants in a pyramid scheme lose money, so the claims that consumers who pay Fortuna \$250 will receive high income or profits of over \$5,000 per month are false and misleading. In addition, providing others with promotional material that contains similar false claims for use in recruiting new participants, is deceptive or unfair, in violation of the law. The FTC's complaint asks the court to order a permanent halt to the alleged deceptive practices and to order redress for the people they signed-up to the scheme.

In papers filed with the court, the FTC contends that Fortuna has already taken over \$6 million from consumers, and transferred at least \$3.55 million of that money to a bank in Antigua, W.I. The temporary restraining order directs defendants immediately to see that the money is returned to the United States.

The Commission vote to authorize the staff to file the complaint was 5-0. The complaint was filed in the U.S. District Court for the Western District of Washington, at Seattle, on May 23 under seal. The seal was lifted on May 28. The court has ordered a hearing on May 30 at 9:30 a.m. to consider the FTC's request for a preliminary injunction continuing the temporary relief until the case is completed.

The FTC's Seattle Regional Office handled the investigation, with invaluable assistance from the Washington State Div. of Financial Institutions' Securities Division; the Bellingham, WA police dept.; the Washington State Attorney's General office; and the Florida Comptroller's Office, Dept. of Banking and Finance's Div. of Financial Investigations.

NOTE: The Commission authorizes the filing of a complaint when it has "reason to believe" that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. The complaint is not a finding or ruling that the defendant actually has violated the law. The case will be decided by the court.

Copies of the complaint are available from the FTC's Public Reference Branch, Room 130, 6th Street and Pennsylvania Avenue, N.W., Washington, D.C. 20580; 202-326-2222; TTY for the hearing impaired 202-326-2502. The complaint, and additional information about the proceeding, are also available at a special Internet site at <http://www.ftc.gov/ro/fortuna.htm>. To find out the latest news as it is announced, call the FTC NewsPhone recording at 202-326-2710. FTC news releases and other materials also are available on the Internet at the FTC's World Wide Web site at: <http://www.ftc.gov>

MEDIA CONTACT: Claudia Bourne Farrell, *Office of Public Affairs*, 202-326-2181

STAFF CONTACT: Charles A. Harwood or Randall H. Brook, *Seattle Regional Office*, 206-220-6358

(Fortuna)
(FTC File No. 962-3158)

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

FEDERAL TRADE COMMISSION, Plaintiff,
v.
FORTUNA ALLIANCE, L.L.C., AUGUSTINE DELGADO,
LIBBY GUSTINE WELCH, DONALD R. GRANT, MONIQUE
DELGADO, and GAIL OLIVER, Defendants.

Civ. No.

COMPLAINT

Plaintiff, the Federal Trade Commission ("Commission"), for its complaint alleges as follows:

1. The Commission brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain permanent injunctive relief, restitution, disgorgement, and other equitable relief for defendants' unfair and deceptive trade practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

JURISDICTION AND VENUE

2. Subject matter jurisdiction is conferred upon this Court by 15 U.S.C. §§ 45(a) and 53(b), and 28 U.S.C. §§ 1331, 1337(a), and 1345.

3. Venue in the Western District of Washington is proper under 28 U.S.C. § 1391(b) and (c), and 15 U.S.C. § 53(b).

THE PARTIES

4. Plaintiff, the Federal Trade Commission, is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The Commission enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The Commission may initiate federal district court proceedings to enjoin violations of the FTC Act and to secure appropriate equitable relief in each case, including restitution and disgorgement. 15 U.S.C. § 53(b).

5. Defendant Fortuna Alliance, L.L.C. ("Fortuna"), is a Nevada limited liability company with its office and principal place of business at 609 A Northshore Drive, Bellingham, Washington 98226. Fortuna markets investments in a pyramid sales scheme throughout the United States and in foreign countries.

6. Defendant Augustine Delgado ("Delgado") founded and, directly or indirectly, owns Fortuna. Fortuna promotional materials call him "Augie" Delgado. Individually or in concert with others, Delgado formulates, directs, controls, or participates in the acts and practices of Fortuna alleged below, and has done so at all times pertinent to this action. He resides and transacts business in the Western District of Washington.

7. Defendant Libby Gustine Welch is a manager or agent of Fortuna. Individually or in concert with others, she formulates, directs, controls, or participates in the acts and practices of Fortuna alleged below, and has done so at all times pertinent to this action. She resides and transacts business in the

Western District of Washington.

8. Defendant Donald R. Grant is an officer or manager of Fortuna. Individually or in concert with others, he formulates, directs, controls, or participates in the acts and practices of Fortuna alleged below, and has done so at all times pertinent to this action. He resides and transacts business in the Western District of Washington.

9. Defendant Monique Delgado is a manager or agent of Fortuna. Individually or in concert with others, she formulates, directs, controls, or participates in the acts and practices of Fortuna alleged below, and has done so at all times pertinent to this action. She resides and transacts business in the Western District of Washington.

10. Defendant Gail Oliver is a manager or agent of Fortuna. Individually or in concert with others, she formulates, directs, controls, or participates in the acts and practices of Fortuna alleged below, and has done so at all times pertinent to this action. She resides and transacts business in the Western District of Washington.

COMMERCE

11. At all times relevant to this complaint, defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

COURSE OF CONDUCT

12. Since approximately November 1995, defendants have operated an investment program commonly known as a "pyramid scheme." Pyramid schemes are characterized by the payment of money to the scheme's promoter in return for which participants receive the right to recruit new participants. Participants then receive payments for each individual they recruit or who appears below them in their pyramid. Earnings in a pyramid scheme are derived primarily from recruiting other participants into the program, not from the sale of products or services.

13. Defendants advertise and market their pyramid scheme via the Internet, using electronic home pages on the World Wide Web. They also use telephones, faxes, and mail to distribute their promotional documents and audio and video tapes.

14. Defendants' promotional materials promise consumers that they will earn a profit of at least \$5,000 per month for a \$250 initial investment. For example, one document (Attachment A) states:

What if you paid . . . \$250 a month which produced a minimum of \$5,250 income each month for you, while you watched? . . .

Well that's exactly what would happen if you hired Fortuna Alliance as your personal Marketing Expert.

The promotional materials also explain that only the initial \$250 investment comes from the consumer, any further payments are deducted from "profits." The materials also encourage consumers to make multiple investments, up to \$1,750 per consumer.

15. Defendants' promotional materials attempt to distinguish their plan from other pyramids by suggesting that the high profits are attributable to a mathematical formula called the Fibonacci series. (See Attachment B.) In fact, the formula for distributing profits in any pyramid scheme has no effect on the end result that most participants lose money.

16. Defendants' have induced thousands of consumers throughout the United States and in foreign countries to pay Fortuna \$250 to \$1,750 to join their pyramid scheme. Defendants have also provided their promotional materials to others for use in recruiting new participants and inducing them to invest in the pyramid scheme.

17. Pyramid schemes are inherently injurious to consumers because they must eventually collapse. Like chain letters, pyramid schemes may make money for those at the top of the chain or pyramid, but end up injuring the vast majority of participants at the bottom who can find few or no recruits.

DEFENDANTS' VIOLATIONS OF THE FTC ACT

18. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits unfair or deceptive acts and practices in or affecting commerce.

COUNT ONE

19. In connection with the offering for sale or sale of investments in a pyramid scheme, defendants have represented, directly or by implication, orally and in writing (including electronic writing on the World Wide Web), that consumers who pay Fortuna \$250 will receive high income, or profits of over \$5,000 per month in return.

19. In truth and in fact, most consumers who pay Fortuna \$250 will not receive high income, or profits of over \$5,000 per month in return. Instead, most participants in the pyramid scheme will lose money.

20. Therefore, the representations set forth in ¶ 19 are false and misleading and constitute unfair or deceptive acts and practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT TWO

21. By providing participants in Fortuna with promotional materials both written and electronic, that contain false representations, including but not limited to the false representations described in ¶ 19 above, to be used in recruiting new participants, defendants have provided these people with the means and instrumentalities for the commission of unfair or deceptive acts and practices.

22. Defendants' practices, as described in ¶ 22, constitute unfair or deceptive acts and practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

INJURY

23. Defendants' violations of Section 5 of the FTC Act, as set forth above, have caused and continue to cause substantial injury to consumers. Absent injunctive relief by this Court, defendants are likely to continue to injure consumers.

THIS COURT'S POWER TO GRANT RELIEF

24. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to issue a permanent injunction against defendants' violations of the FTC Act and, in the exercise of its equitable jurisdiction, grant such other relief as the Court may deem appropriate to halt and redress violations of the FTC Act, including restitution and disgorgement of unjust enrichment.

PRAYER FOR RELIEF

WHEREFORE the Commission respectfully requests that this Court, as authorized by Section 13 of the FTC Act, 15 U.S.C. § 53(b), and pursuant to its own equitable powers:

(25) Award the Commission all temporary and preliminary injunctive and ancillary relief that may be necessary to avert the likelihood of consumer injury during the pendency of this action, and to preserve the possibility of effective final relief, including, but not limited to, temporary and preliminary injunctions, appointment of a receiver, and an order freezing each defendant's assets;

(26) Permanently enjoin defendants from violating the FTC Act as alleged in this complaint;

(27) Award all relief that the Court finds necessary to remedy the defendants' violations of Section 5(a) of the FTC Act, including, but not limited to, the refund of monies paid and the disgorgement of ill-gotten gains; and

(28) Award the Commission the costs of bringing this action, as well as any other equitable relief that the Court may determine to be proper and just.

Dated:

Respectfully submitted,

STEPHEN CALKINS
General Counsel

CHARLES A. HARWOOD
Regional Director

Randall H. Brook
Eleanor Durham
ATTORNEYS FOR PLAINTIFF
FEDERAL TRADE COMMISSION

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

FEDERAL TRADE COMMISSION, Plaintiff,

v.

**FORTUNA ALLIANCE, L.L.C., AUGUSTINE DELGADO, LIBBY GUSTINE
WELCH, DONALD R. GRANT, MONIQUE DELGADO, and GAIL OLIVER,
Defendants.**

Civ. No. C96-0799 D

**TEMPORARY RESTRAINING ORDER
FREEZING ASSETS AND PROVIDING OTHER EQUITABLE
RELIEF**

Plaintiff, the Federal Trade Commission ("Commission"), having filed a complaint for a permanent injunction and other relief, including restitution to consumers, pursuant to Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), and having moved for an *ex parte* temporary restraining order and for an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, and the Court having considered the pleadings, declarations, exhibits, and memorandum filed in support thereof, it is the finding of this Court that:

1. This Court has jurisdiction of the subject matter of this case and there is good cause to believe it will have jurisdiction over all parties hereto.
2. There is good cause to believe the Commission will ultimately succeed in establishing that defendants Fortuna Alliance, L.L.C., Augustine Delgado, Libby Gustine Welch, Donald R. Grant, Monique Delgado, and Gail Oliver, and each of them, have engaged in and are likely to engage in acts and practices that violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).
3. There is good cause to believe that immediate and irreparable damage will be done to the public and to this Court's ability to grant full and effective relief among the parties hereto absent entry of this Order on an *ex parte* basis.
4. Weighing the equities and considering the Commission's likelihood of ultimate success, a Temporary Restraining Order is in the public interest.

I. - CEASE AND DESIST

IT IS THEREFORE ORDERED that defendants are hereby temporarily restrained and enjoined from:

A. Promoting, offering for sale, or selling any memberships or participation rights in Fortuna Alliance or any other pyramid scheme.

B. Providing promotional materials or services to any person or entity who promotes, offers for sale, or sells memberships or participation rights in Fortuna Alliance or any other pyramid scheme.

C. Making, or assisting in the making of, directly or by implication, orally or in writing, any statement or representation of material fact that is false or misleading about the profits or earnings that may be expected by any participant in any investment program or plan.

II. - ASSET FREEZE

IT IS FURTHER ORDERED that, except as provided in Section IV below, as stipulated by the parties, or as directed by further order of the Court, defendants Fortuna Alliance, L.L.C. ("Fortuna"), Augustine Delgado, and Libby Gustine Welch are hereby temporarily restrained and enjoined from, directly or through any other person or entity:

- A. Transferring, converting, encumbering, selling, concealing, dissipating, disbursing, assigning, spending, withdrawing, or otherwise disposing of any funds, real or personal property, accounts, contracts, membership or mailing (including "Email") lists, shares of stock or other assets, or any interest therein, wherever located, that are (a) owned or controlled by any of these defendants, in whole or in part; or (b) in the actual or constructive possession of any of these defendants; or (c) owned, controlled by, or in the actual constructive possession of any corporation, partnership, or other entity directly or indirectly owned, managed, or controlled by, or under common control with, any of these defendants, including, but not limited to, any assets held by or for any of these defendants at any bank or savings and loan institution, or with any broker-dealer, escrow agent, title company, commodity trading company, precious metal dealer, or other financial institution or depository of any kind;
- B. Opening or causing to be opened any safe deposit boxes titled in the name of any of these defendants, or subject to access by any of these defendants; and
- C. Incurring charges on any credit card issued in the name, singly or jointly, of any of these defendants.

The assets affected by this section shall include both existing assets and assets acquired after issuance of this Order, and these defendants shall hold and account for these assets and all payments received by them, including but not limited to borrowed funds or property and gifts.

III. - NON-INTERFERENCE IN ASSET FREEZE

IT IS FURTHER ORDERED that defendants Donald R. Grant, Monique Delgado, and Gail Oliver are hereby temporarily restrained and enjoined from taking, with respect to the assets of Fortuna, Augustine Delgado, and Libby Gustine Welch, any of the actions prohibited to Fortuna, Augustine Delgado, and Libby Gustine Welch in Section II above, except as provided in Section IV below.

IV. - REPATRIATION OF FOREIGN ASSETS

IT IS FURTHER ORDERED that defendants shall:

- A. Immediately upon service of this Order, or as soon thereafter as Antiguan banking hours permit, direct that the Swiss American Bank of Antigua transfer to Fortuna Alliance's bank account at Whatcom State Bank all funds previously transferred by or from Fortuna Alliance, Augustine Delgado, or Libby Gustine Welch to that bank.
- B. Immediately upon service of this Order, or as soon as relevant banking hours permit, transfer to the territory of the United States all funds, documents, and assets in foreign countries held either: (1) by Fortuna, Augustine Delgado, or Libby Gustine Welch; (2) for their benefit; or (3) under their direct or indirect control, jointly or singly. This includes, but is not limited to, all funds retransferred by the Swiss American Bank of Antigua to any other bank or asset holder.
- C. Hold and retain all repatriated funds, documents, and assets, and prevent any transfer, disposition, or dissipation of these funds, documents, and assets, except to the extent that Section XI of this Order requires delivery of them to the receiver.
- D. Provide plaintiff and, with respect to Fortuna's assets, the receiver, with access to defendants' records and documents held by financial institutions outside the territorial United States, by

signing the Consent to Release of Financial Records attached to this Order.

E. Provide plaintiff and, with respect to Fortuna's assets, the receiver with a full accounting of all funds, documents and assets outside of the territory of the United States which are held either: (1) by them; (2) for their benefit; or (3) under their direct or indirect control, jointly or singly;

V. - MAINTENANCE OF RECORDS

IT IS FURTHER ORDERED that defendants are hereby temporarily restrained and enjoined from:

A. Failing to create and maintain books, records, and accounts which, in reasonable detail, accurately, fairly, and completely reflect the incomes, disbursements, transactions, and use of monies by defendants.

B. Destroying, erasing, mutilating, concealing, altering, transferring or otherwise disposing of, in any manner, directly or indirectly, any contracts, membership or mailing (including "Email") lists, accounting data, correspondence, advertisements, computer tapes, disks, or other computerized records, books, written or printed records, handwritten notes, telephone logs, telephone scripts, "verification" tapes or other audio or video tape recordings, receipt books, invoices, postal receipts, ledgers, personal and business canceled checks and check registers, bank statements, appointment books, copies of federal, state or local business or personal income or property tax returns, and other documents or records of any kind that relate to the business practices or business or personal finances of any defendant.

VI. - DUTIES OF ASSET HOLDERS

IT IS FURTHER ORDERED that, except as stipulated by the parties or as directed by further order of the Court, any financial or brokerage institution, business entity, or person that holds, controls, or maintains custody of any account or asset, including any membership or mailing (including "Email") lists, real or personal property of defendants Fortuna, Augustine Delgado, or Libby Gustine Welch, or has held, controlled, or maintained custody of any account or asset of any of these defendants at any time since December 31, 1995, shall:

A. Prohibit all persons and entities except, with respect to Fortuna's assets, the receiver appointed by this Order and his designated representatives or agents, from withdrawing, removing, assigning, transferring, pledging, encumbering, disbursing, dissipating, converting, selling, or otherwise disposing of any of these assets.

B. Deny all persons and entities, except, with respect to Fortuna's assets, the receiver appointed by this Order and his designated representatives and agents, access to any safe deposit box that is titled in the name of any of these defendants, either individually or jointly, or otherwise subject to access by any of these defendants.

C. Provide counsel for plaintiff and, with respect to Fortuna's assets, the receiver, within five business days of receiving a copy of this Order, a certified statement setting forth:

1. the identification number of each account or asset titled in the name, individually or jointly, of any of these defendants, or held on behalf of, or for the benefit of, any of these defendants, including all trust accounts managed on behalf of these defendants or subject to any of these defendants' control;
2. the balance of each identified account, or a description of the nature and value of the asset as of the close of business on the day on which this Order is served, and, if the account or other asset has been closed or removed since November 1, 1995, the date closed or removed, the total funds removed in order to close the account, and the name of the person or entity to whom the account or other asset was remitted; and

3. the identification and location of any safe deposit box that is either titled in the name, individually or jointly, of any of these defendants, or is otherwise subject to access by any of these defendants.

D. Upon request and within five business days, provide to counsel for plaintiff and, with respect to Fortuna's assets, to the receiver copies of all records or other documentation pertaining to the account or asset described in Paragraph C above, including but not limited to originals or copies of account applications, account statements, signature cards, checks, drafts, deposit tickets, transfers to and from the accounts, all other debit and credit instruments or slips, currency transaction reports, 1099 forms, and safe deposit box logs.

E. With respect to Fortuna's assets, cooperate with all reasonable requests of the receiver relating to implementation of this Order, including transferring funds at the receiver's direction and producing records related to these defendants' accounts.

VII. - SERVICE OF TRO

IT IS FURTHER ORDERED that copies of this Order may be served by first class mail, overnight delivery, facsimile, or personally, by employees or agents of the FTC or the receiver, upon any bank, savings and loan institution, credit union, financial institution, brokerage house, escrow agent, money market or mutual fund, title company, commodity trading company, common carrier, storage company, trustee, commercial mail receiving agency, mail holding or forwarding company, or any other person, partnership, corporation, or legal entity that may be in possession of any records, assets, property, or property right of any defendant, and any Internet service provider or other person, partnership, corporation, or legal entity that may be subject to any provision of this Order. For purposes of service on anyone in possession of records, assets, property, or property rights, actual notice of this Order shall include notice from service by facsimile transmission of Sections VI, VII, X, and XIII of this Order, provided that this notice is followed within five business days by delivery of a complete copy of this Order. For purposes of service on any Internet service provider, actual notice of this Order shall include notice from service by facsimile transmission or electronic mail of the text of Sections VII and XIX.B of this Order, provided that this notice is followed within five business days by delivery of a complete copy of this Order.

VIII. - DEFENDANTS' FINANCIAL STATEMENTS

IT IS FURTHER ORDERED that each defendant shall, within four business days from service of this Order, prepare and deliver to the counsel for the Commission and, with respect to Fortuna's assets, the receiver, completed financial statements on the forms attached to this Order. The completed financial statements shall be accurate as of the date of service of this Order upon the defendant. The defendants shall attach to these completed financial statements copies of all state and federal income and property tax returns for each individual and entity since January 1, 1995 and copies of all policies of insurance in effect since January 1, 1995, with attachments and schedules thereto, insuring against loss of, or damage to, real or personal property owned or held by or for the limited liability company or individual defendant.

IX. - ACCESS TO PREMISES

IT IS FURTHER ORDERED that defendants shall allow plaintiff and the receiver, and their representatives, agents, and assistants, immediate access to Fortuna's business premises and any other locations where Fortuna's property or business records are located. The locations of defendant Fortuna's business premises specifically include, but are not limited to, the Fortuna offices and facilities in Bellingham, WA and Carson City, NV. The purpose of this access shall be to inspect and inventory all defendants' property, assets, and documents and to inspect and copy any documents relevant to this action. For purposes of this provision, the term "document" shall include all those items described in Paragraph V.B above. The Commission shall have the right to remove documents from defendants'

premises in order that they may be inspected, inventoried, and copied. The documents so removed shall be returned to Fortuna's premises, or any other location directed by the receiver, within seven business days unless the receiver agrees to a longer period.

X. - APPOINTMENT OF RECEIVER AND RECEIVER DUTIES

IT IS FURTHER ORDERED that Michael A. Grassmueck, Inc., is appointed as receiver with the full power of an equity receiver for Fortuna and its subsidiaries and affiliates, and of all funds, properties, premises and other assets directly or indirectly owned, wherever situated, beneficially or otherwise, by this defendant with directions and authority to accomplish the following:

A. Take custody, control, and possession of all funds, property, premises, mail, and other assets of, or in the possession or control of Fortuna, including the contents of any safe deposit box, wherever situated, with full power to divert, return to sender, hold without opening, open, or copy any mail, and to sue for, collect, receive and take in possession all goods, chattels, rights, credits, monies, effects, lands, leases, books, work papers, and records of accounts, including electronic files on any media, and other papers and documents of defendant Fortuna and members of the public whose interests are now held by or under the direction, possession, custody or control of Fortuna. With respect to the premises of defendant Fortuna that are located outside the State of Washington, the receivership custody, control, and possession shall be implemented initially on behalf of the receivership estate by the Commission and, if the receiver and the Commission deem it necessary, agent(s) of the receiver. The persons implementing this Order at each non-Washington location shall: (1) effect service of this Order at the location; (2) complete a written listing of all employees, "volunteers," and other agents of Fortuna and any other persons found at the site, including, to the extent feasible, the name, home address, social security number, job description, and, for any employees of Fortuna, the method of compensation and a statement of all accrued and unpaid commissions and compensation; (3) prepare an inventory of electronic equipment found on site; and (4) secure the location by changing door locks and passwords, disconnecting any computers and modems, and preventing any other means of access to the computers or other records or property maintained at that location.

B. Conserve, hold, and manage all such assets, pending stipulation of the parties or further order of this Court; to obtain an accounting thereof; and to report to this Court and the Commission any violations of this Order or of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), that the receiver may become aware of by any defendant, their respective officers, directors, agents, servants, employees, "volunteers," attorneys, salespersons, successors, assigns, subsidiaries, affiliates, corporations, and other persons or entities under their control and all persons in active concert or participation with them.

C. Hold, preserve, and administer the business of Fortuna until further order of this Court, with full authority to perform all acts necessary or incidental thereto, including terminating employees, "volunteers," and independent contractors

D. Cease all promotion, operation, or maintenance of Fortuna Alliance or any other pyramid scheme or any business incident thereto, including but not limited to any business that involves purchases by or distributions to any members of Fortuna Alliance or any other pyramid scheme.

E. Continue and conduct any lawful business of Fortuna not incident to any pyramid scheme, in such manner, to such extent, and for such duration as the receiver may in good faith deem to be necessary or appropriate to profitably and lawfully operate that business, if at all; **provided** that the continuation and conduct of the business shall be conditioned upon Fortuna first demonstrating to the satisfaction of the Court, at the show cause hearing scheduled in Section XXIII below, that the business can be lawfully operated at a profit using the funds and other assets of the receivership estate. Fortuna shall immediately, and thereafter from time to time upon request of the receiver, advise the receiver concerning each location at which defendant Fortuna conducts

business and all matters relevant to the continuation and conduct of that business.

F. Employ any managers, agents, employees, servants, accountants, and technical specialists as may in the receiver's judgment be advisable or necessary in the management, conduct, control, or custody of the affairs of defendant Fortuna and the assets thereof, and otherwise generally to assist in the receivership.

G. Make any payments and disbursements that may be necessary and advisable for the preservation of the properties of Fortuna and as may be necessary and advisable in discharging the receivership duties.

H. Give information, in a form to be provided or approved by counsel for the plaintiff, regarding the status of Fortuna and this action to current, former, or prospective consumer participants in Fortuna's pyramid scheme that the receiver in its judgment deems advisable or necessary and practicable, including but not limited to notice through answering machines, faxes, electronic mail, and postings on Fortuna's home pages on the World Wide Web.

I. Receive and collect any and all sums of money due or owing Fortuna in any manner whatsoever, whether the same are now due or shall hereafter become due and payable, except to the extent that debts are owed by members of the public who agreed to participate in any pyramid scheme, and to do such things and enter into such agreements in connection with the administration, care, preservation, and maintenance of the properties of Fortuna as the receiver may deem advisable.

J. Institute, prosecute, and defend, compromise, adjust, intervene in, or become party to any actions or proceedings in state, federal, or foreign courts as may in the receiver's opinion be necessary or proper for the protection, maintenance, and preservation of the assets of Fortuna or the carrying out of the terms of this Order, and likewise to defend, compromise, or adjust or otherwise dispose of any or all actions or proceedings instituted against the receiver or against Fortuna and also to appear in and conduct the defense of any suit or adjust or compromise any actions or proceedings now pending in any court by or against Fortuna where the prosecution, defense, or other disposition of those actions or proceedings will, in the judgment of the receiver, be advisable or proper for the protection of the properties of Fortuna.

K. Make periodic reports, observations, and recommendations to this Court, and to seek guidance and instructions from this Court, if the receiver deems it necessary, upon one day's written or oral notice to all parties who have filed an appearance in this proceeding.

L. The receiver and its accountants, attorneys, agents, and consultants shall be compensated from the assets of the receivership estate for their normal hourly charges and for all expenses incurred by them in fulfilling the terms of this Order. This compensation for the receiver's personnel shall be at the rate of \$125 per hour for Michael Grassmueck, \$40 per hour for the receiver's staff, and the customary hourly rates for other agents and consultants. The receiver shall also be compensated for automobile mileage expenses at a rate of 29.94 per mile, photocopies at a rate of 154 per page, and for long distance, postage, travel, and other expenses at actual cost. The receiver may pay itself and its accountants, attorneys, agents, and consultants on a regular basis as and when billed from assets of the receivership estate, provided that the receiver shall provide a monthly accounting to the Court, that the Court shall retain the right to accept or deny any particular charges, and that the receiver shall apply to the Court for approval of these charges at regular intervals of three months.

XI. - TURN OVER TO RECEIVER

IT IS FURTHER ORDERED that, immediately upon service of this Order upon them, defendants, and any other person or entity served with a copy of this Order, shall immediately deliver over to the receiver:

- A. Possession and custody of all funds, assets, property owned beneficially or otherwise, and all other assets, wherever situated, of Fortuna.
- B. Possession and custody of all books and records of accounts, all financial and accounting records, balance sheets, income statements, bank records (including monthly statements, canceled checks, records of wire transfers, and check registers), client lists, membership and mailing lists (including Email), title document, and other papers of Fortuna.
- C. Possession and custody of all funds and other assets belonging to members of the public now held by Fortuna.
- D. All passwords or codes required to access any hardware, software, or electronic files on any media.
- E. All keys, passwords, identification numbers, entry codes, and combinations to locks required to open or gain access to any of Fortuna's property or effects, Fortuna's computer files (including all backup tapes), and all monies in any bank deposited by or to the credit of Fortuna, wherever situated.
- F. Information identifying the accounts, employees, "volunteers," properties, or other assets or obligations of Fortuna.
- G. A statement providing the total number of individuals and entities, and the name, address, phone number, and payment record of each of them, who is listed as a member or participant in the Fortuna program, whether directly or through any other entity, and the total dollar amount of money received from each customer and paid out to each customer.

XII. - NON-INTERFERENCE WITH RECEIVER

IT IS FURTHER ORDERED that the defendants shall refrain from interfering with the receiver taking custody, control, or possession and from interfering in any manner, directly or indirectly, with the custody, possession, and control of the receiver; shall fully cooperate with and assist the receiver appointed in this action; and shall take no action, directly or indirectly, to hinder or obstruct the receiver in the conduct of its duties or to interfere in any manner, directly or indirectly, with the custody, possession, management, or control by the receiver.

XIII. - 3D PARTY COOPERATION WITH RECEIVER

IT IS FURTHER ORDERED that any bank, savings and loan institution, credit union, financial institution, brokerage house, money market or mutual fund, common carrier, storage company, escrow agent, title company, commodity trading company, trustee, Internet service provider, or any other person, partnership, corporation, or other legal entity that is served with a copy of this Order, shall cooperate with all reasonable requests of the receiver relating to implementation of this Order, including transferring funds and the contents of safe deposit boxes at the receiver's discretion and producing for the receiver records related to defendants' accounts.

XIV. - RECEIVER'S BOND

IT IS FURTHER ORDERED that the receiver shall file with the Clerk of this Court within five days of entry of this Order a bond in the sum of \$500,000 with sureties to be approved by the Court, conditioned that the receiver will well and truly perform the duties of the office and duly account for all monies and properties which may come into its hands and abide by and perform all things which he shall be directed to do.

XV. - STAY OF OTHER ACTIONS

IT IS FURTHER ORDERED that except by leave of this Court, the defendants and all customers, principals, investors, creditors, stockholders, lessors, and other persons seeking to establish or enforce any claim, right or interest against or on behalf of the defendants, or its subsidiaries or affiliates, and all others acting for or on behalf of those persons including attorneys, trustees, agents, sheriffs, constables, marshals, and other officers and their deputies and their respective attorneys, agents, servants, and employees be and are hereby stayed from:

A. Commencing, prosecuting, continuing, or enforcing any suit or proceeding against Fortuna, or its subsidiaries or affiliates, or the receiver, except that any action may be filed to toll any applicable statutes of limitations.

B. Commencing, prosecuting, continuing, or enforcing any suit or proceeding in the name of the defendants or their subsidiaries or affiliates.

C. Accelerating the due date of any obligation or claimed obligation, enforcing any lien upon, or taking or attempting to take possession or retaining possession of, property of defendant Fortuna, or its subsidiaries or affiliates, or any property claimed by Fortuna, or attempting to foreclose, forfeit, alter, or terminate any interests of Fortuna in any property, whether these acts are part of a judicial proceeding or otherwise.

D. Using self-help or executing or issuing, or causing the execution or issuance of any court attachment, subpoena, replevin, execution, or other process for the purpose of impounding or taking possession of or interfering with or creating or enforcing a lien upon any property, wheresoever located, owned or in the possession of the Fortuna, or its subsidiaries or affiliates, or the receiver appointed pursuant to this Order or any agents appointed by the receiver.

E. Doing any act or thing whatsoever to interfere with the receiver taking control, possession, or management of the property subject to this receivership, or to in any way interfere with the receiver, or to harass or interfere in any manner with the duties of the receiver; or to interfere in any manner with the exclusive jurisdiction of this Court over the property and assets of defendant Fortuna or its subsidiaries or affiliates.

Provided, however, that nothing in this section shall prohibit any federal, state, or local law enforcement or regulatory authority from commencing or prosecuting an action against any defendant.

XVI. - CREATION OF OTHER BUSINESSES

IT IS FURTHER ORDERED that defendants are hereby temporarily restrained and enjoined from creating, operating or controlling any business entity, whether newly-formed or previously inactive, including any partnership, limited partnership, joint venture, sole proprietorship, or corporation, without first providing the Commission with a written statement disclosing: (1) the name of the business entity; (2) the address and telephone number of the business entity; (3) the names of the business entity's officers, directors, principals, managers and employees; and (4) a detailed description of the business entity's intended activities.

XVII. - EXPEDITED DISCOVERY

IT IS FURTHER ORDERED that Plaintiff is granted leave, to initiate discovery prior to the proposed discovery plan required by FRCP 26(f) and, pursuant to FRCP 30(a), to take the deposition of any person, in any judicial district, at any time after the date of this Order, upon three days notice; pursuant to FRCP 33, defendants' responses to any interrogatories served by the plaintiff shall be within ten days after service of the interrogatories; pursuant to FRCP 34, defendants' response to any request by plaintiff for production of documents shall be within five days after service of the request; pursuant to FRCP 36

defendants' responses to any request for admissions served by plaintiff shall be within five days after service of the requests.

XVIII. - CONSUMER CREDIT REPORTS

IT IS FURTHER ORDERED that pursuant to Section 604(1) of the Fair Credit Reporting Act, 15 U.S.C. ' 1681b(1), any consumer reporting agency may furnish a consumer report concerning any defendant to plaintiff or the receiver.

XIX. - NOTICE TO RELATED PERSONS AND ENTITIES

IT IS FURTHER ORDERED that:

A. Defendants shall immediately provide a copy of this Order to each affiliate, subsidiary, division, sales entity, successor, assign, officer, director, employee, "volunteer," independent contractor, agent, attorney, and representative, and shall, within ten days from the date of entry of this Order, provide plaintiff with a sworn statement that defendants have complied with this provision of the Order, which statement shall include the names and addresses of each such person or entity who received a copy of the Order.

B. Immediately upon service of this Order upon them, defendants, and any other person or entity served with a copy of this Order, including any Internet service provider that currently provides facilities for promotional materials of the Fortuna Alliance program through electronic means, shall forthwith take whatever action is necessary to ensure that any home page on the World Wide Web containing those promotional materials which is or has been addressable by users of the Web carry only the following statement plus the link information that follows:

The Federal Trade Commission (FTC) has filed a lawsuit charging that Fortuna Alliance, Augustine Delgado, and other individuals have been operating a fraudulent and unlawful pyramid sales scheme. The United States District Court for the Western District of Washington has issued a temporary restraining order temporarily prohibiting further sales and promotional activities of Fortuna Alliance. You may obtain additional information directly from the FTC.

Each page carrying this message shall also provide a hypertext link to the FTC home page (<http://www.ftc.gov/ro/fortuna.htm>) or other home page designated by counsel for the FTC. For Fortuna's own home pages, the language above may be modified by the receiver as provided in Paragraph X.H of this Order.

C. Immediately upon service of this Order upon them, defendants shall Email a copy of the statement in Paragraph B above, as well as a notice that further information is available at the designated FTC home page and any other information requested by the receiver as provided in Paragraph X.H of this Order, to all persons and entities on its current Email distribution lists.

XX. - FILING OF PLEADINGS

IT IS FURTHER ORDERED that defendants shall file their opposition, including any declarations, exhibits, memoranda, or other evidence on which defendants intend to rely, not less than three business days before the hearing on the order to show cause why a preliminary injunction should not issue. Defendants shall serve copies of all these materials on plaintiff by delivery or facsimile to designated counsel for the Federal Trade Commission, at 915 Second Avenue, Suite 2806, Seattle, Washington 98174, prior to 4:00 p.m. on the day that it is filed.

XXI. - WITNESSES AT HEARINGS

IT IS FURTHER ORDERED that, if any party to this action intends to present the testimony of any witness at the hearing on a preliminary injunction in this matter, that party shall, at least seventy-two hours prior to the scheduled date and time of hearing, file with this Court and serve on counsel for the other party, a statement of the name, address, and telephone number of that witness, and either a summary of the witness' expected testimony, or the witness' declaration or affidavit revealing the substance of the witness' expected testimony; and that, after the service of the statement, the served party thereafter shall have forty-eight hours from the time of service of the witness information to provide information to the Court and to the serving party for any witness whose testimony the served party intends to present.

XXII. - EXPIRATION

IT IS FURTHER ORDERED that the Temporary Restraining Order granted herein expires ten days after entry unless, within that time, the Order for good cause shown is extended for an additional period not to exceed ten days, or unless it is extended with the consent of the parties.

XXIII. - SHOW CAUSE

IT IS FURTHER ORDERED that each of the defendants shall appear before this Court on the 30th day of May, 1996, at 10:00 o'clock a.m., to show cause, if any there be, why this Court should not continue the appointment of the receiver and enter a preliminary injunction, pending final ruling on the Complaint against these defendants, enjoining them from further violations of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), continuing the relief provided herein and the freeze of their assets, and imposing whatever additional relief may be appropriate.

XXIV. - RETENTION OF JURISDICTION

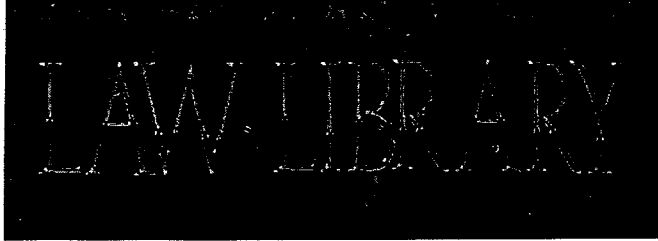
IT IS FURTHER ORDERED that this Court shall retain jurisdiction of this matter for all purposes.

SO ORDERED, this 24th day of May, 1996, at 9:30 am.

Walter T. McGovern
United States District Judge

PRESENTED BY:

[signature]
Randall H. Brook, WSBA # 4860
Eleanor Durham
Attorneys for Plaintiff
Federal Trade Commission



Go To Select your destination: ▼

THE HONORABLE WALTER T. McGOVERN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

FEDERAL TRADE COMMISSION, Plaintiff,

Civ. No. C96-799M

v.

**STIPULATED FINAL
JUDGMENT AND ORDER AS
TO CERTAIN DEFENDANTS**

FORTUNA ALLIANCE, L.L.C., *et al.*,
Defendants

Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), has filed a complaint for a permanent injunction and other relief pursuant to Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. 53(b), naming as defendants Fortuna Alliance, L.L.C., Augustine Delgado, Libby Gustine Welch, and Donald R. Grant, (the "Fortuna Defendants") and alleging violations of Section 5 of the FTC Act, 15 U.S.C. 45.

The Fortuna Defendants and the Commission, by and through their respective counsel, have agreed to entry of this Order by this Court in order to resolve all matters in dispute between them in this action. The Fortuna Defendants have consented to the entry of this Order without trial or adjudication of any issue of law or fact herein. NOW, THEREFORE, the Fortuna Defendants and the Commission having requested the Court to enter this Order, **IT IS HEREBY ORDERED, ADJUDGED, AND DECREED** as follows:

FINDINGS

- A. This Court has jurisdiction of the subject matter of this action and the parties consenting hereto.
- B. Entry of this Order is in the public interest.
- C. The Fortuna Defendants have waived all rights to seek judicial review or otherwise challenge or contest the validity of this Order.
- D. This Order does not constitute and shall not be interpreted to constitute either an admission by the Fortuna Defendants or a finding by the Court that the Fortuna Defendants have engaged in violations of the FTC Act.

DEFINITIONS

For purposes of this Order the following definitions apply:

A. "Multi-level marketing program" means any marketing strategy in which participants pay money to the program promoter in return for which program participants obtain the right to (1) recruit additional participants, or to have additional participants placed by the promoter or any other person into the program participant's downline, tree, cooperative, income center, or other similar program grouping; (2) sell goods or services; and (3) receive payment; PROVIDED the payments received by program participants are derived primarily from the sale or purchase of the goods or services, and not from recruiting additional participants nor having additional participants placed into the program participant's downline, tree, cooperative, income center, or other similar program grouping. For purposes of this Order, the phrase "goods or services" does not include a membership or opportunity to participate in another sales or marketing program.

B. "Chain or pyramid marketing program" is a sales device whereby a person, under a condition that he or she make a payment, is granted a license or right to recruit for consideration one or more additional persons who are also granted a license or right upon condition of making a payment, and may further perpetuate the chain or pyramid of persons who are granted a license or right upon such condition. A limitation as to the number of persons who may participate, or the presence of additional conditions affecting eligibility for the above license or right to recruit or the receipt of profits therefrom, does not change the identity of the program as a chain or pyramid marketing program.

C. "Person" means a natural person, organization or other legal entity, including a corporation, partnership, proprietorship, association, cooperative, government or governmental subdivision or agency, or any other group or combination acting as an entity.

D. "Assisting" means providing the means and instrumentalities for or otherwise facilitating any conduct that a defendant knows or should know violates any provision of Sections I or II of this Order. This includes, but is not limited to, formulating or providing or arranging for the formulation or provision of written or electronic promotional materials.

ORDER

I.

IT IS THEREFORE ORDERED that the Fortuna Defendants, whether acting directly or through any business, entity, corporation, subsidiary, division, or other device, in or affecting commerce, as "commerce" is defined in the FTC Act, 15 U.S.C. 44, are permanently enjoined from engaging, participating, or assisting in any manner or capacity whatsoever in the advertising, promoting, offering for sale, or sale, of any chain or pyramid marketing program, except that the Fortuna Defendants are not enjoined from engaging, participating, or assisting in multi-level marketing programs.

II.

IT IS FURTHER ORDERED that the Fortuna Defendants, whether acting directly or through any business, entity, corporation, subsidiary, division, or other device, in connection with the advertising, promoting, offering for sale, or sale of any marketing or investment program, in or affecting commerce, as "commerce" is defined in the FTC Act, are hereby permanently restrained and enjoined from making, or assisting another in

making, directly or by implication, orally or in writing, any misrepresentation about any material fact, including, but not limited to, misrepresentations about earnings that program participants have actually made or can potentially make.

III.

IT IS FURTHER ORDERED that refunds of membership fees shall be offered to all eligible members of Fortuna Alliance by an independent Redress Contractor selected by the parties from those currently under contract to the FTC. The Redress Contractor shall use a notice and claim form containing the text of Attachment A to this order, and follow its standard procedures for administering redress funds in FTC cases. The Redress Contractor shall also provide with the notice a copy of the FTC's consumer information pamphlet called "Multilevel Marketing Plans."

The costs of administering the redress program shall come from a Redress Fund created from funds currently held by the court-appointed receiver. The balance of the Redress Fund shall be used to pay refunds. If requests for refunds exceed this initial Redress Fund, the Fortuna Defendants shall make sufficient additional funds available to the Redress Contractor to pay all refunds in full. The Fortuna Defendants shall secure this obligation with an irrevocable letter of credit confirmed by a U.S. bank, delivered and payable to the Redress Contractor as beneficiary, in an amount of \$2.8 million. The terms of the letters of credit and confirmation are attached as Attachment B.

For purposes of this section, an "eligible member" is one (1) whose membership fee(s) were actually paid to Fortuna, that is, not gifted or otherwise provided without payment; (2) who did not receive payments from Fortuna equal to or exceeding the membership fee(s) paid; and (3) who returns a properly filled out claim form. The Redress Contractor will accept claim forms up to 120 days of the mailing date on the notice, notwithstanding the shorter time period stated on the notice, and will commence making payments as soon as practicable thereafter. If a member has received payments from Fortuna but those payments were less than the membership fees paid, then any refund will be reduced by the amount of payments received.

If the Fortuna Defendants fail to meet the payment obligations set forth in this section, they shall pay the costs and attorneys fees incurred by the FTC and its agents in any attempts to collect amounts due pursuant to this Order.

IV.

IT IS FURTHER ORDERED that the Fortuna Defendants shall aid and assist the Commission, or the designated Redress Contractor, without compensation from the Redress Fund or the FTC and in any manner reasonably requested by the Redress Contractor, in determining which Fortuna members may be eligible for refunds and in obtaining information from Fortuna's records to locate those members.

V.

IT IS FURTHER ORDERED that within 15 days of entry of this Order, the FTC shall (1) place on the FTC Internet website the text of this Stipulated Order and the notice as set out in Attachment A; and (2) notify the two Internet Service Providers previously used by Fortuna for its websites that the prohibition on Fortuna's use of the websites is released.

VI.

IT IS FURTHER ORDERED that:

A. The receiver shall transfer \$320,000 of Fortuna Alliance funds to the Redress Contractor identified in Section III within five days after entry of this Order.

B. Upon entry of this Order, Fortuna Alliance, L.L.C. shall be solely responsible for paying, challenging, or otherwise resolving (1) all outstanding claims of indebtedness to its creditors, where those claims arose or accrued before the appointment of the receiver by this Court, and (2) any accruals to those claims, where those accruals occurred after the appointment of the receiver, and the receiver is hereby released and discharged from all liability or obligation to those creditors on those claims.

C. The receiver may use Fortuna Alliance funds to pay the fees and costs of foreign counsel retained by the receiver for the purpose of securing foreign assets related to this case. Resolution of liability for payment of any other claims against Fortuna Alliance funds, except for those covered in section III and paragraphs VI.A-B above, shall be subject to agreement between the Fortuna Defendants and the receiver, or otherwise resolved by further order of this Court.

D. The receiver shall file its final accounting and application for discharge by the later of March 15, 1997, or within 30 days after receiving notice that the letter of credit confirmation has been delivered to the Redress Contractor, as described in section III above, or by such other date as the Court may direct. The parties shall file any comments or objections to the receiver's accounting and application within 10 days after service upon them of the filing. The receiver shall file any reply to those comments or objections within 10 days after service on it of the comments or objections.

E. Upon discharge, and after completing such disbursements as the Court may order, the receiver shall pay the remaining funds in the receivership estate to the Redress Contractor, or if at that time the redress program has been fully administered, to Fortuna Alliance L.L.C. or such agent as may be designated by the Fortuna Defendants' counsel, Robert O. Sailer.

VII.

IT IS FURTHER ORDERED that:

A. When the Redress Contractor notifies the FTC that the Redress Contractor has received the \$2.8 million letter of credit confirmation provided for in Section III, the parties shall take whatever steps are necessary and appropriate, if not already taken, to lift any foreign court injunction against the transfer of the Fortuna Defendants' or Fortuna Alliance members' assets and, thereafter, to terminate all related foreign court claims or actions, including those in Antigua and Belize.

B. Neither the FTC, the Fortuna Defendants, nor the court-appointed receiver shall assert claims for fees, costs, or damages against any other party to the foreign actions for claims arising out of those actions.

C. The Fortuna Defendants shall withdraw and not reassert any administrative claims against the FTC.

D. The Fortuna Defendants' counterclaims and additional party claims, as stated in their Second Amended Answer, Counterclaims, and Additional Party Complaint, are hereby dismissed with prejudice, provided, however, that the Fortuna Defendants are not barred from raising new claims against the receiver related to the administration or management of the receivership estate. Similarly, all counterclaims which could have been brought by the FTC and by third-party defendants and additional parties shall be considered to be released and dismissed with prejudice.

VIII.

IT IS FURTHER ORDERED that upon (1) entry of this Order; and (2) delivery to the Redress Contractor of the irrevocable letter of credit confirmation, as described in Section III above, the freeze of the Fortuna Defendants' assets, including personal bank accounts wherever located, as ordered in Sections II and VI of the May 23, 1996, Temporary Restraining Order and the June 12, 1996, Preliminary Injunction, and the lien or encumbrance placed against Blue Mountain Farm, 6324 Saxon Road, Acme, Washington, as ordered by Section III of the June 12, 1996, Preliminary Injunction, shall be permanently released and discharged. The Court-appointed receiver and the Fortuna Defendants are authorized to file notice of this Order with the appropriate entities to effectuate the terms of this provision.

IX.

IT IS FURTHER ORDERED that all prior orders of this Court for contempt sanctions and arrest warrants against certain of the defendants are hereby vacated.

X.

IT IS FURTHER ORDERED that, for a period of five years from the date of entry of this Order, defendants Fortuna Alliance, L.L.C. and Augustine Delgado, whether acting directly or through any trust, corporation, subsidiary, division, or other device, in connection with the continuation of any part of Fortuna Alliance's business or the advertising, promoting, recruitment, offering for sale, or sale of any marketing or investment program, in commerce, as "commerce" is defined in the FTC Act, shall:

A. Maintain and make available to representatives of the Commission, upon reasonable notice, sample copies, in printed form except for category 5, of:

1. Each type of contract or agreement used with members or participants in the program.
2. All printed advertisements or promotional material relating to the program.
3. All advertising or other promotional or commercial material posted in any Internet news group, on the World Wide Web, on any electronic bulletin board system, in any online interactive conversational space or chat room, in the classified advertising section of any online service, or in any other location accessible by modem communications. Each copy shall be accompanied by an indication of the online location where the material was posted.
4. All advertising or other promotional or commercial material made available through any fax-back service.
5. Electronic copies, in HTML format, of any advertising or other promotional material made available on the World Wide Web, together with copies of all graphics files, audio scripts, and other computer files used in presenting information on the World Wide Web. The records shall include the Internet address (URL) of the site, as well as any other information needed to gain access to the site.

B. Maintain and make available to representatives of the Commission, upon reasonable notice, records for every consumer complaint or refund request and responses thereto. These records need only be maintained for two years after the last action taken for a particular complaint or refund request.

XI.

IT IS FURTHER ORDERED that, for a period of five years from the date of entry of this Order, defendants Fortuna Alliance, L.L.C. and Augustine Delgado, in connection with the continuation of any part of Fortuna Alliance's business or the advertising, promoting, recruitment, offering for sale, or sale of any marketing or investment program, in commerce, as "commerce" is defined by the FTC Act, shall:

A. Provide a copy of this Order to, and obtain a signed and dated acknowledgment of receipt of the same from, each officer, director, and managing agent of the program.

B. Maintain, and upon reasonable notice make available to representatives of the Commission, the original and dated acknowledgments of the receipts of copies of this Order required by Paragraph XI.A above.

XII.

IT IS FURTHER ORDERED that for a period of five years from the date of entry of this Order, defendants Augustine Delgado, Libby Gustine Welch, and Donald R. Grant shall notify the FTC in writing of any affiliation or employment with any new marketing or investment business, in commerce, as "commerce" is defined in the FTC Act, within 21 days of the commencement of that affiliation. Each notice shall include the defendant's then-current business and home address and phone number, and a statement of the nature of the new business or employment along with a description of his or her interest, duties, and responsibilities in the business or employment.

XIII.

IT IS FURTHER ORDERED that the Fortuna Defendants shall, within 180 days after the date of entry of this Order, file with the Court a report, in writing, setting forth the manner and form in which he or she has complied with this Order.

XIV.

IT IS FURTHER ORDERED that all notices required of defendants by this Order shall be made to the following address:

Regional Director
Federal Trade Commission
915 Second Avenue, Suite 2896
Seattle, Washington 98174

XV.

IT IS FURTHER ORDERED that in the event that the letter of credit confirmation required by Section III above is not delivered to the Redress Contractor within 120 business days of entry of this Order, or if any party seeks to dissolve the orders freezing assets held in foreign accounts before or without transfer of funds sufficient to cause issuance of the letter of credit and confirmation, this Order shall be null and void as soon as the plaintiff notifies this Court of the occurrence of one of these events.

XVI.

IT IS FURTHER ORDERED that this Court shall retain jurisdiction of this matter for all purposes.

SO ORDERED, this _____ day of , 199__, at Seattle, Washington.

Hon. Walter T. McGovern
UNITED STATES DISTRICT JUDGE

The parties hereby consent to the terms and conditions set forth above and consent to entry of this Order without further notice to the parties. This Order may be signed in separate counterparts, and all the counterparts together shall together constitute a single agreement. The Fortuna Defendants hereby waive any right that may arise under the Equal Access to Justice Act, 28 U.S.C. 2412.

FEDERAL TRADE COMMISSION

Randall H. Brook
Eleanor Durham
Maxine Stansell
Charles A. Harwood
Regional Director

Attorneys for Plaintiff
Federal Trade Commission

DEFENDANTS

By:

Fortuna Alliance, L.L.C.
Augustine Delgado
Libby Gustine Welch
Donald R. Grant

PERKINS COIE

By:

Ronald M. Gould, WSBA #6458
James F. Williams, WSBA #23613
Perkins Coie
1201 Third Avenue
Seattle, WA 98101

JUDD & SAILER, P.L.L.C.

By:

Robert O. Sailer, WSBA #5430

Attorneys for Fortuna Alliance, L.L.C., Augustine Delgado, Libby Gustine Welch, and Donald R. Grant

ATTACHMENT A

FTC v. Fortuna Alliance, L.L.C.

Claims Administration Center

c/o [Redress Contractor, addr, phone #]

[date]

Dear Fortuna Alliance Member:

In May 1996, the Federal Trade Commission ("FTC") sued Fortuna Alliance, LLC ("Fortuna") and the individuals named above. The FTC claimed that the defendants were operating an illegal pyramid scheme and had made deceptive claims about profits that could be earned by becoming a member of Fortuna Alliance. Fortuna Alliance and the individual defendants denied all the charges.

The parties to the lawsuit have mutually agreed to settle this dispute by stipulating to a consent order. This agreement is not an admission of liability. Under the settlement, Fortuna will not offer or make payments to members based primarily on membership dues paid by members of your co-op or income center. Fortuna Alliance has also agreed to set up a fund to allow any current member who wishes a refund to obtain it. The defendants are obligated to pay all eligible refunds in full.

To be eligible to receive a refund, you must fill out the information required on the enclosed claim form and return it to the address above no later than [90 days after mailing]. If you are eligible and you elect to receive a refund, your Fortuna Alliance membership will be canceled. If you've already received payments from Fortuna Alliance that are more than your initial membership fee (for example, \$250 per Elite center), you are not eligible for a refund from this settlement. Also, you must have personally paid money for your membership. If it was gifted to you or received in any way other than by your paying Fortuna Alliance for it, you may not get a refund through this program.

You can elect to remain a member of Fortuna Alliance by simply not returning this form. Fortuna Alliance will be allowed to operate a multi-level marketing business consistent with the terms of the consent order. But any profits you earn in the future must come primarily from sales or purchases of goods or services. You will not be able to receive profits primarily from the distribution of membership fees or dues.

Neither the FTC nor the Claims Administrator make any recommendation about whether you should continue membership in Fortuna Alliance.

Sincerely,
The Claims Administration Center

[Redress Contractor] is the only Claims Administration Center authorized by the Federal Trade Commission to mail notices and claim forms and process and pay refund claims for the FTC vs. Fortuna Alliance et al. settlement. You are not required to pay anything to receive a refund. If any other company or individual contacts you and requests that you send them money or information in return for a refund from Fortuna Alliance, please call the Claims Administration Center immediately at the phone number above.

Privacy Act Notice

This information is being collected in order to make a distribution of funds in connection with a consent decree entered by the U.S. District Court for the Western District of Washington pursuant to 15 U.S.C. 53(b). In addition, this information may be disclosed for other purposes authorized by the Privacy Act, 5 U.S.C. 552a and 47 Fed. Reg. 32,622, including disclosure to other government agencies. Failure to provide the requested information could delay processing or, in some cases, make it impossible for us to process your claim.

ATTACHMENT B

[OUTLINE OF TERMS OF LETTERS OF CREDIT AND CONFIRMATION]

Terms Substantially Similar by and from:

**Issuing Bank (Antigua Overseas Bank Ltd.) and
Confirming/Paying Bank - Bank of America International (N.Y.)**

The following is substantially the terms of the irrevocable Letter of Credit ("L/C") the Antigua Overseas Bank Ltd. and the Bank of America International (N.Y.) would agree to issue and confirm/pay on behalf of Fortuna Alliance, L.L.C., once collateral for the L/C is in place.

To/From Bank of America International (Confirming and paying bank)
One World Trade Centre
New York NY

Test Key:
Currency and Amount: USD 2,800,000

ATTENTION: L/C Department

Beneficiary: The Redress Contractor

We have issued, in your favour, and for the account of Fortuna Alliance, LLC, our irrevocable standby letter of credit number _____/97, which is available for a maximum amount of \$US 2,800,000 against presentation of draft(s) drawn at sight on us and marked "drawn under L/C number _____/97," accompanied by a signed statement from the Redress Contractor certifying that the funds request is in accordance with the district court order in the case of *F.T.C. v. Fortuna Alliance, L.L.C., et al.*

Special Condition

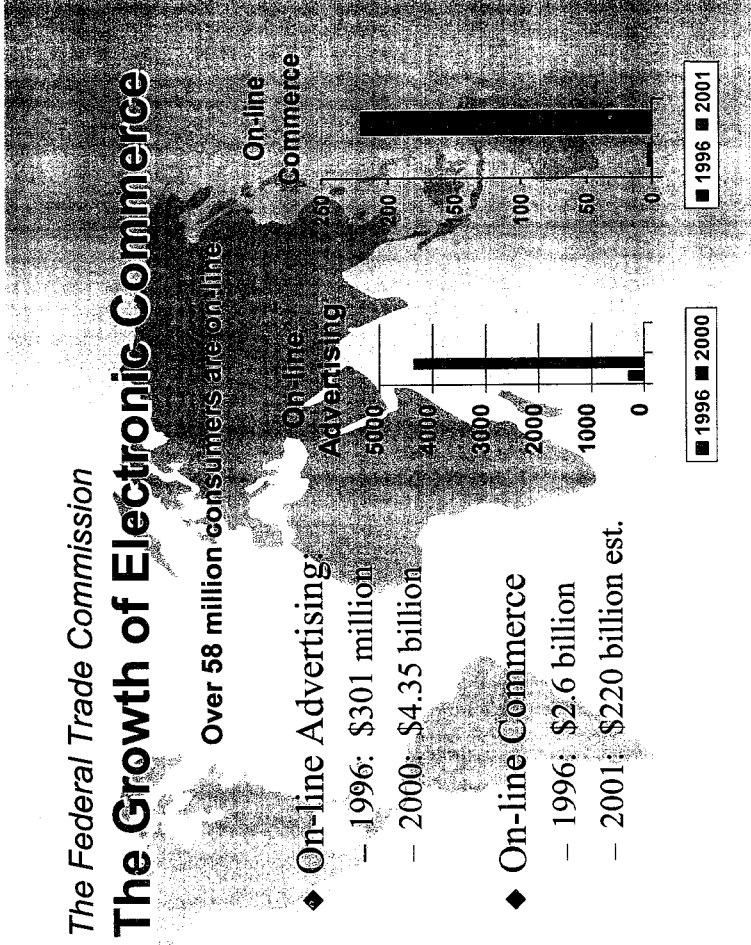
- a) Drawings are not permitted in amounts of less than US\$25,000;
- b) All fees, including confirmation fees, are for the applicants account;
- c) This letter of credit is not assignable or transferable.

Expiry: This letter of credit will expire 150 days from date of issuance [unless another date is agreed to in writing by the parties prior to issuance].

Except so far as expressly stated, this documentary credit is subject to the Uniform Customs and Practices for Documentary Credits (1993), International Chamber of Commerce Publication No. 500.

We hereby engage with the bonafide holders of all drafts drawn and documents presented under and in compliance with the terms of the letter of credit that such drafts and documents will be duly honored upon presentation to us, on or before the expiry date of this letter of credit.



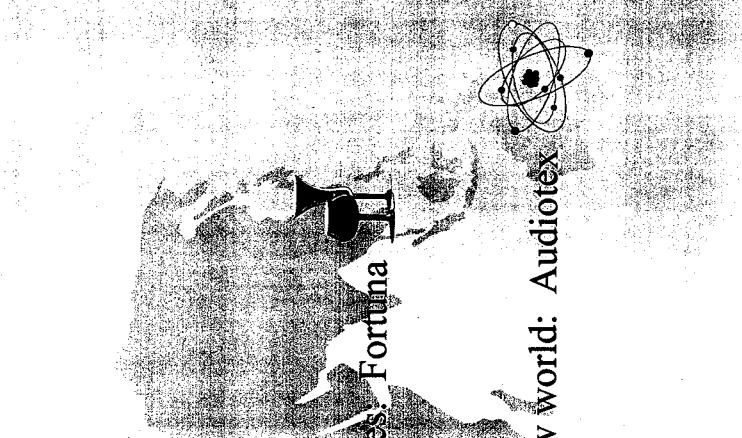


The Federal Trade Commission

Law Enforcement

Over 25 Federal Actions

- ◆ Old wine in new bottles: Fortuna 
- ◆ Fraud in the brave new world: Audiotex 



The Federal Trade Commission

Consumer Education

◆ Web Sites -- www.ftc.gov, www.consumer.gov

◆ Teaser Sites -- The Ultimate Prosperity Page



FEDERAL TRADE COMMISSION

WORKING FOR CONSUMER PROTECTION
AND A COMPETITIVE MARKETPLACE

Current News Releases

[Consumers Lose Billions Annually to Fraud, FTC Chairman Tells Senate Subcommittee](#)

[Prepared Statement of the Federal Trade Commission Concerning Fraudulent Marketing Schemes](#)

[FTC To Junk E-Markets: "No Scamming While You're Spamming."](#)



Who We Are & How We Serve You



Legal Framework



Consumer Protection



Antitrust/ Competition



Business Guidance



Economic Issues



Formal Actions, Opinions & Activities



News Releases, Publications & Speeches



Regional Offices

Privacy Statements

[Contact Us](#)

[Search](#)

[Site Directory](#)

[Glossary](#)

[New Additions](#)

[Related Sites](#)

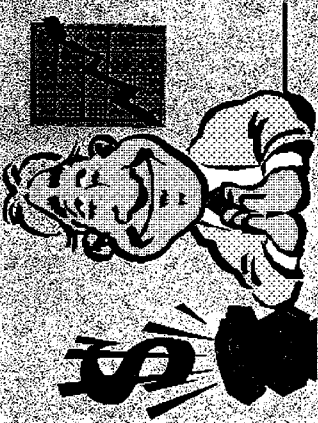
Last Update: Thursday, February 05, 1998

File Edit View Go Bookmarks Options Directory Window Help

Netcape - [The Ultimate Prosperity Page]

The Ultimate Prosperity Page

THE ULTIMATE HOME BASED BUSINESS IN AMERICA!!!



Earn \$60,000 to \$100,000 YOUR VERY FIRST MONTH!!!

Hundreds of people have earned over \$50,000 in their first 30 days -- and you can too!


Start your own outrageously profitable part-time business!
Use your telephone and computer to make money even if you are not home.

The Ultimate Prosperity Page

File Edit View Go Bookmarks Options Directory Window Help

Netcape - [The Ultimate Prosperity Page]

If you responded to an ad like The Ultimate Prosperity Page...



YOU COULD GET SCAMMED!

The Ultimate Prosperity Page does not advertise a real business opportunity. This ad is a fake, posted by the Federal Trade Commission to raise awareness about the hazard of business opportunity fraud on the Net. *No information about you has been transmitted to or collected by the FTC.*

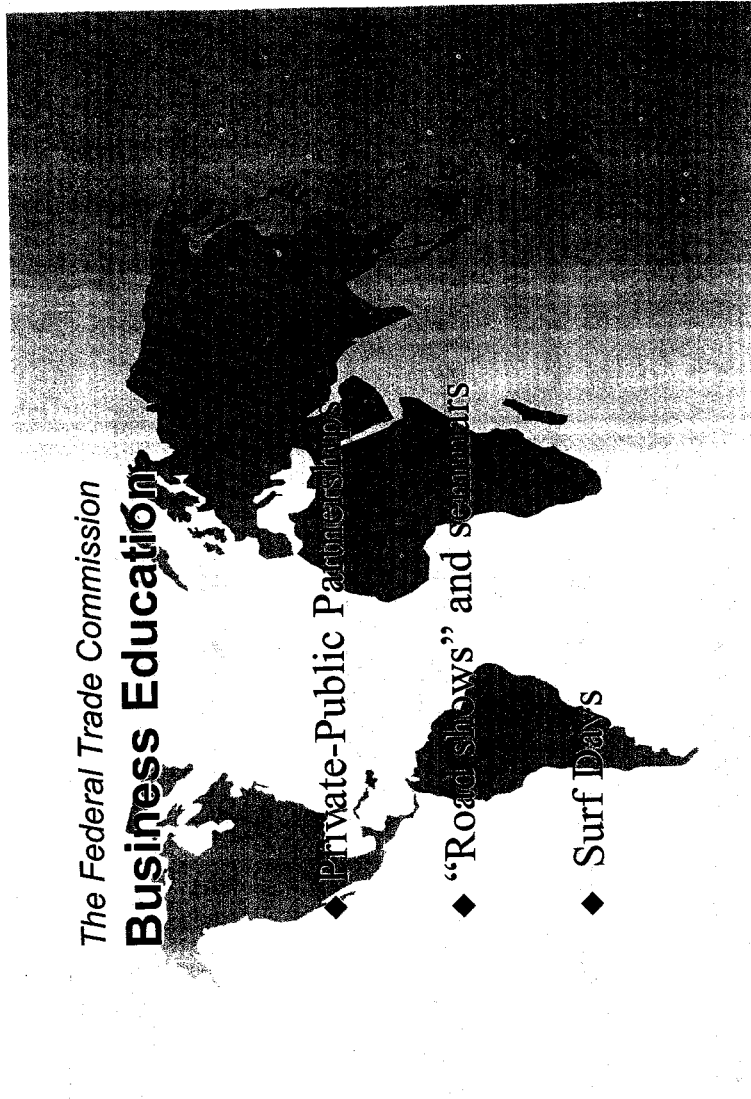
DON'T BE A VICTIM OF CYBERFRAUD

- Beware of online business opportunity advertisements that make exaggerated earnings claims and ads that offer little product information but lots of glowing promises.
- Use *extreme* caution before sending bank account or credit card information online. The Net is NOT a secure environment for financial transactions yet.
- Also use caution when transmitting your address and other personal information. This information is used by scam artists to compile "sucker" lists.

BEFORE YOU INVEST...

- Get disclosure documents and review them carefully. In most cases, the law requires business opportunity and franchise promoters to give potential buyers detailed information about the business and about company finances.
- Check to make sure the business opportunity is compliant with applicable state registration laws.

File Edit View Go Bookmarks Options Directory Window Help



TO: business@xxx.com

FROM: pyramid@ftc.gov

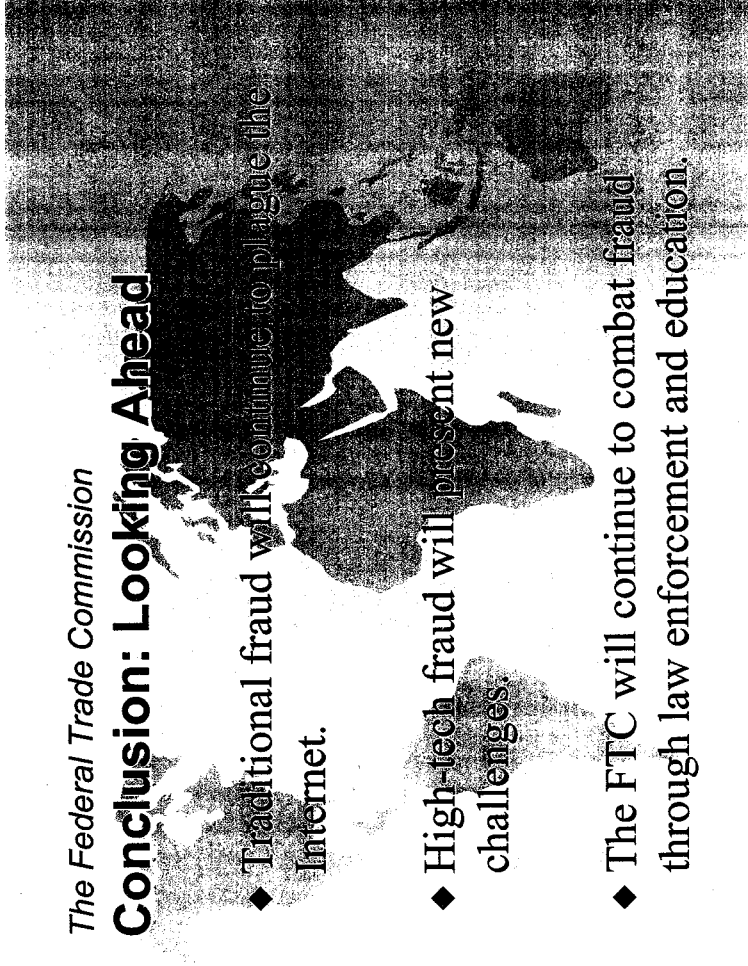
**SUBJECT: A MESSAGE FROM THE U.S.
FEDERAL TRADE COMMISSION**

If you do business in the U.S., you may be interested to know that pyramid schemes are illegal . . .

The Federal Trade Commission

Conclusion: Looking Ahead

- ◆ Traditional fraud will continue to plague the Internet.
- ◆ High-tech fraud will present new challenges.
- ◆ The FTC will continue to combat fraud through law enforcement and education.

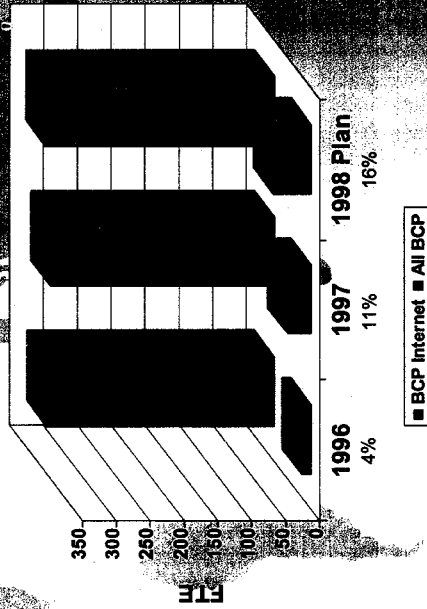


The Federal Trade Commission

Internet Resources

Bureau of Consumer Protection

Internet staff years as a percentage of total Bureau staff years



The Federal Trade Commission

Contacting the FTC

Web Address:

www.ftc.gov

E-mail Address:

consumerline@ftc.gov

Postal Address:

Federal Trade Commission
Consumer Response Center
Washington, DC 20580

Telephone:

(202) FTC-HELP
(202) 382-4357



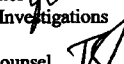



MEMORANDUM

EXHIBIT # 4

February 5, 1998

TO: PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
MEMBERSHIP LIAISONS

FROM: RENA M. JOHNSON, Counsel 
DENNIS McCARTHY, Investigator 
JOHN NEUMANN, Investigator 
Permanent Subcommittee on Investigations

VIA: TIMOTHY J. SHEA, Chief Counsel 
Permanent Subcommittee on Investigations

RE: Traditional Fraudulent Schemes Perpetrated Over the Internet

	<u>Page</u>
I. Introduction	2
II. Internet 101: A Primer	3
III. The Internet as the Medium for Commission of Traditional Frauds	4
1. Undelivered Internet and online services	5
2. Damaged, defective, misrepresented, undelivered, or stolen merchandise ..	5
3. Auction sales	5
4. Pyramid schemes	5
5. Misrepresented online business opportunities and franchises	6
6. Work-at-home schemes	6
7. Prizes and sweepstakes	7
8. Credit card schemes	7
9. Books and other self-help guides	7
10. Magazine subscriptions	7
IV. The Internet as the Instrumentality of Traditional Fraud	8
V. Factors Contributing to Proliferation of Internet Fraud	12
VI. Legal and Practical Issues	15
VII. Conclusion	16
APPENDIX I: State and Federal Criminal Laws Targeting Computer Crime	
APPENDIX II: Governmental Agencies Sharing Jurisdiction Over Internet Fraud	

I. Introduction

In the late nineteenth century, French social theorist Gabriel Tarde constructed his “law of insertion,” which noted how newer criminal modes are superimposed on older ones through a process of imitative learning and technological innovation.¹ Thus, for example, the snake oil salesmen who entranced crowds at the vaudeville shows of the nineteenth century paved the way for the telemarketers of the twentieth century, who in turn set the stage for the infomercials of the past decade. Now, as the twenty-first century looms, Tarde’s insight is being validated again – this time in ways Tarde himself scarcely could have imagined.²

Among the 175 countries presently connected to the Internet, the United States has the largest proportion of Internet users. The exact number of such users is subject to some debate, however; it has been estimated to be as high as fifty million³ and as low as 5.8 million.⁴ A more realistic estimate is that 28.8 million persons in the United States age sixteen and over have access to the Internet, 16.4 million use the Internet, 11.5 million use the World Wide Web, and 1.51 million have used the Web to purchase something.⁵ The number of subscribers is expected to rise to approximately half a billion worldwide by the year 2000.⁶

Internet commerce is predicted to rise correlatively. In 1995, consumers made an estimated quarter of a billion dollars of credit card purchases over the Internet.⁷ In 1996, 2.1 million American households were banking online.⁸ By the year 2000, Internet commerce is expected to increase to between \$6.6 billion⁹ and \$7.4 billion.¹⁰

This rise in the use of the Internet as a vehicle of commerce and communication has yet another correlative. Because it can be used to transfer text, pictures, and sounds, as well as money, credit card numbers, and personal information, the potential for criminal use of the Internet is infinite.¹¹ Corresponding to the phenomenal growth of the Internet, the number of security incidents reported to the Computer Emergency Response Team Coordination Center at Carnegie Mellon University¹² has increased by 498%, and the number of Web sites affected worldwide has increased by 702%.¹³ Law enforcement groups are quickly learning that almost any crime that can be committed in the real world can also be committed in the virtual world – except that by using the Internet, criminals can target more victims faster, cheaper, and with an alarmingly lower chance of apprehension.

The first hearing of PSI’s Internet fraud investigation will focus on the proliferation of traditional fraudulent schemes now being perpetrated over the Internet. “Fraud” is generally defined as “[a]n intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right.”¹⁴ In the context of the Internet, traditional fraud can be classified into two categories, depending on the role the Internet plays in the crime.¹⁵ First, the Internet may be used as the venue of committing such traditional frauds as pyramid schemes, bogus medical treatments, work-at-home promotions, and sweepstakes scams. In these cases, the type of fraud being committed is not new; rather, it is the use of the Internet as the medium of commission that is new. Second, the Internet may be the instrument used to commit the fraud. In these cases, the computer connected to the Internet is the physical site of

the fraud, or is the source of or reason for the particular form of assets lost. In other words, the fraud is unique to computers and the Internet. The use of such weapons as viruses, logic bombs, and Trojan horses (described *infra* Sec. IV, p. 11), to commit fraud fits into this category.¹⁶

This memorandum first provides an informational background section on the Internet. It then discusses in greater detail the two categories of traditional Internet fraud outlined above. The memorandum goes on to discuss the aspects of the Internet that make it such an attractive tool for cybercrooks, as well as some of the legal and practical issues that pose obstacles to law enforcement efforts to identify, apprehend, and prosecute online fraudsters. Finally, this memorandum concludes by outlining the goals of our first hearing.

II. Internet 101: A Primer

The Internet began in 1969 as a Department of Defense initiative to connect itself via computer with military research contractors, including a large number of universities engaged in military-funded research. Following the proliferation of university computers during the 1980s, and the establishment of the National Science Foundation's supercomputer centers and corresponding National Science Foundation Network ("NSFNet"), the modern Internet was born. Because, however, NSFNet permitted traffic related only to research and education, independent commercial network services developed for other kinds of traffic.¹⁷

In 1989 the Internet reached the mainstream of popular interest with the arrival of the World Wide Web,¹⁸ a subset of the Internet.¹⁹ Before the Web came along, users could access Internet sites through other methods, such as the File Transfer Protocol ("FTP"), Telnet, and Gopher.²⁰ The Web, which is now the most popular means of entering the Internet,²¹ allows users to access Internet sites by means of a software package called a "browser."²² What makes the Web so appealing is that it enables the display of full-color graphics.²³ What makes it so powerful is its hyperlink feature, through which highlighted words enable users to access relevant information on other Internet sites, thereby allowing users quickly and easily to explore numerous "Web sites,"²⁴ which exist only on computers connected to the Web and otherwise have no physical location. This activity is known in the vernacular as "surfing the Web."²⁵ Web sites each have a unique Internet address, known as a Universal Resource Locator ("URL") or "domain name."²⁶ URLs end in letters that identify the Web site's resource type. For example, the URL for the United States Senate's Web site is *www.senate.gov*. In this URL, *.gov* refers to a government resource. Similarly, a URL ending in *.com* refers to a private company resource, and *.org* refers to an organization.²⁷ A company called Network Solutions, Inc., of Reston, VA, administers the server that distributes new address information to the other root servers worldwide. It also registers the most popular domain names, including ".com" and ".org," for a \$100 registration fee for the first two years and \$50 per year thereafter. Network Solutions performs these functions pursuant to a contract the National Science Foundation awarded it five years ago. The imminent expiration of this contract at the end of March 1998 has sparked a hotly contested debate over whether Network Solutions' lucrative but efficient monopoly should end in favor of open competition among software firms in assigning domain names.²⁸

There are other areas of the Internet besides the World Wide Web, including the User Network, or "Usenet." Before the advent of the Web, Usenet was the biggest attraction on the Internet.²⁹ Usenet is a worldwide network of special interest electronic bulletin boards where messages about a subject are posted at a central location for anyone to read and reply.³⁰ Usenet consists of thousands of public discussion groups called "newsgroups." Each newsgroup has a specific topic, such as chemistry, feminism, alternative music, or television shows. Using a computer program called a news-reading program, a user can subscribe to newsgroups, read the articles, and write his own articles. Contributing an article is called "posting." Usenet's audience numbers in the tens of millions, and there are about 15,000 newsgroups.³¹

No single entity governs the Internet. The only structure even coming close to resembling a governing body consists of four primary organizations that coordinate the technological management of the Internet.³² Membership in each of these organizations is drawn primarily from the research and technical communities. Aside from providing technical direction, however, these groups pay little if any attention to the content of material found on the Internet or the practices of its users.³³

III. The Internet as the Medium for Commission of Traditional Frauds

The Internet and the many commercial online services provide a valuable new information source for consumers, and tremendous opportunities for retailers, who are finding that the Internet is a low cost method to quickly reach millions of potential consumers.³⁴ However, cyberspace has another side: Fraudulent sellers seeking to exploit the virtues of the Internet – including colors and graphics, anonymity, and mass marketing at low cost – to commit the same types of frauds that have been promulgated for generations.³⁵ In the past two years, the attorneys general of Minnesota, Illinois, Missouri, and Massachusetts have brought twenty civil Internet consumer cases covering such issues as health care product sales, business opportunities, credit repair, illegal gaming, and product and service offerings ranging from phony securities and university degrees to miracle drugs.³⁶ In these cases, use of the Internet is not essential for the crime to occur – these types of fraud occur frequently without use of the Internet, through the mail, telephone, and print mediums. The use of the Internet, however, facilitates the commission of the fraudulent act by enabling the crook to commit the crime faster, process greater amounts of information, and become more difficult to identify and trace.³⁷ The Internet also lends an air of legitimacy that may not be available to fraudsters committing traditional fraud.

The National Fraud Information Center ("NFIC"), a project of the non-profit National Consumers League, was first established in 1992 to combat telemarketing fraud. In 1996, NFIC expanded its mission and began collecting consumer complaints about Internet fraud via a toll-free number and a Web site. NFIC is now the primary clearinghouse for consumer complaints about Internet fraud. NFIC relays these complaints to the Federal Trade Commission and the National Association of Attorneys General. During all of 1996, NFIC received a total of 389 complaints regarding Internet fraud.³⁸ During 1997, in contrast, NFIC has received an average of 100 complaints *per month* dealing with Internet fraud.³⁹ The ten Internet fraud scams consumers most frequently report to NFIC are:⁴⁰

1. Undelivered Internet and online services: One common scam targeting consumers in this area involves attempts to convince victims to pay hundreds or thousands of dollars to get their own Web site, which many Internet service providers give to subscribers at little or no cost.⁴¹ Other scams promise but fail to provide free Internet access with the purchase of software; convince users to pay for a password to access nonexistent pictures; or trick consumers into paying for advertisements that never materialize.⁴²
2. Damaged, defective, misrepresented, undelivered, or stolen merchandise: The types of merchandise being both bought and sold fraudulently over the Internet range from lasers⁴³ to baseball cards.⁴⁴ For example, one common promotion is for a "black box" that promises satellite telephone connections at low cost. In reality, such technology has not yet been perfected for consumer telephone communications.⁴⁵

Online retailers are also frequent fraud victims in this category. Overall, electronically purchased goods are significantly more susceptible to fraudulent purchases than physically delivered goods. According to one statistic, 7% of all attempts to purchase goods online are fraudulent.⁴⁶ This is due at least in part to the ease with which criminals can establish fictional identities using temporary e-mail accounts they set up by providing Internet service providers with stolen or counterfeit credit card numbers. From these aliases they order goods and request they be delivered to a mail drop or vacant house or, in the case of software, downloaded directly over the Internet. Once the criminal receives the product, he can cause the e-mail address to disappear without a trace. The result: The product is lost and the merchant is stuck with a bad debt, which is then passed on to bona fide consumers.

Forty-two percent of all attempted fraudulent online purchases involve attempts to purchase software.⁴⁷ This is because criminals can download software directly from the Internet, thereby eliminating the possibility of apprehension upon delivery. No signature is required upon receipt of goods in the virtual world, and no physical address is required for delivery, which is why the risk for online software merchants is appreciably greater.

3. Auction sales: Internet web sites are used to auction all types of merchandise, including antiques, new and used computer equipment, videos, and games. In many cases these items are never delivered or their value is overstated.⁴⁸ In one reported case, a consumer was the successful bidder for a computer hard drive and mailed a money order to the vendor. When the consumer received a damaged hard drive and tried to contact the vendor, he found that the vendor's e-mail account had been closed and his phone line had been disconnected.⁴⁹
4. Pyramid schemes attempt to imitate legitimate multilevel marketing or "network marketing" opportunities in that they may appear to offer a legitimate product or service for the victim to sell. Unlike a legitimate multilevel marketing operation, however, a pyramid scheme operates by generating fast cash through the recruitment of new participants into the scheme. Instead of focusing on generating sales and building a downline, the participant's only goal is to recruit.⁵⁰ The Internet facilitates this type of fraud by allowing the perpetrators to quickly reach millions of potential victims.⁵¹

Chain letters, which are closely related to pyramid schemes, offer the opportunity to make quick money by creating a chain in which other participants send the victim money. In the most simple versions, the victim receives an e-mail message via the Internet and is asked to send money to five persons on a list. The victim then adds his name to the list and waits for the cash to flow in. Like pyramid schemes, the main function is to recruit and generate cash, not to develop a legitimate business opportunity.⁵² In both types of scheme, the pyramid or chain eventually collapses when new participants are not recruited. When this happens, the last persons to buy into the scheme bear the loss of their investment – which can run into thousands of dollars – while the perpetrators of the scheme abscond with their fortunes intact.

5. Misrepresented on-line business opportunities and franchises: Examples of such frauds include purchases of ATM machines that will supposedly be leased back to the seller and generate profits for buyers; potential earnings that are misrepresented or unsubstantiated; and promised business assistance that is never provided.

One popular fraud in this category is the “travel-agent-in-a-box” fraud, which offers the victim instant certification as a travel agent upon payment of a hefty fee. The allure of this scam is the promise that the victim will be able to take advantage of special discount travel rates. What the scam does not disclose, however, is that most major airlines, hotels, and car rental agencies require that anyone claiming travel agent rates show a valid International Airline Travel Agent Network card on demand, and that to obtain such a card a travel agent must earn a minimum of \$7,000 in commissions (as opposed to sales) each year.

6. Work-at-home schemes: “Make Money Stuffing Envelopes!” Traditional work-at-home schemes, such as painting calendars or clipping news articles, share space on the Internet with modern versions offering the consumer the chance to “use your home PC to make money fast in your spare time.” Such scams promise the consumer large sums of money for doing simple tasks at home, but require the consumer to buy the materials from the fraudulent company in advance. When the consumer doesn’t, for example, paint calendars fast enough, he doesn’t make enough money to cover his costs. Alternatively, the fraudulent company requires the consumer to sell the calendars himself, but the market is so small that the consumer can never recoup his investment, much less turns a profit.⁵³

For example, Computer Business Services, Inc. (“CBSI”) marketed a home-based computer opportunity on the Internet by touting its “turnkey” business opportunity – a collection of computer hardware and software that cost investors between \$3,000 and \$16,000 – and claiming investors could “Earn \$4,000 Per Month From Your Home With A Computer!” CBSI represented that the hardware and software would enable the investor to provide a variety of services ranging from computerized monitoring for senior citizens to voicemail. In 1996, the Federal Trade Commission (“FTC”) brought suit against CBSI, alleging that its profits and earnings claims were deceptive and that most investors never earned close to \$4,000. In August 1996, CBSI agreed to a settlement which required it to pay \$5 million in consumer redress to FTC. In May 1997, however, CBSI declared bankruptcy, so the extent to which consumers will receive restitution is questionable.⁵⁴

Another common Internet fraud is the tracer program scam, which urges the victim to "Help Locate Money for People!" Tracer programs promise that the consumer can make money by finding lost assets, such as inactive bank accounts ceded to the state, and returning them to their rightful owners, often to discover that the clients are not willing to pay the fee but instead opt to contact the agency directly. The victim, of course, must pay a hefty fee himself for the report explaining where to look for the lost assets.⁵⁵

7. Prizes and sweepstakes: These include online contests that require consumers to pay a registration fee or require consumers to provide a bank account number before the "prize" can be obtained. For example, the consumer "wins" a free trip with the payment of a registration fee, but the consumer is required to buy a companion ticket at full price in order to use the free trip.⁵⁶
8. Credit card schemes offer Visas or MasterCard with a high credit line, sometimes in a fictitious name while promising minimal or no credit checks. These scams defraud the consumer through high fees or by requiring that the victim open a trust account with an offshore bank, where his funds are commingled with those of other victims and used for the personal benefit of the fraudster.
9. Books and other self-help guides: These types of scams offer the consumer manuals on how to hypnotize people, listings of celebrities' phone numbers and addresses, books on how to stop paying taxes, etc. After sending payment, the consumer never receives the book or guide.⁵⁷
10. Magazine subscriptions: Consumers receive offers from companies falsely representing themselves as subscription services for well-known magazine publishers or making false claims of discounts on magazine subscriptions. Consumers who take advantage of these offers then find their bank accounts debited multiple times for the magazines when in fact they authorized only one debit.⁵⁴

Two additional types of traditional fraudulent schemes are prominent on the Internet and merit brief notice. The first of these is health fraud. This type of fraud ranges from the promotion of unproven – and sometimes dangerous – alternative medical treatments to the sale of substandard or worthless medical devices. Because of its global nature, many products offered over the Internet may not comport with FDA standards, as the results of a Washington, DC, television station's investigation into home AIDS tests marketed over the Internet⁵⁹ revealed. The station purchased over the Internet a home AIDS test that claimed to determine whether a person is HIV positive by testing a saliva sample. With the assistance of a physician, the test was administered to an HIV positive volunteer. Although multiple tests were conducted, each result was either inconclusive or negative. Further investigation revealed that the test ordered came from the Bahamas, and had not been approved for use in the United States. In fact, the FDA has approved only two home AIDS tests for use in the United States, both of which require blood samples. Despite this restriction, at least nine home AIDS tests are available for purchase on the Internet.

Another online fraud worth noting is investment fraud. Stock and bond fraud is rampant in cyberspace. On September 22, 1997, the chairman of the United States Securities and Exchange Commission testified before the Permanent Subcommittee on Investigations that "the Internet is being used as a new vehicle to perpetrate securities fraud...because it provides anonymity, broad circulation and the appearance of legitimacy at low cost."⁶⁰ Promotions for exotic investments in ostrich farming, gold mining, and wireless cable television are prevalent, as are "pump and dump" promotions of penny stocks promising high returns. For example, one publisher of an Internet investing newsletter relentlessly promoted stock in a company called Systems of Excellence — without revealing that he held substantial shares of stock in the same company. The newsletter was posted all over Internet bulletin boards and promoted in chat rooms, causing the stock price to soar from \$0.27 to \$5.00 per share in a six-month period. The publisher earned about half a million dollars before the Securities and Exchange Commission halted trading of the stock. Subsequently, the publisher pled guilty to charges of conspiracy to commit securities and tax fraud.⁶¹

IV. The Internet as the Instrumentality of Traditional Fraud

In common law, "instrumentality" refers to the diversion of a lawfully possessed item to facilitate the commission of a crime⁶². In this category, the processes of the Internet facilitate the fraud,⁶³ which depends upon the use of the technology for its completion. This section will outline the types of technological devices and programs on which commission of such fraud relies.

Logic Bombs: A logic bomb is a destructive program that "detonates" upon the occurrence of a specific event, causing considerable damage to the targeted computer's programs or files. A "time bomb," for example, goes off at a particular time;⁶⁴ other bombs may detonate on a specific date.⁶⁵ As with other destructive programs such as viruses and worms, logic bombs are easily spread through the Internet when victims access Web sites or download files.

Mail Bombs: A mail or letter bomb is an electronic mail message which causes unexpected and harmful effects when the message arrives, is read, or is loaded into memory and executed. For example, one journalist was mail bombed with thousands of pieces of unwanted mail that jammed his mailbox and eventually shut down his Internet access on Thanksgiving weekend in 1994.⁶⁶ Mail bombs lobbed against an online retailer clog the victim's mailbox or jam his computer system.⁶⁷ This prevents the retailer from receiving e-mail from or responding to legitimate customers.⁶⁸

Sniffers are programs that monitor and record data of network users, such as their names and passwords when they log on. Armed with this information, the crook who installed the sniffer can impersonate an authorized user and log in to access information.⁶⁹ A sniffer can also pick up credit card numbers, which the installer can then use to purchase goods fraudulently.

Software Available Online: A plethora of software — much of it pirated and available for free on the Internet — was designed specifically to assist fraudsters in committing online crime. In one recent incident, three North Carolina teenagers downloaded from the Internet free software called "Credit Master," which replicates the algorithm, or mathematical sequence, banks use to assign credit card numbers. The teens created counterfeit credit card accounts using this software, then

used the phony numbers to purchase expensive electronic equipment they had delivered to vacant homes.

Spam is bulk electronic mail, or junk e-mail. See Exhibit 1 (examples of spam; some forwarded to PSI's e-mail address by consumers). Spammers sift through electronic discussion groups (such as chat rooms or bulletin boards), Web pages, member directories, and anything else they can find to amass as many addresses as possible,⁷⁰ usually by using software specifically designed to accomplish this task. Spam is an attractive advertising and marketing tool because it can reach literally millions of people in seconds and at very little cost to the sender. These same attributes, however, have rendered spam a tremendous problem on the Internet. First, while the cost of spam is minimal to the sender, Internet service providers ("ISPs") like America Online, CompuServe, and Prodigy bear the enormous cost of processing the spam. The recipients of spam also bear the cost of receiving, opening, and reading spam while they are online. Second, the sheer volume of spam clogs ISPs, thereby slowing down their ability to process other mail and provide fast Internet service. In some cases, spam has raised the level of traffic so high that it has crippled ISPs' systems.⁷¹ Finally, instead of providing true return e-mail address information, known as "headers," much junk e-mail contains forged headers, rendering it difficult if not impossible for a dissatisfied consumer or ISP to trace the culprit.⁷² For example, a company known as Cyber Promotions offers a program called the Cyber-Bomber, which promises to send bulk e-mail without the risk of account termination by the ISP. The program offers to fake the e-mail sender's address, hide the message path, and even alter the digital serial number -- which is all information contained in headers and necessary to trace the origin of spam.⁷³

For these reasons, spam has become its own worst enemy and, in the process, the target of at least two pending bills: The Murkowski bill, S. 771, which would require junk e-mail to be clearly marked as such for easy deletion, and the (Christopher) Smith bill, H.R. 1748, which would ban spam outright.

Spoofing: As mentioned below, *see infra* Sec. V, p. 13, anonymity is central to the Internet. Unfortunately, there is presently no good way for Internet users to authenticate each other's identity, even when they desire to do so. In other words, there is no sure fire way to make certain that when you order a shirt from Company X's Web site that you are in fact providing your credit card number to the real Company X; the site could be operated by an imposter. Likewise, Company X is unable to authenticate that you are the person whose name is on the credit card instead of an imposter.

In Internet vernacular, this type of impersonation or forging is called spoofing. In a spoofing attack, the fraudster creates a misleading context in order to trick the victim into making an inappropriate security-relevant decision. A spoofing attack is like a con game: The fraudster sets up a false but convincing world⁷⁴ around the victim. The victim does something that would be appropriate if the false world were real. Unfortunately, as the Company X example above illustrates, activities that seem reasonable in the false world may have disastrous effects in the real world.⁷⁵

There are several different types of spoofing. Web spoofing is a kind of electronic con game in which the fraudster creates convincing but false copies of Web sites. When a victim accesses the fraudster's Web site, every site he goes to after that is routed through the fraudster's site. The false Web sites created by the fraudster look just like the real ones; they have all the same pages and links. However, the fraudster controls the false Web sites, so that all network traffic between the victim's browser and the real Web is monitored by the fraudster.⁷⁶ See Exhibit 2 (diagram explaining Web spoofing).⁷⁷

Because the fraudster can observe or modify any data going from the victim to Web servers, as well as controlling all return traffic from Web servers to the victim, the fraudster has many options, including surveillance and tampering. Through surveillance, the fraudster can passively watch the traffic, recording which pages the victim visits and the content of those pages. When the victim fills out a form, the entered data is transmitted to a Web server, so the fraudster can record that too, along with the response sent back by the server. Since most online commerce is done via forms, this means the fraudster can observe and record any account numbers or passwords the victim enters.⁷⁸

The fraudster is also free to tamper with any of the data traveling in either direction between the victim and the Web. For example, if the victim is ordering a product online, the fraudster can change the product number, the quantity, and the ship-to address. The fraudster can also modify the data returned by a Web server by, for example, inserting misleading or offensive material in order to trick the victim or to cause antagonism between the victim and the server.⁷⁹

Another type of spoofing tricks the user's software into an inappropriate action by presenting misleading information to that software. Examples of such attacks include Transmission Control Protocol (TCP) spoofing, in which Internet packets are sent with forged return addresses, and Domain Name Server (DNS) spoofing, in which the fraudster forges information about which machine names correspond to which network addresses.⁸⁰

In a twist on this theme, five Los Angeles teenagers earlier this year sent "flash" messages to America Online subscribers impersonating AOL employees. The flash messages advised that a vengeful former employee had deleted thousands of credit card numbers from AOL's database.⁸¹ The message asked subscribers to provide their name, address, password, and credit card number. When the unsuspecting subscribers complied, the teenagers used the credit card numbers to purchase merchandise like sunglasses and compact discs over the Internet.⁸² The teens had the merchandise delivered to the house of a neighbor of one teen whose owner worked during the day. The teens picked up the merchandise from the front porch of the house, then sold it to their high school classmates. During a post-arrest interview, one of the teens reportedly stated that the group's leader justified the crime by reasoning that nobody was hurt by their activity, since the persons whose credit card numbers they had used would not be required to pay for the unauthorized charges. This rationale, of course, ignores the hassle the credit card holder must endure in order to clear up his credit report, as well as the monetary loss the credit card companies and merchants suffer, which is typically passed along to other consumers in the form of higher interest rates and prices.

Although presently there is no good way for Internet users to authenticate each other's identity, technology called digital signatures is being developed as a tool by which Internet users will be able to accomplish this. Use of a digital signature will allow the recipient to verify the true identity of a message's author. A digital signature acts like a packing list written in a secret code. Using a personal electronic "key," typically a string of numbers, a person sending a message creates an encoded list of information that is transmitted along with the message. The recipient opens the message and checks the contents. Then, using a separate "key" previously provided by the sender, the recipient tries to decode the digital signature. If the key works and the information about the content of the message is correct, the recipient can be certain of who sent the message and that it was not altered in transmission.⁸³

A Trojan horse is a program containing hidden malicious code.⁸⁴ A Trojan horse can, for example, automatically transfer money from a consumer's account to an illegal account whenever a legal transaction is made.⁸⁵ In one recent case, consumers visiting a Website were required to download a file in order to view sexually explicit photographs. Unbeknownst to the user, the downloading of the file caused a hidden Trojan horse to disconnect his Internet service provider and reroute his connection through the country of Moldova. The consumers, who were charged astronomical long-distance telephone rates for their Internet connections until they finally logged off,⁸⁶ generally remained unaware of the fraud until they received their monthly telephone billing statements reflecting the charges.

Viruses: A computer virus is a program that replicates itself and spreads through a computer system or network. Viruses may be benign or destructive; the latter variety may cause unexpected screen displays, delete computer files, create false information, or cripple a computer's ability to process information.⁸⁷ Some examples of viruses that have recently plagued the Internet include:

- "Michelangelo," which activates on March 6, the artist's birthday, and can wipe out the entire hard drive of a computer.⁸⁸
- "Gingrich," which randomly converts word processing files into legalese often found in contracts. Victims can combat this virus by typing their names at the bottom of infected files, thereby signing them, as if signing a contract.⁸⁹
- "Clipper," which scrambles all the data on a hard drive, rendering it useless.⁹⁰
- "Lecture," which deliberately formats the hard drive, destroying all data, then scolds the user for not catching it.⁹¹
- "Clinton," which is designed to infect programs, but eradicates itself when it cannot decide which program to infect.⁹²
- "SPA," which examines programs on the hard disk to determine whether they are properly licensed. If the virus detects illegally copied software, it seizes the computer's modem, automatically dials 911, and asks for help.⁹³

Viruses are activated whenever the boot sector or host file is loaded into a computer's memory and executed. They are spread from one computer to another through floppy disks and computer networks.⁶⁴ Viruses can be spread through the Internet when a victim downloads information from a Web site or from a file attached to an e-mail sent by the perpetrator. For those malcontent users who seek ready-made viruses, an Internet bulletin board in France has a large collection of diverse viruses that a perpetrator can download.⁶⁵

Viruses can wreak havoc on businesses as well as consumers. Whether introduced by a competitor, an unhappy former employee, or a disgruntled customer, a virus intended to impede commerce typically will cause major damage, such as erasing files, mixing information so that it makes no sense, or locking up hardware so that the system's software must be reloaded. In addition to these effects of the virus on the computer system, businesses sustain significant losses from secondary effects: The costs of virus eradication and system repair, operational slow-downs or even stoppages while the problem is being resolved, and undetermined losses of market share that might occur as a result of the problem.⁶⁶

Worms are active programs that spread through computer networks, potentially causing considerable damage. One of the most famous worms was launched on the Internet in 1988 by a graduate student at Cornell. The Internet worm eventually infected and shut down thousands of computers on the Internet.⁶⁷

V. Factors Contributing to Proliferation of Internet Fraud

Several aspects of the Internet merit particular attention because of the role they play in the proliferation of Internet fraud. One of these is interaction. Because the Internet is an interactive, low-cost medium, it is a more attractive means of communication than print, radio, television, or telephone for sellers of goods and services. As a result, consumers are required to make security-related decisions whenever they are faced with the option of divulging information over the Internet.

For example, on the Internet, a consumer can go to a retail store's Web page, view a shirt, decide to purchase it, and provide the seller with the information necessary to consummate the deal -- size and color of the shirt, name and credit card number of the buyer, shipping address -- without ever changing mediums. The consumer must weigh the benefits of divulging the information against the risk of an undesirable result, such as a breach of privacy or unauthorized tampering with data. Deciding to type in a credit card account number in order to purchase a shirt, despite the risk that the consumer may not receive the shirt, is one example of a security-relevant decision. Choosing to accept a downloaded document is also a security-relevant decision, since in many cases a downloaded document is capable of containing malicious elements that harm the person receiving the document.⁶⁸ See *supra* Sec. IV, p. 11 (describing Trojan horses).

Even the decision to accept the accuracy of information displayed by a computer connected to the Internet is security-relevant. For example, if the consumer decides to buy a stock based on information obtained from an online stock ticker, the consumer implicitly decides to trust that the

information provided by the ticker is correct. If somebody presents the consumer with incorrect stock prices, the consumer may engage in a transaction that he would not have otherwise made.⁹⁹

Another aspect of the Internet that plays a significant role in online fraud is context. A Web browser like Netscape Navigator or Microsoft Explorer presents many types of context on which users rely on to make decisions. For instance, the text and pictures on a Web page, including the presence of a corporate logo, might give the user the impression that the page originated at a certain corporation.¹⁰⁰ Likewise, neon green text on a purple background may give the user the idea that the Web page belongs to *Wired* magazine.¹⁰¹ The user recognizes particular graphical items, like file-open boxes, as having a certain purpose. Experienced Web users react to such cues in the same way that experienced drivers react to stop signs without reading them.¹⁰²

The names of objects may or may not convey their context. Users often incorrectly deduce what is in a file by its name. Is *manual.doc* the text of a user manual? It might be another kind of document, or it might not be a document at all. Web addresses are another example. Is *www.MICROSOFT.COM* the address of a large software company? For a while, that address led to a completely different entity. (By the way, the round symbols in *MICROSOFT* are the number zero, not the letter O.) Was *dole96.org* Bob Dole's 1996 presidential campaign? It was not; it pointed to a parody site.¹⁰³

Users often get context from the timing of events. If two things happen at the same time, a user may think they are related. For example, if the consumer clicks over to his bank's page and a dialog box appears that asks for a username and password, the consumer is likely to assume that he should type the name and password that he uses for online banking. If the user clicks on a link and a document immediately starts downloading, the user is likely to assume that the document came from the site whose link he accessed. Either assumption could be wrong.¹⁰⁴

Anonymity likewise plays an important role in the proliferation of fraudulent activity on the Internet. Anonymity is an integral part of the Internet culture. Every day, hundreds of people use the cloak of electronic anonymity to share their deepest secrets about childhood sexual abuse, alcoholism, rape, and other sensitive topics with sympathetic strangers on electronic bulletin boards or computer-network "chat rooms." The ability to send anonymous and untraceable messages can also shield political and religious dissidents, whistle-blowers, and human rights advocates from possible reprisals.¹⁰⁵ However, it raises significant problems in the sphere of criminal activity.

The most simple and common method of disguising one's identity in cyberspace is to use a "screen name" or pseudonym, but anyone with reasonable computer skills can trace this type of message to its source. It is also easy to sign up for an electronic mail service under an assumed name,¹⁰⁶ but this method likewise does not guaranty untraceable anonymity because of the ability to trace the path of electronic messages back to the computer from which they came.

Two methods of achieving anonymity are commonly used by cybercrooks: Hacking another person's e-mail account, and using anonymous remailers. The more technically sophisticated cybercrooks use hacked e-mail accounts to promote their schemes. Fraudsters can determine the

password to someone's e-mail account using a device known as a password sniffer, see supra Sec. IV, p. 9 (describing sniffers). They can also trick the user into divulging his password by technologically impersonating an employee of the user's ISP, see supra Sec. IV, p. 9 (describing spoofing). Once the crook obtains the user's password, he has access to the user's e-mail account, which he can then use to send fraudulent solicitations.

Anonymous remailers are free e-mail forwarding sites that convert return addresses to pseudonyms and render e-mail untraceable.¹⁰⁷ The result is e-mail messages that are routed without forwarding or preserving any identifiable header information about the sender.

To use an anonymous remailer, an individual sends a message to one of the estimated 20-25 remailers worldwide. The remailer accepts the incoming message, strips off all traces of the author's identity, assigns a new, randomly generated account number to the message, and retransmits the message to its destination, whether to a single electronic mail box or to thousands of addressees, or through a series of other remailers. Because the messages are remailed in a random sequence, different from the order in which they arrive, persons who may be monitoring the remailers cannot match the outgoing messages with the incoming messages to identify who sent which message.¹⁰⁸ The anonymous remailer maintains a record for a brief period during which it relays any responses to the originator. It then destroys the record of where the message came from. This process alone makes identification of the originator nearly impossible.

Another factor contributing to the success of Internet fraud is the prevalence of advertising on online services. Many Internet service providers charge their users a flat monthly rate for using the service, then sell advertising space -- sometimes indiscriminately -- to make up the difference. In the virtual world, as in the physical world, wherever a consumer finds a slew of advertisements, he is likely to find some false or misleading claims.

Yet another factor is the ease with which the Internet lends itself to "disguised" promotion of fraudulent schemes. Cybercrooks accomplish this primarily through the use (or, according to "netiquette" standards, *abuse*) of "bulletin boards" and "chat rooms," which are online areas fertile for fraud in disguise. The Internet and the commercial online services provide bulletin boards, or areas on the Internet where running conversations are posted, allowing anyone to read and reply to any message.¹⁰⁹ Bulletin boards allow interested parties to exchange information in general topic areas, such as baseball, cats, or investing. In some cases, individuals contributing to the bulletin board have financial ties to companies or businesses that sell products or services related to the bulletin board subject area. This may not be obvious to the online user. What may appear to be an open discussion is sometimes a sales pitch in disguise. Because the identities or affiliations of online bulletin board operators and participants are frequently known, and may be difficult to discern, it is difficult to detect disguised advertising.¹¹⁰

Some commercial online services also provide live discussion groups called "chat rooms" or "chat forums." Service subscribers "drop in" for an online, "real time" conversation by typing in their comments, generally while using an online pseudonym. These forums provide the chance to discuss a variety of subjects, including products and services. Accordingly, marketers -- and

fraudsters -- have used these chat rooms to promote their products without disclosing their interests.¹¹¹

Finally, one of the most significant factors leading to the proliferation of Internet fraud is the fact that the adults of today's society are the first generation of modern Internet users. Every day, more persons access the Internet to conduct research, surf the Web, or post messages on bulletin boards. However, because the Internet is a relatively new medium, even persons who are otherwise "street smart" find themselves at a disadvantage when it comes to recognizing some of the more subtle scams on the Internet. In frauds in which the Internet is used as a tool, the risk of a consumer failing to recognize a fraudulent scheme is even greater, given the minimal technological skills necessary to become an Internet user.

VI. Legal and Practical Issues

A number of state and federal criminal laws cover fraudulent activities on the Internet. Federal laws include the Computer Fraud and Abuse Law of 1984, the Electronic Communications Privacy Act of 1986, and mail and wire fraud statutes. State laws include computer crime statutes and expansion of the traditional concept of property to include electronic and computer technologies. See Appendix I (describing state and federal criminal laws targeting Internet fraud).

The Internet presents unique challenges that law enforcement will have to overcome in order to cope with the present and future proliferation of online fraud. For example, the physical act of a computer-related fraud, or the *actus reus*,¹¹² may be demonstrated best by an electronic impulse that, unfortunately, is difficult to define and track, considering that a computer crime can occur in three milliseconds using a program code that tells the software to erase itself after the computer executes the action. This essentially eliminates the evidentiary trail. It also hampers the establishment of the element of causation: How can an investigator show causation if the offender erases the executing instructions?¹¹³

Another consideration is venue, which is the question of which court shall hear a specific legal action. Venue over a criminal prosecution, for example, generally lies with a court in the geographic location where the offense was committed.¹¹⁴ In many cases, however, an offense is deemed to have occurred where any act performed in furtherance of the offense occurs, where the victim's residence or principle place of business is located, or (in the case of computer crime) where an unlawfully accessed computer system is located. To alleviate this confusion, some state laws include provisions specifying where venue shall lie in such cases.¹¹⁵

The multi-venue case highlights a related issue, which is the need for law enforcement coordination. The speed with which an individual can cross interstate or international boundaries to commit fraud on the Internet raises yet another concern for law enforcement: Investigative coordination. Since a cybercrook can quickly move from state to state, and from country to country, many different victims may, in short order, be reporting intrusions to federal and local authorities, thus leading to parallel investigations. At the federal level alone, multiple agencies -- including the FBI, Secret Service, and FTC -- may have jurisdiction over the same federal offense. In such

circumstances, there is always the risk that investigators from the different agencies may unnecessarily duplicate efforts or, even worse, inadvertently interfere with one another.¹¹⁶ See Appendix II (describing federal, state, and local agencies sharing jurisdiction over Internet fraud).

Likewise, the global nature of the Internet renders fraud committed thereon a worldwide problem calling for an organized international response. As on the domestic front, Internet fraud differs from traditional international crimes. First, it is easier to commit: No borders to cross, minimal human effort involved, and a greatly reduced chance of apprehension. Second, Internet fraud has received far less attention than other international crimes. For an international program to be effective, the nations involved must recognize that the criminal conduct in question poses a domestic threat and that international cooperation is necessary to respond effectively to the problem.

The United Nations has called upon its member states to consider modernizing their criminal laws to combat computer crime. However, such crimes must be perceived as sufficiently serious before they are included in existing international agreements that are primarily focused on war crimes and terrorism. In the United States, one of the most heavily computerized nations in the world, our society has not until recently mobilized against computer criminals. It is thus not surprising that other, less computerized nations have not yet joined in our chorus of concern.¹¹⁷

VII. Conclusion

Given the prediction that Internet fraud will rise dramatically with the corresponding increase of consumer use of the Internet, we seek to accomplish two goals through this investigation and the presentation of its results at the first hearing. Our first goal is that of consumer education. Today's society of consumers is the first generation of modern Internet users and are not as technologically savvy as future generations will be. While the Internet holds great potential for commerce and communication, the relatively few bad apples that roam rampant in cyberspace cause consumers to shy away from using the Internet to its full potential much to the dismay of potential and actual online businesses. Consumers must be armed with the knowledge of how to detect online fraud, and must know where to report it when they encounter it.

Our second goal is that of determining the federal government's proper role in preventing and enabling the prosecution of online fraud, and how that role complements or duplicates state government and consumer protection efforts. Because the Internet is still a relatively new technology, and because nobody is yet certain of all the implications of conducting business in cyberspace, Congress must approach its role with caution. The need to control fraud must be balanced with the economic benefits that will certainly come from the enormous growth of commercial activities on the Internet. The appropriate question to ask is not what regulations to impose, but indeed to what extent regulation is appropriate given the changing nature of the use of the Internet and the technology that enables online commerce.

RJ/DM/JN:mdr
M:\PS\INTERNET\MEMOS.98\BRIEFING.STF

- ¹ Stephen M. Rosoff, Henry N. Pontell, and Robert Tillman, Computer Crime: Hackers, Phreaks, and Cyberpunks, at 389 (citing Gabriel Tarde, The Laws of Imitation (1903)).
- ² Id.
- ³ Criminal/Civil Rights Subcomm., Internet Working Group, Nat'l Ass'n of Attorneys Gen., The Internet and Crime: A Report to the Internet Working Group of the National Association of Attorneys General 2 n.1 (June 1997) (hereinafter "NAAG Internet and Crime Report") (citing Fed. Communications Comm'n).
- ⁴ Hoffman, Novak, and Kalsbeek, Internet and Web use in the United States, at 2 (visited Jan. 28, 1998) <<http://www2000.ogsm.vanderbilt.edu/baseline/internet.demos.july9.1996.html>>.
- ⁵ Id. at 8.
- ⁶ NAAG Internet and Crime Report, supra n. 3, at 2 n.1.
- ⁷ U.S. Gen. Accounting Office, Payments, Clearance, and Settlement 131 (June 1997).
- ⁸ Id.
- ⁹ Tom Murphy, Internet Commerce Still Years Away, Stuart News/Port St. Lucie News, Dec. 8, 1996, at E2.
- ¹⁰ Robert Bowden, Apple Takes a Bad Financial Bite Entering '97, Tampa Tribune, Jan. 7, 1997, at Business 5. According to one report, however, even if retail Internet commerce reaches \$7.2 billion by 2000, it will only comprise 4% of all retail sales. See Elizabeth Corcoran, What Intuit Didn't Bank On, Wash. Post, Jun. 22, 1997, at H5 (graphic; survey by Forrester Research).
- ¹¹ See NAAG Internet and Crime Report, supra n. 3, at 2 (citing Fed. Communications Comm'n).
- ¹² The Computer Emergency Response Team Coordination Center was established by the Software Engineering Institute at Carnegie Mellon University in 1988 to respond to computer emergencies on the Internet, to serve as a central point for identifying vulnerabilities, and to conduct research to improve the security of existing systems. The center is supported by the Defense Advanced Research Projects Agency, the National Science Foundation, and other federal agencies.
- ¹³ Scott Charney & Kent Alexander, Computer Crime, 45 Emory L.J. 931, 935 & n.10 (1996) (based on 1994 statistics).
- ¹⁴ Black's Law Dictionary 337 (5th ed. 1983).

- ¹⁵ See Xan Raskin & Jeannie Schaldach-Paiva, Eleventh Survey of White Collar Crime: Computer Crime, 33 Am. Crim. L. Rev. 541, 543 (1996) (citing National Institute of Justice, U.S. Dep't of Justice, Computer Crime: Criminal Justice Resource Manual 2 (1989)).
- ¹⁶ A third type of Internet fraud occurs when the computer becomes the target of the fraud. Our second hearing on Internet fraud will focus on fraud committed by the invasion of electronically maintained databases, or "hacking." Discussion of this type of crime is thus outside the scope of the first hearing.
- ¹⁷ See NAAG Internet and Crime Report, supra n. 3, at 2.
- ¹⁸ The World Wide Web is a cross-section of the Internet consisting of all the resources that can be reached by means of certain Internet protocols. Christian Crumlish, The Internet for Busy People 9 (1996). In less technical terms, the Web is a way of communicating words, pictures, and sound on the Internet. Information on the Web is organized into "pages" that are much like the pages of a magazine. Daniel J. Barrett, Bandits on the Information Superhighway 10 (1996)
- ¹⁹ See NAAG Internet and Crime Report, supra n. 3, at 2.
- ²⁰ "FTP" is a method for sending and receiving files quickly between computers connected to the Internet. "Telnet" is a protocol that was devised for UNIX computers, long before computers were using Windows software, to log into remote computers on the Internet. "Gopher," which preceded the World Wide Web, organizes Internet connections into menus or directory listings. It is similar to the World Wide Web except it contains only text, see Daniel J. Barrett, supra n.18, at 5 (1996), and does not have page formatting or hyperlinks. See Christian Crumlish, supra n. 18, at 176.
- ²¹ NAAG Internet and Crime Report, supra n. 3, at 3.
- ²² Id. A browser enables a user to navigate from Web page to Web page using a convenient point-and-click user interface. See Daniel J. Barrett, supra n. 18, at 10. Examples of Internet browsers include Netscape Navigator and Microsoft Explorer.
- ²³ NAAG Internet and Crime Report, supra n. 3, at 3.
- ²⁴ Id.
- ²⁵ Id.
- ²⁶ Christian Crumlish, supra n. 18, at 5.
- ²⁷ Id.

- ²⁸ Amy Harmon, Internet Group Challenges U.S. Over Web Addresses, N.Y. Times, Jan. 26, 1998.
- ²⁹ Id. at 121.
- ³⁰ Id. at 122.
- ³¹ Daniel J. Barrett, supra n. 18, at 8-9.
- ³² The ultimate authority rests with the Internet Society ("ISOC"), a voluntary membership organization whose purpose is to promote global information exchange through Internet technology. ISOC appoints an executive board called the Internet Architecture Board ("IAB"), which has responsibility for the technical management and direction of the Internet. IAB develops standards by which computers and software applications can communicate. The second group is the Internet Engineering Steering Group ("IESG"), which works with IAB to coordinate the work of the third group, the Internet Engineering Task Force ("IETF"), a volunteer organization that meets regularly to discuss technical problems. The fourth group is the Internet Assigned Numbers Authority, which deals with Internet addressing matters under a contract from DOD and the University of Southern California Information Sciences Institute. See NAAG Internet and Crime Report, supra n. 3, at 32.
- ³³ Id.
- ³⁴ Setting up a Web site on the Internet is easy and can be inexpensively done through an Internet service provider. See Christian Crumlish, supra n. 18, at 228.
- ³⁵ See August Bequai, Prosecuting Cyber-Crimes, Computer Audit Update, Apr. 1996, at 22, 23.
- ³⁶ Christine Milliken, Office of the State Attorney General and Cyberspace 9 (1997) (unpublished manuscript, on file with the National Association of Attorneys General).
- ³⁷ David L. Carter, Computer Crime Categories: How Techno-Criminals Operate 3-4 (July 1995) (unpublished manuscript, on file with Michigan State University School of Criminal Justice).
- ³⁸ NAAG Internet and Crime Report, supra n. 3, at 19.
- ³⁹ Web Watch Against Cybercrooks Unveiled by Consumers League, Balt. Sun, Sept. 11, 1997.
- ⁴⁰ Internet Exploited to Rip Off Consumers, Wash. Times, Sept. 11, 1997.
- ⁴¹ Fraud Watch Consumer Information (visited Sept. 23, 1997) <<http://www.fraudnewsletter.com/info.html>>.

- ⁴² National Consumers League: Top 10 Internet Frauds for 1997 (visited Oct. 3, 1997) <<http://www.natlconsumersleague.org/top10.htm>>.
- ⁴³ See, e.g., Internet Consumer Fraud Information Service (visited Sept. 23, 1997) <<http://www.geocities.com/SiliconValley/Vista/9765/fraud.html>> (warning of Malaysian group buying lasers over Internet using stolen credit cards).
- ⁴⁴ See, e.g., Bad Traders on the Net (last modified Sept. 7, 1997) <<http://www.localnet.com/~theedge/badtrade.html>>.
- ⁴⁵ Fraud Watch Consumer Information, *supra* n. 41.
- ⁴⁶ Lee Hawkins, Jr., Security Firms See Opportunity in Crime, Milwaukee Journal Sentinel, Mar. 17, 1997, at Business 7 (citing John Pettitt, spokesman for CyberSource Corp.).
- ⁴⁷ Id.
- ⁴⁸ National Consumers League: Top 10 Internet Frauds for 1997, *supra* n. 42.
- ⁴⁹ National Consumers League: Sample E-Mails from Consumers Who Have Been Internet Fraud Victims (visited Oct. 3, 1997) <<http://www.natlconsumersleague.org/ifwmail.htm>>.
- ⁵⁰ Fraud Watch Consumer Information, *supra* n. 41.
- ⁵¹ Barry Wise, who will testify at our February 10 hearing, was the victim of an elaborate Internet fraud scheme known as Fortuna Alliance.
- ⁵² Fraud Watch Consumer Information, *supra* n. 41.
- ⁵³ Nancy Tamosaitis, Cyberspace Scams: How to Avoid Info Highway Robbery, Home PC, May 14, 1997 (quoting Daniel J. Barrett).
- ⁵⁴ Fraud Watch Newsletter (visited Sept. 24, 1997) <<http://www.fraudnewsletter.com/1June97/html>>.
- ⁵⁵ Fraud Watch Consumer Information, *supra* n. 41.
- ⁵⁶ National Consumers League: Top 10 Internet Frauds for 1997, *supra* n. 42.
- ⁵⁷ Id.
- ⁵⁸ Id.

- ⁵⁹ The results of this investigation were broadcast on June 17, 1997, by WBRC-TV, the Washington, DC, affiliate of the National Broadcasting Company, during its "News 4 at 4:00" broadcast.
- ⁶⁰ Hearing on Fraud In the Micro-Capital Markets, Including Penny Stock Fraud Before the Permanent Subcomm. on Investigations of the Senate Comm. on Governmental Affairs, 105th Cong., 1st Sess. (Sept. 22, 1997) (statement of Arthur Levitt, Chairman, U.S. Securities and Exchange Commission).
- ⁶¹ Leslie Eaton, Fraud Case Focuses on Internet, N.Y. Times, Sept. 14, 1997, at 5, col. 1.
- ⁶² David L. Carter, supra, n. 37 at 3.
- ⁶³ Id.
- ⁶⁴ Id.
- ⁶⁵ Xan Raskin & Jeannie Schaldach-Paiva, supra n. 15 at 543 n.13.
- ⁶⁶ Dorothy E. Denning, Crime and Crypto on the Information Superhighway, Journal of Criminal Justice Education (Spring 1995).
- ⁶⁷ Vic Sussman, Policing Cyberspace, U.S. News & World Report, Jan. 23, 1995, at 55, 58 (citing FBI Special Agent William Tafoya).
- ⁶⁸ Peter H. Lewis, Computer Jokes and Threats Ignite Debate on Anonymity, N.Y. Times, Dec. 31, 1994, at 1.
- ⁶⁹ Crime on the Internet (visited July 25, 1997)
<<http://www.digitalcentury.com/encyclo/update/crime.html>>.
- ⁷⁰ Thomas E. Weber, The Three Most Dreaded Words in Cyberspace? 'You've Got Mail!', Wall St. J., Oct. 2, 1997, at B1.
- ⁷¹ See Junk Mailer Cyber Gains Short Reprieve From Internet Cutoff, Wall St. J., Oct. 2, 1997.
- ⁷² Fraud Watch Newsletter, supra n. 50; see also Peter G. Neumann & Lauren Weinstein, Spam, Spam, Spam! Unsolicited Electronic Mail Advertisements, Communications of the Ass'n for Computing Machinery, Inc., June 1997, at 112.
- ⁷³ Fraud Watch Newsletter, supra n. 54.
- ⁷⁴ Crime on the Internet, supra n. 69.

⁷⁵ Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach, Web Spoofing: An Internet Con Game (visited Aug. 8, 1997) <<http://www.geocities.com/CapeCanaveral/3498/spoofing.html>>.

⁷⁶ Id.

⁷⁷ Id.

⁷⁸ Id.

⁷⁹ Id.

⁸⁰ Id. (footnotes omitted).

⁸¹ See L.A. Times, Apr. 12, 1997.

⁸² In a similar case, Sprint recently warned the customers of its Internet service, Sprint Internet Passport, that someone was disseminating fraudulent e-mail messages in an effort to persuade on-line computer users into giving out their credit card numbers.

⁸³ Peter H. Lewis, supra n. 68.

⁸⁴ Dorothy E. Denning, supra n. 66.

⁸⁵ Stephen M. Rosoff, Henry N. Pontell, & Robert Tillman, Computer Crime: Hackers, Phreaks, and Cyberpunks, at 389, 391 (citing, Robert L. Perry, Computer Crime (1986)).

⁸⁶ NAAG Internet and Crime Report, supra n. 3, at 20.

⁸⁷ Xan Raskin & Jeannie Schaldach-Paiva, supra n. 15, at 543 n.12 (citing Camile Cardoni Marion, Computer Viruses and the Law, 98 Dick. L. Rev. 625, 627 (1989)).

⁸⁸ Fighting Computer Viruses' Insidious Spread, USA Today, Mar. 6, 1997.

⁸⁹ Carter & Katz, Computer Crime: The Emerging Challenge for Law Enforcement, FBI/Law Enforcement Bulletin, December 1996, at 1, 5.

⁹⁰ Id.

⁹¹ Id.

⁹² Id.

⁹³ Id.

- ⁹⁴. Dorothy E. Denning, supra n. 66.
- ⁹⁵. Carter & Katz, supra n. 89, at 5.
- ⁹⁶. Id. at 6.
- ⁹⁷. Dorothy E. Denning, supra n. 66.
- ⁹⁸. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach, supra n. 75.
- ⁹⁹. See id.
- ¹⁰⁰. Id.
- ¹⁰¹. *Wired* magazine covers the impact of technology on business, culture and life. It also has a Web site, <<http://www.wired.com>>, that contains a selection of its monthly magazine articles and offers links to other sites of interest.
- ¹⁰². Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach, supra n. 75.
- ¹⁰³. Id.
- ¹⁰⁴. Id.
- ¹⁰⁵. Peter H. Lewis, supra n. 68; see, e.g., Matthew McAllester, Democracy of Internet Threatens Some Nations, *Phil. Inq.*, Nov. 20, 1997.
- ¹⁰⁶. Peter H. Lewis, supra n. 68.
- ¹⁰⁷. Vic Sussman, supra n. 67.
- ¹⁰⁸. Peter H. Lewis, supra n. 68.
- ¹⁰⁹. Christian Crumlish, supra n. 18, at 260.
- ¹¹⁰. Stephen Barrett, M.D., Online Scams: A Message from the Federal Trade Commission (visited Sept. 23, 1997) <<http://www.quackwatch.com/02ConsumerProtection/onscam.html>> (citing Federal Trade Comm'n).
- ¹¹¹. Id.
- ¹¹². The *actus reus* is the "guilty act" or the physical component of a criminal act. For example, in burglary, the *actus reus* is the physical act of breaking into the dwelling of another. See Barron's Law Dictionary 9 (2nd ed. 1984).

¹¹³ David L. Carter, *supra* n. 37, at 5-6.

¹¹⁴ Black's Law Dictionary 806 (5th ed. 1983).

¹¹⁵ See, e.g., Ark. Code Ann. § 5-41.105 (Michie 1993); Del. Code Ann. tit. 11, § 938 (1995); Ga. Code Ann. § 16-9-94 (1992); Ky. Rev. Stat. Ann. § 434.860 (Michie/Bobbs-Merrill 1985); Miss. Code Ann. § 97-45-11 (1994); N.H. Rev. Stat. Ann. § 638.19 (1986); S.C. Code Ann. § 16-16-30 (Law. Co-op. 1985); S.D. Codified Laws Ann. § 43-43B-8 (Supp. 1995); Tenn. Code Ann. § 39-14-603 (1991); Va. Code Ann. § 18.2-152.10 (Michie 1988 & Supp. 1995); W. Va. Code § 61-3C-18 (1992).

¹¹⁶ Scott Charney & Kent Alexander, *supra* n. 13, at 947.

¹¹⁷ *Id.* at 948-49.

EXHIBIT #1

Author: Varda Ullman Novick <vnovick@netcom.com> at internet
Date: 10/9/97 9:44 AM
Priority: Normal
TO: psi at Governmental-Affairs
Subject: IF YOU KNOW SOMEONE WHO HAS CANCER..... (fwd)

----- Message Contents -----
[A friend received this and asked me to forward it to you]

----- Forwarded message -----
Return-Path: <05111630@usa.net>
Received: from nsl.hgo.net (nsl.hgo.net [206.152.112.1])
by mail5.netcom.com (8.8.5-r-beta/8.8.5/(NETCOM v1.01)) with ESMTF id
VAA06286; Wed, 8 Oct 1997 21:05:33 -0700 (PDT)
From: 05111630@usa.net
Received: from hgo.net (ts010d10.hil-ny.concentric.net [206.173.18.118])
by nsl.hgo.net (8.8.7/8.8.7) with SMTP id XAA29619;
Wed, 8 Oct 1997 23:59:37 -0400 (EDT)
Received: from mailhost@nowhere.com by nowhere.com (8.8.5/8.6.5) with SMTP
id GAA01464 for <>; Wed, 08 Oct 1997 22:55:33 -0600 (EST) Date: Wed, 08 Oct
97 22:55:33 EST To: Friend@public.com Subject: IF YOU KNOW SOMEONE WHO HAS
CANCER..... Message-ID: <12345@greatmail.com> Reply-To:
MichaelVala@hotmail.com Comments: Authenticated sender is
<hooray@anywhere.com> X-UIDL: 586950631010ab7890bbc43189182cvt X-PMFLAGS:
35651712 0

From: 05111630@usa.net
Date: Wed, 08 Oct 97 22:55:33 EST
To: Friend@public.com
Subject: IF YOU KNOW SOMEONE WHO HAS CANCER.....
Reply-to: MichaelVala@hotmail.com

Pardon my intrusion, I am searching for anyone
who either has, or knows someone with cancer. It
does not matter what kind of cancer. I sell a prod-
uct that cures any type of cancer. I offer to every-
one my website url which will give the scientific
data people need to cure themselves of cancer. My
website is: <http://www.godscancerfruit.com>
IF YOU HAVE NO NEED FOR THIS INFORMATION,
PLEASE PASS IT ON TO SOMEONE
WHO DOES! Thanks and have a great day!

Gregg Moore
PRESIDENT
CANCER KILLERS, INC
334-649-4480 PHONE
FAX 334-649-4480
8880 EASTWOOD DRIVE
SEWMEES, ALABAMA 36575

Author: bashley@ktb.net at internet
 Date: 9/30/97 9:37 PM
 Priority: Normal
 TO: psi at Governmental-Affairs
 Subject: GET PAID \$300.00 FOR GIVING AWAY TWO WAY HOME SECURITY SYSTEMS

----- Message Contents -----

Mailspam like this defrauds everyone. I hope this is the sort of stuff you're interested in and hope to eliminate.

Bev

 Horn broken. Watch for finger.

----- Forwarded message -----
 Return-Path: <gohoisa54@sprintmail.com>
 Received: from mailgate22 (mailgate22-hms0.a001.sprintmail.com [205.137.196.54])
 by ktb2.ktb.net (KTBNET-2.0) with SMTP
 id VAA09478 for <bashley@ktb2.ktb.net>; Tue, 30 Sep 1997 21:02:29 -0700
 Received: by mailgate22 (SMI-8.6/SMI-SVR4)
 id UAA09191; Tue, 30 Sep 1997 20:57:05 -0700
 Date: Tue, 30 Sep 1997 20:57:05 -0700
 Received: from sdn-ts-002caventp16.dialup.sprint.net(206.133.242.51) by
 mailfep4-hmel via smap (KCS.24)
 id Q_10.1.1.10/Q_15407_1_3431ca05; Tue Sep 30 20:56:53 1997
 To: V.I.P.#OnTheMet.com
 From: gohoisa54@sprintmail.com (James)
 Comments: Authenticated sender is <gohoisa54@sprintmail.com>
 Subject: GET PAID \$300.00 FOR GIVING AWAY TWO WAY HOME SECURITY SYSTEMS!!!
 Message-Id: <199709302424DAA34109@post.a001.sprintmail.com>

For removal, please put remove on subject line and email me at
 Success@Gosnet.com
 *Don't press reply, it won't get back to me. Follow instructions
 down below.

-How would you like to get paid \$300.00 for giving
 away a two way home security system valued at
 \$1,320.00. This system gives you so many options it is
 incredible.

-How would you like to get paid \$140.00 to \$280.00 for each two
 way home security system that your down line gives away.

-This opportunity is available now in your area. The only
 cost to start this incredible opportunity is a \$94.00 start up kit.
 This includes your activation, home security(2 systems) , shipping,
 and handling fees.

DON'T REPLY WITH YOUR REPLY BOTTOM
 TO OBTAIN INFO ON THIS OPPORTUNITY:
 1)Email me at user2384@xsend.com
 -Please include name, PHONE #, and email address. Please include
 phone#!!!!!!!!!!!!
 -Please put *MORE INFO* ON SUBJECT LINE, if you don't the reply will take
 longer.
 3)If email comes back undeliverable please leave message
 at (805)675-8565.

Subj: Hello
Date: 97-10-25 20:37:29 EDT
From: Donald@juno.com
Reply-to: John552@sid.com
To: Donald@juno.com

Hello!

Do you want to:

- >Legally slash your personal/business taxes dramatically?
- >Protect any & all assets from any form of judgment?
- >Learn how to preserve your personal privacy?
- >Create a 6 figure income in the next 4-6 months?

For more information, please call [REDACTED]

My name is Gary and I was introduced to this awesome information just like you. This is not new information. It has been used by the ultra wealthy for decades to make millions and to increase their wealth. This information is so powerful that it allows anyone to earn a six figure income within only a few months. My job is to get you the information on how the business works. Your job is to take the time to get all the information that will ensure your business success. Take control of your own personal finances. I will talk to you soon. Gary

If you don't know:

- >how to make your money work 3-5 times harder for you?
- >how to set up off shore trusts and protect your owned personal property from liens and levies and seizures?
- >how to legally shelter assets from Taxes?
- >how to make a six figure income from home?

[REDACTED]

If you are tired of multi- level marketing that:

- >promises support but doesn't deliver.
- >only gives small percentages of earnings.
- >90% of your line disappears after 1 month.
- >product is hard to market.

Our business has:

- >100% team support.
- >100% satisfaction guarantee on own product.
- >90% commission to all directors
- >100% exclusive marketing rights to our product.
- >a plan to be financially secure in 24 months.
- >a product that every American and Canadian needs.
- >a system that is not multi-level marketing.

Leave your name and phone number. Twice and I or one of my associates will call you. (your address is not necessary)

If your skeptical, that's okay. So was I, but don't let that stop you from getting all the information so you can make a relaxed and intelligent decision about this opportunity.

Lets stop:

- >working for a job that we really don't care for.
- >working for people who don't care about our needs.
- >working 3 months out of every year just to pay our taxes.
- >working away from home.
- >worrying about cut backs and down sizing.
- >giving the proceeds of our labor to someone else.

Isn't time to change your financial situation around and start enjoying life?

Call the toll free number [REDACTED] today.

(I promise that there will be no pressure on your part to join us)

----- Headers -----
Return-Path: <Donald@juno.com>
Received: from mri83.mail.aol.com (mri83.mail.aol.com [152.163.116.121]) by air14.mail.aol.com (x05) with SMTP; Sat, 25 Oct 1997 20:37:29 -0400
Received: from Internet-Aid.com ([199.44.173.3])
by mri83.mail.aol.com (8.8.5/8.8.5/AOL-4.0.0)
with SMTP id UAA26442;
Sat, 25 Oct 1997 20:36:56 -0400 (EDT)
From: Donald@juno.com
Received: from [153.37.147.192] by Internet-Aid.com
(SMTPD32-4.0) id A0661180076; Sat, 25 Oct 1997 20:35:50 -0400
To: Donald@juno.com
Comments: Authenticated sender is <Donald@juno.com>
Reply-to: John552@sid.com
Subject: Hello
Message-Id: <199710253464JAA55425@post.com>
Date: Sat, 25 Oct 97 20:36:25 EST EDT

EXHIBIT #2

How the Attack Works

The key to this attack is for the attacker's Web server to sit between the victim and the rest of the Web. This kind of arrangement is called a "man in the middle attack" in the security literature.

URL Rewriting

The attacker's first trick is to rewrite all of the URLs on some Web page so that they point to the attacker's server rather than to some real server. Assuming the attacker's server is on the machine `www.attacker.org`, the attacker rewrites a URL by adding `http://www.attacker.org` to the front of the URL. For example, `http://home.netscape.com` becomes `http://www.attacker.org/http://home.netscape.com`. (The URL rewriting technique has been used for other reasons by two other Web sites, the Anonymizer and the Zippy filter. See page 9 for details.)

Figure 1 shows what happens when the victim requests a page through one of the rewritten URLs. The victim's browser requests the page from `www.attacker.org`, since the URL starts with `http://www.attacker.org`. The remainder of the URL tells the attacker's server where on the Web to go to get the real document.

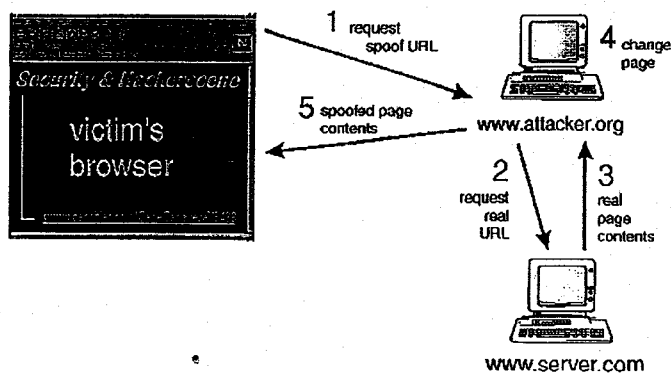


Figure 1: An example Web transaction during a Web spoofing attack. The victim requests a Web page. The following steps occur: (1) the victim's browser requests the page from the attacker's server; (2) the attacker's server requests the page from the real server; (3) the real server provides the page to the attacker's server; (4) the attacker's server rewrites the page; (5) the attacker's server provides the rewritten version to the victim.

APPENDIX #1

APPENDIX I
State and Federal Criminal Laws Targeting Computer Crime

I. **Federal**

Several federal statutes cover acts fitting within the realm of Internet fraud.

A. **Mail and Wire Fraud**

Most Internet fraud cases can be prosecuted under the federal mail and wire fraud statutes,¹ which prohibit using interstate mail and wire communications to further a fraudulent scheme to obtain money or property. These statutes apply to “any computer-aided theft involving the use of interstate wire, the mails or a federally insured bank.”² The federal mail and wire fraud statutes apply to intangible as well as tangible property.³ Cases: United States v. Briscoe, 65 F.3d 576 (7th Cir. 1995) (fraudulent transfer of funds through computer system violates wire fraud statute); United States v. Slusher, 1995 WL 417077 (S.D.N.Y. 1995) (exchange of DMV license approval for bribes through DMV’s computer terminals constitutes violation of wire fraud statute).

B. **Computer Fraud and Abuse Law of 1984 & Computer Abuse Amendments Act of 1994**⁴

This is what is commonly referred to as the federal computer crime statute. While most of its provisions address unauthorized access to electronically maintained databases, several provisions address Internet fraud. Section 1030(a)(5) criminalizes acts that prevent “authorized use” of a computer, which apparently extends to denial of service schemes. The aspect of the crime that triggers federal jurisdiction is that the act must be committed on a computer used in interstate commerce or communications, and must affect another computer.

Section 1030(a)(5) also criminalizes certain types of reckless conduct as misdemeanors, which may facilitate prosecution of hackers who cause the transmission of malevolent software, such as computer viruses.⁵

Section 1030(a)(6) prohibits knowingly, and with intent to defraud, trafficking in

¹18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud) (1994).

²Xan Raskin & Jeannie Schaldach-Paiva, Eleventh Survey of White Collar Crime: Computer Crime, 33 Am. Crim. L. Rev. 541, 564 (1996) (quoting Stanley S. Arkin et al., prevention and Prosecution of Computer and Technology Crime, 3-33 (1991)).

³See 18 U.S.C. § 1346 (1994).

⁴See 18 U.S.C. § 1030 (1994).

⁵See 18 U.S.C. § 1030(a)(5)(B)(i) (1994).

passwords which either would affect interstate commerce. This provision would address the collection and subsequent distribution of passwords collected by sniffers.

C. Electronic Communications Privacy Act of 1986⁶

The ECPA updated the federal law pertaining to wire and electronic communications interception to prohibit unauthorized interception of computer communications. It is not clear, however, which provisions of the ECPA cover electronic communications such as e-mail, which is both transmitted and stored. See, e.g., Steve Jackson Games, Inc., v. United States Secret Serv., 36 F.3d 457, 458 (5th Cir. 1994) (government seizure of computer used to operate electronic bulletin board and containing private electronic mail that had been sent to and stored on bulletin board, but not read by intended recipient, was not "interception").

II. State

States have sought to address Internet fraud by expanding the scope of their computer crime statutes.⁷ For example, some states have expanded the traditional concept of property to include electronic and computer technologies.⁸ Other states have enacted "aiding and abetting" statutes that prohibit use of a computer to facilitate fraud.⁹ Approximately 25% of states have criminalized denial of service, which is any activity that impairs the ability of authorized users to obtain the full utility of their computer system or Website.¹⁰ Unauthorized execution of

⁶See 18 U.S.C. §§ 2510-2521, 2701-2710 (1994).

⁷Xan Raskin & Jeannie Schaldach-Paiva, Eleventh Survey of White Collar Crime: Computer Crime, 33 Am. Crim. L. Rev. 541, 564 (1996) (citing Anne W. Branscomb, Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime, 16 Rutgers Computer & Tech. L.J. 1, 32-36 (1990)).

⁸See, e.g., Mass. Gen. Laws Ann. Ch 266, § 30(2) (West 1990) (larceny statute providing that "term 'property' . . . shall include . . . electronically processed or stored data, either tangible or intangible, [and] data while in transit"); Nev. Rev. Stat. § 205.4755 (1993) ("property" includes "information, electronically produced data, program(s), and any other tangible or intangible item of value").

⁹See, e.g., Haw. Rev. Stat. § 708-891(b) (1985 & Supp. 1992) (person commits computer fraud by "access[ing] or caus[ing] to be accessed any computer, computer system, computer network, or any of its parts with the intent of obtaining money, property or services by means of embezzlement or false or fraudulent representations"); Ariz. Rev. Stat. Ann. § 13-2316 (1989) (computer fraud requires "intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false or fraudulent pretenses").

¹⁰See, e.g., La. Rev. Stat. Ann. § 14:73.4 (West 1986) (offense against computer users takes place when authorized user is intentionally denied "full and effective use of or access to a computer, a computer system, a computer network, or computer services").

programs that slow down the computer's ability to process information falls under such statutes. Other states have criminalized the unlawful insertion of viruses, worms, logic bombs, and other devices which may be inserted on computers or transmitted over telephone lines or on floppy disks to contaminate or destroy data.¹¹

¹¹See, e.g., Cal. Penal Code § 502(b)(10) (Deering & Supp. 1995) ("computer contaminant" defined to include viruses and worms and other sets of instructions designed to "usurp the normal operation of the computer"); Conn. Gen. Stat. § 53a-251(e) (1994) (unlawful to make or cause to be made unauthorized display, use, disclosure or copy of data, or add data to data residing within computer system); Del Code Ann. Tit. 11, § 935 (1987 & Supp. 1994) (proscribing "interrupt[ion] or add[ition of] data to data residing within a computer system"); Minn. Stat. § 609.87 (1994) (criminalizing "[d]estructive computer program" that degrades performance, "disables," or "destroys or alters" data); W. Va. Code § 61-3C-8 (1992 & Supp. 1995) (prohibiting "disruption or degradation of computer services").

APPENDIX #2

APPENDIX II
Governmental Agencies Sharing Jurisdiction Over Internet Fraud

I. Federal

A. Criminal Jurisdiction

Two federal investigative agencies share jurisdiction over the bulk of traditional frauds committed over the Internet: the Federal Bureau of Investigation ("FBI") and the United States Secret Service. FBI's Office of Computer Investigations and Infrastructure Protection specializes in investigating high technology crimes such as Internet fraud, theft of computer information, and computer intrusions and impairment. In addition, the FBI established a National Computer Crime Squad in its Washington, D.C. field office that is specifically charged with investigating violations of the Federal Computer Fraud and Abuse Act of 1986. This act also empowered the Secret Service to investigate fraud and related activities concerning computers. Secret Service's Financial Crimes Division is responsible for investigating incidents of Internet fraud, as well as traditional financial crimes that can take place over the Internet, such as money laundering and credit card fraud.

Cases investigated by FBI and Secret Service are prosecuted by the United States Department of Justice ("DOJ"). DOJ's Computer Crime and Intellectual Property Section ("CCIPS") is responsible for implementing DOJ's Computer Crime Initiative, which is a comprehensive program designed to address the growing global computer crime problem. CCIPS attorneys litigate cases, provide litigation support to other prosecutors, train law enforcement personnel, and coordinate international efforts among law enforcement agencies to combat computer crime. In addition, DOJ has a Computer/Telecommunications Coordinator program in each of the ninety-four United States Attorney's Offices, where at least one Assistant United States Attorney serves as an in-house expert for the prosecution of high technology crimes.

The bulk of traditional Internet fraud defrauds the consumer of a low dollar amount, somewhere in the neighborhood of \$100 - \$500. Cyberfraudsters, of course, make their money by defrauding a high volume of consumers. Nevertheless, because of the low dollar amount of the individual frauds perpetrated, the bulk of federal *criminal* enforcement does not focus on traditional frauds perpetrated over the Internet. Instead, it focuses on the invasion of electronically maintained databases, also known as "hacking," which will be the subject of our second hearing.

B. Civil Jurisdiction

The primary federal agency exercising civil jurisdiction over Internet fraud is the Federal Trade Commission ("FTC"). FTC is responsible for investigating allegations of consumer fraud and bringing suit to stop fraudulent activities, including those perpetrated over the Internet. For example, FTC successfully froze an estimated \$13 million in assets that one company reaped from over 25,000 consumers by promulgating a pyramid scheme over the Internet.

FTC has also coordinated "Surf Days" on which federal, state, and local law enforcement groups "surf the 'Net'" to identify possibly fraudulent Web sites relating to a specific subject matter, such as health fraud or sweepstakes gimmicks. On "Internet Pyramid Surf Day," for example, law enforcement officials from four federal agencies and seventy state and local agencies located over 500 Web sites offering potentially illegal pyramid schemes. Participants preserved the information found at those sites for possible future law enforcement action. In addition, FTC sent e-mail messages to the operators of each of the sites warning them that their pyramid schemes are illegal, describing the characteristics of illegal pyramids, and providing FTC's home page address to help entrepreneurs and consumers distinguish between illegal pyramids and legal multi-level marketing plans.¹ FTC plans to revisit the Web sites in the future and take further action if evidence suggests they are illegal operations.

In addition to enforcement activities, FTC also operates a consumer education program to inform consumers about deceptive and fraudulent practices. FTC administers this program through regular publications as well as through its Web site, <<http://www.ftc.gov>>.

Another federal agency that has done an exemplary job in proactively combating Internet fraud is the Securities and Exchange Commission ("SEC"). SEC has jurisdiction over fraudulent investment activities on the Internet. Recently, SEC began an Internet enforcement program under its Division of Enforcement to search the Internet for fraudulent investment opportunities. For example, in 1996 the SEC filed several civil actions against companies soliciting unregistered securities or fraudulent off-shore investments over the Internet. SEC actions have resulted in injunctions against the fraudulent activity, freezing of defendants' assets, and levying of monetary penalties against defendants. SEC operates a Web site, <<http://www.sec.gov>>, that consumers can access to learn more about securities fraud on the Internet.

II. State

Each state has an office of the attorney general with the power to investigate and prosecute the use of the Internet to commit or facilitate fraud. As the state's chief legal officers, attorneys general can bring both civil and criminal actions against those accused of perpetrating fraud on the Internet.² For example, state attorneys general have filed numerous civil Internet consumer cases covering fraudulent health care product sales, business opportunities, credit repair, and miscellaneous product and service offerings.³ Earlier this year, the Idaho attorney general's investigation of securities fraud over the Internet resulted in the arrest and conviction of the perpetrator.⁴

One obstacle states face in prosecuting online fraud is the absence of physical boundaries on the Internet. Establishing jurisdiction may be difficult because a company located in one state can easily and readily use the Internet to defraud consumers located in another state. Conflict among state laws may further complicate Internet prosecutions by states. In other words, an Internet activity may be legal one state but illegal in another. Such conflicts of laws pose particular problems with the use of Web sites, because persons can access them regardless of their location and thus without regard to the law of any particular

state.

Despite these difficulties, states do have one advantage over prosecution by federal agencies: They generally have more flexibility with regard to the dollar value of cases they accept, and thus can prosecute cases of Internet fraud that would otherwise fall through the cracks in the federal system.

III. Local

Local law enforcement agencies also have jurisdiction to investigate and prosecute Internet fraud. However, local law enforcement agencies often lack sufficient resources, equipment, and specialized training to effectively prosecute these cases. In order to address these problems, some local law enforcement agencies are working with multi-jurisdictional task forces. For example, a High Tech Crime Task Force has been established in California that includes the participation of the California Highway Patrol, California Department of Justice, and local law enforcement agencies from several counties in the Sacramento region to investigate computer and other high technology crimes.⁵ Similar high technology crime units are operating or are being considered in other regions, including Illinois, Massachusetts, Ohio, Michigan, and Pennsylvania.⁶

1. See "Federal-State Surfing Catches a Wave of Potential Internet Scams; Over 500 Pyramid Operations Put on Notice," FTC press release, Dec. 12, 1996.

2. Criminal/Civil Rights Subcomm., Internet Working Group, Nat'l Ass'n of Attorneys Gen., *The Internet and Crime: A Report to the Internet Working Group of the National Association of Attorneys General 1* (June 1997) (hereinafter "NAAG Internet and Crime Report")

3. Christine Milliken, Office of the State Attorney General and Cyberspace 9 (1997) (unpublished manuscript, on file with the National Association of Attorneys General).

4. *Id.* at 12.

5. NAAG Internet and Crime Report, *supra* n.1 at 28.

6. *Id.* at 28-29.

**Senate Permanent Subcommittee
on Investigations**EXHIBIT # 5**Supplemental Questions of Senator Max Cleland**

and

**Responses by Robert Pitofsky,
Chairman of the Federal Trade Commission****Online Privacy****Question 1:**

I recently heard that over one-third of the companies in America monitor their employees' email, computer files and telephone voice mail. While this is not a fraud issue per se, it is a privacy issue with perhaps some dangerous implications. I'd like to get your thoughts, Mr. Pitofsky, on whether you think there should be privacy laws in cyberspace?

Response:

The FTC has been focusing on privacy issues in cyberspace over the past three years because it has become apparent that electronic commerce will not meet its full potential unless consumers' privacy is protected in this new medium. The question is how best to achieve privacy protection.

Our preference has been to encourage self-regulation in the first instance. Accordingly the agency held a number of public workshops to facilitate self-regulation by bringing together industry members, consumer and privacy advocates, and government agencies. Because workplace issues are beyond our primary mission of protecting consumers, the agency has not focused on the issues you pose of monitoring of employees' e-mail, computer files, and telephone voice mail. Our focus has been the privacy protections afforded consumers in general, and children in particular, as they use the Internet to engage in commerce and gather information. In fact, the FTC is currently undertaking a survey of 1,200 World Wide Web sites to assess whether industry self-regulatory efforts have led sites to post privacy policies. The results of this survey will be sent to the Congress in June.

Consumer Education**Question 2:**

Mr. Pitofsky, I understand that the FTC has also launched a significant consumer education initiative. Could you describe for me the consumer protection program that you have put in place?

Response:

The FTC works to stem fraudulent, misleading and deceptive practices through actions that involve both law enforcement and consumer education. Acting on the belief that the most effective consumer protection is education, the FTC tries to alert as many consumers as possible to the tell-tale signs of fraud. The agency's information dissemination program is vital to our mission. It is accomplished in large part by working with a variety of "partners" -- for example, other federal agencies, state and local consumer protection agencies, trade associations, professional organizations, volunteer groups, corporations, Better Business Bureaus, the military -- and through a variety of media -- newspapers, classified ads, public service announcements, bus placards, the Internet, brochures, bookmarks, and puzzles, to name a few.

Among the innovations the FTC uses to alert consumers to fraud on the Internet are "teaser" sites. Too often, consumers do not find useful information until it is too late. By using "teaser" web sites, the agency is trying to reach consumers before they make a purchase or invest their money. These "teaser" sites are web pages, accessible by major search engines and indexing services, that mimic fraudulent sites. Internet shoppers looking for vacation deals, for example, may find an innocent-looking site that offers a spectacular, luxury dream vacation at a money-saving price. A lovely sunset appears. Three clicks into the "come-on," the FTC seal appears. The site alerts consumers who respond that they can get scammed and offers tips on how to distinguish fraudulent vacation pitches from legitimate ones. The site also enables the consumer to link to the FTC's web site for additional information. Other sites address Internet business opportunities, work-at-home schemes, and weight loss products. The public has responded very favorably to these sites.

The FTC also has devised tutorials in the form of interactive puzzles and quizzes to reinforce what consumers have read in their newspapers or on the FTC's web site. For example, for an announcement about actions in the investment fraud area, the FTC launched an online quiz called "Test Your investment I.Q." A series of typical telemarketing misrepresentations asks consumers to define the investment offering as solid or risky. The site also featured the "Top 10 Lines" used by fraudulent telemarketers when they make their pitch, and a feature called "What They Say Isn't Always What They Mean" to help consumers see through the lines favored by the slick telemarketers. In connection with "Project MouseTrap," a series of actions against fraudulent invention promotion firms, the FTC created an activity designed to test a consumer's "patent-ability" -- a crossword puzzle containing critical terms from the worlds of patents and idea promotion. These teaser sites and tutorials serve as complements to the brochures the agency publishes and promotes.

ConsumerLine, the FTC's consumer information page at its web site, accounts for about one-third of all the visits to www.ftc.gov. It offers the full text of over 100 print pieces that the agency produces, including Consumer Alerts and Facts for Consumers brochures, as well as the separate education "campaigns" the agency mounts on specific issues. The FTC's web site, www.ftc.gov -- and particularly ConsumerLine -- have been recognized many times in the last year as a "best of the Web" for ease of use and quality of information.

Building on the success of its home page, the Commission solicited other agencies to

create a new consumer site at www.consumer.gov. Since last December, this site has provided the public "one-stop shopping" for federal information on consumer issues ranging from auto recalls to drug safety to information resources for investors. The site is arranged topically, so that consumers can find information about an issue without having to know the name of the agency that deals with the issue. In addition, the site's **Scam Alert!** offers the latest information on fraudulent and deceptive practices in the marketplace. This feature appears on each page as necessary and contains enforcement information and tips to avoid scams. Original FTC partners included the Securities and Exchange Commission, the Consumer Products Safety Commission, the Food and Drug Administration, and the National Highway Transportation Safety Administration. Since the launch of consumer.gov, several more federal agencies have joined as partners: the Department of Agriculture, the Department of Education, the Department of Health and Human Services, the Federal Deposit Insurance Corporation, the Department of Housing and Urban Development, the Federal Communications Commission, and the Environmental Protection Agency. The FTC was particularly proud to spearhead this effort to make federal consumer information more accessible.

The Commission has sought Internet companies and industry associations to join as partners in educating consumers about online issues. Many organizations already have circulated public service messages on their Internet sites, cautioning consumers to avoid particular scams and linking them to the Commission's web site where they can find appropriate information. The Commission also has published a series of cyber-related brochures, which also are on the web site, and a bookmark, "How to Be Web Ready," that has been promoted heavily. In fact, corporations have linked to the bookmark (e.g., Circuit City and Micron), as have associations such as the Direct Marketing Association, and others are in the process of linking. In a joint effort with the National Association of Attorneys General, the Commission plans to publish "Site Seeing on the Internet," a booklet for parents, within the next few months.

In addition to using the Internet to educate consumers about fraud (online and off), the agency also strives to use the Internet to educate businesses about their responsibilities to consumers. **BusinessLine** (at www.ftc.gov) includes the full text of all the compliance guides published by the Bureau of Consumer Protection. In addition, FTC staff regularly speak at industry conferences. In mid-March, for example, two staff attorneys will speak on Internet advertising and online fraud at a national conference of Internet service providers, called ISPCON, in Baltimore, MD.

Law Enforcement Tools

Question 3:

In traditional consumer scams con artists know it's more difficult for law enforcement to come after them when they are in one location and their victims are in another. With Internet fraud, the situation becomes even more challenging, given the fact that there are no geographic borders in cyberspace. We saw, for example, that when Fortuna Alliance was shut down in this country, Fortuna Alliance II simply re-opened its shop in Antigua. Mr. Pitofsky, let me echo my colleagues by asking what tools can Congress give you to make your enforcement job easier?

Response:

As stated in our testimony, the FTC Act currently provides us with the legal tools we need to combat most unfair and deceptive practices that occur online. Yet, I believe that the Commission lacks the resources to meet both growing Internet fraud and its traditional consumer protection law enforcement responsibilities in areas such as credit practices, telemarketing, and national advertising.

To effectively carry out its mission, the Commission must handle more consumer complaints while increasing its enforcement actions against Internet fraud. In the first instance, I believe that the Commission's new Consumer Response Center ("CRC") needs resources to convert its telephone number to a toll-free number, thereby enabling any consumer with a serious Internet problem to make a report and receive timely advice. The CRC also needs additional personnel and equipment to maintain a high-level of service while handling the surge in letters, telephone calls and e-mails received from the public. The expansion of the CRC is necessary, not only to respond directly to consumers, but also to take rapid action against perpetrators of fraud. It is the CRC that primarily feeds the national database relied on by investigators, litigators, and prosecutors within the Commission and scores of other law enforcement offices -- from the Department of Justice and the FBI to the offices of state Attorneys General.

The Commission also requires additional resources to remain effective in its law enforcement actions against new, sophisticated, and often international fraud on the Internet. We have announced four additional Internet cases just since the Subcommittee's hearings in February, bringing our total number of federal Internet actions to over 30. Yet, in Chairman Collins' words, we are beginning to "rob from Peter to pay Paul." Our consumer protection mission resources have remained constant, but our dedication of consumer protection budget work years or "FTE's" to Internet issues has risen from 4% to 16% since 1996. The Commission cannot adequately carry out enforcement in areas like home equity fraud, fair credit lending, telemarketing fraud, and food and drug advertising if resources are required to address pressing Internet problems. At the same time, we should not permit fraud to stifle the growth of the important, emerging online marketplace. Therefore, I believe additional resources will assist the Commission fulfilling its consumer protection mission.



Senate Permanent Subcommittee
on Investigations

EXHIBIT # 6

1701 K Street, NW • Suite 1200 • Washington, DC 20006 • (202) 636-3323 • FAX (202) 635-0747 • <http://www.natconsumersleague.org>

Board of Directors

Linda F. Goldner
President

Brandolyn T. Clanton Pinkston
Chair

Charlotte Newton
Vice Chair

Esther Shapiro
Vice Chair

Markley Roberts
Treasurer

Don Rounds
Secretary

Jack A. Blum
Counsel

Robert R. Nathan
Honorary Chair

Esther Peterson (1906-1997)
Honorary President

Erna Angevine

Dorothy M. Austin

Debra R. Berlyn

Alan Bosch

Jim Conran

Ellen C. Craig

Theodore R. Debro, Jr.

Joseph K. Doss

Evelyn Dubrow

Glenn English

Mary Finger

Carolyn Forrest

Eugene Glover

Ruth Harmer-Carew

Pastor Herrera, Jr.

Mary Heslin

Arlene Holt

Sandra Willett Jackson

Ruth Jordan

Jane M. King

Harry Kranz

Jorge J. Lambrinos

O'donna Mathews

Robert W. Mayer

Joyce Miller

Larry Mitchell

Patricia Royer

Bert Seidman

Samuel A. Simon

Caroline B. Stelmann

Ricki Stochaj

Leland H. Swenson

Patricia Tyson

Barbara Van Blake

Gladys Gary Vaughn

Clair E. Villano

March 2, 1998

Timothy J. Shea

Chief Counsel and Staff Director

Senate Permanent Subcommittee on Investigations

432 Hart Senate Office Building

Washington, DC 20510-6250

Dear Mr. Shea:

In response to your February 24 letter and the supplemental questions about Internet fraud posed by Senator Max Cleland, please allow me to provide the following answers. We request that these be added to the record of our testimony at the Fraud on the Internet hearing on February 10, 1998.

1. In regard to banking on the Internet, what safeguards are in place to assure that individuals do not lose their life savings at the hands of savvy Internet con artists?

Banks use encryption programs to "scramble" the information that is transmitted online so that even if it is intercepted, it cannot be "read" by others. Encryption programs are also used by online vendors so that consumers can provide financial information such as their credit card numbers safely. These encryption programs are either the vendors' own or provided by their Internet service providers. While it is unlikely, a very sophisticated computer "hacker" might be able to break these codes, and the industry continues to refine them.

The greater danger of Internet fraud, in our view, is from entities that pretend to be banks and are not, or banks that are not overseen by U.S. regulators. Our National Fraud Information Center has received reports from consumers about advertisements on the Internet by foreign banks offering high interest rates or special services such as trusts. In some cases, those banks are phony or their services are misrepresented. Furthermore, if the institution closes, depositors are not protected by FDIC insurance. Since there is no way of ensuring the safety and soundness, or even the existence, of these offshore banks, consumers could lose all of their money.

2. How does the National Consumers League promote public awareness about the Internet Fraud Watch and our fraud center web site?

Representing Consumers for 99 Years

Printed on Recycled Paper

We constantly promote awareness about Internet fraud and our Internet Fraud Watch program through our newsletters, press releases, speeches, media interviews, and other public outreach. Government agencies such as the Federal Trade Commission, nonprofit organizations like the American Association of Retired Persons, and legitimate Internet and online marketers also promote our web site and fraud reporting services. Many have links from their web sites to ours.

In fact, the problem is not promoting our Internet Fraud Watch program, but rather keeping up with the demand for the information and services we provide. We receive 1,200 to 1,500 e-mails each week from consumers who want advice about Internet or online solicitations or to report fraudulent solicitations to law enforcement agencies through the Internet Fraud Watch. Because of our limited resources and the fact that private contributions do not cover our costs, it is difficult for us to handle the growing volume of questions and fraud reports.

3. How does the National Consumers League help consumers differentiate between legitimate web sites and bogus ones?

While we do not provide public information about specific companies, one way that we help consumers spot fraudulent web sites is by telling them to look for the warning signs: money making schemes that rely on recruiting others to join the plan, not on sales of products or services; prize offers or sweepstakes that require paying a fee to "win;" services that guaranty credit cards or loans to people with bad credit if they pay a fee up front; companies offering Internet services or other products or services for ridiculously low prices; wild claims that no legitimate company would make for investment returns or profits on business opportunities.

However, it is not always possible to tell if a web site, or an advertisement in an online service, or an unsolicited e-mail offer is legitimate just by looking at it. So we advise people to do their homework: check the company's complaint record with their state and local consumer protection agency and the Better Business Bureau; find out if businesses that have special licensing or registration requirements, such as securities brokers, have complied; ask for references for business opportunities and franchises; get all investment offers information in writing and seek professional advice.

To protect themselves even further, we urge consumers not to pay in cash (the 4th most frequent method of payment reported to us in incidents of Internet fraud!) and to use credit cards whenever possible. Whether they are providing their credit card numbers online in a secured environment, or offline by telephone or mail, consumers have important dispute rights that they can exercise if the products or services are never delivered or were misrepresented.

Finally, we caution consumers about the dangers of dealing with any seller long-distance. While some state and federal laws that prohibit unfair and deceptive practices apply to promotions via the Internet and online services, pursuing a claim may be difficult if the seller is in another part of the country, or even another part of the world.

I hope that this additional information is helpful and welcome any further questions the committee may have. Thank you very much for your interest in protecting consumers and legitimate marketers from Internet fraud.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Susan Grant", with a stylized flourish extending to the right.

Susan Grant, Vice President for Public Policy
Director, National Fraud Information Center/
Internet Fraud Watch Programs



Senate Permanent Subcommittee
on Investigations

EXHIBIT # 7

April 6, 1998

The Honorable Susan Collins
Chairman, Permanent Subcommittee on Investigations
Committee on Governmental Affairs
Washington, DC 20510-6250

Dear Chairman Collins,

Once again, let me thank you for the opportunity to have appeared before your Subcommittee on February 10, 1998 to discuss the important issue of fraud on the Internet. As I stated at the hearing, America Online, Inc. is committed to providing its members with the tools necessary to prevent their falling prey to fraudulent schemes on the Internet. We have and will continue to make providing a safe and secure environment for electronic commerce one of the company's top priorities. This letter is intended to provide answers to the two supplemental questions provided by Senator Max Cleland. In addition, I would like to clarify one statement that I gave in response to a question posed at the hearing by Senator John Glenn.

Question 1:

Senator Cleland's question relates to the protection of consumers' life savings from "savvy Internet con artists." While it is impossible to prevent con artists from preying on consumers on the Internet, America Online believes that the safeguards it has put in place assist consumers in using the Internet conscientiously and smartly so as to avoid being defrauded. As I stated in my written and oral testimony, AOL provides several tools to enable consumers to avoid having contact with any person or business with which they are not familiar. We do this both by providing a mechanism for consumers to control the electronic mail they receive and by providing alerts when downloadable files are sent that could enable a con artist to have access to a consumer's private information. In addition, we have created online areas like our Neighborhood Watch to inform consumers about how to use AOL and the Internet safely and to notify AOL of any possible problems. We believe that arming consumers includes reinforcing two key messages: 1) don't believe everything you see and hear; and 2) if it sounds too good to be true, it probably is. Finally, in addition to providing the tools to help consumers avoid and report fraud, AOL has also created its Certified Merchant Program, which provides consumers with a list of merchants that have satisfied AOL's merchant screening process and with which the company believes consumers can safely do business online.

Question 2:

AOL is committed to ensuring that our members are fully educated and armed to deal with situations in which they are confronted with con artists online. Just as in the offline world

The Honorable Susan Collins
April, 6, 1998

buyers must "beware" of the merchants with whom they deal, on the Internet it is critical that consumers enter into transactions with merchants they trust. As I mentioned above, AOL offers its members a Certified Merchant Program through which the company can point consumers to merchants that we know are offering good trustworthy services.

In addition, AOL has a network of lawyers and security professionals whose jobs include helping to ensure that fraud on the Internet is minimized. A critical aspect of these activities includes ongoing cooperation with law enforcement officials across the country and the globe to uncover and prosecute perpetrators of fraud. While AOL's commitment to offering consumers a safe and secure environment for electronic commerce is clear, the ultimate responsibility for policing the Internet cannot fall entirely on the shoulders of Internet service providers who enable consumers to access online merchants. Given the size and scope of the online medium, where merchants from all across the globe can sell their wares, placing such a requirement on ISPs generally would be unworkable and unwise.

Finally, I would like to clarify my answers to a series of questions posed by Senator John Glenn at the hearing. The dialogue to which I am referring appears on page 51 of the transcript of my testimony. Senator Glenn asked whether America Online makes its mailing lists available to third parties for sale or lease. I answered that question and the Senator's follow-up questions in the negative, since I understood the question to be concerned with the company's release of information connecting members' online and offline identities. Upon reviewing the transcript however, I now believe that Senator Glenn was merely asking about whether AOL makes its mailing lists, including the names and addresses of our members, available for sale or rental. The correct answer to that question is that we do, under very controlled circumstances for specified purposes lease our member lists -- including only names and addresses -- but at no time make any information available that would enable a third party to connect a member's online identity and offline identity.

I hope that the above information both answers Senator Cleland's questions and clarifies my response to Senator Glenn's inquiries.

Please let me know if I can offer any additional assistance.

Sincerely,



Tatiana Gau
Vice President,
Integrity Assurance

NATIONAL FRAUD INFORMATION CENTER

Senate Permanent Subcommittee
on Investigations

EXHIBIT # 9

A Project of National Consumers League
ABOUT THE NATIONAL FRAUD INFORMATION CENTER
and the
INTERNET FRAUD WATCH

The National Fraud Information Center, a project of the nonprofit National Consumers League, was established in 1992 to combat telemarketing fraud. In 1996, the Internet Fraud Watch was created, expanding the scope of the League's fraud-fighting efforts to scams in cyberspace.

Consumers can get advice about how to tell fraudulent from legitimate telemarketing and Internet promotions by calling the NFIC's central toll-free number, 1-800-876-7060, going to its web site, <http://www.fraud.org>, sending an e-mail to fraudinfo@psinet.com, or writing to P.O. Box 65868, Washington, DC 20035. Trained counselors help consumers identify the danger signs of fraud, such as: demands for payment in order to claim prizes or sweepstakes winnings; high-pressure sales tactics; refusal to provide written information; unrealistic claims of potential profits or earnings; and sound-alike charities. Counseling services are available in English and Spanish, Monday through Friday from 9 a.m. to 5 p.m. Eastern time.

In addition to individual counseling, consumers receive fact sheets and brochures on specific topics. Another vital source of information and advice is the NFIC web site. The Internet Fraud Watch section, <http://www.fraud.org/ifw.htm>, provides tips for consumers on how to avoid the most common types of Internet and online fraud and how to protect their privacy. The web site also features general telemarketing fraud tips and a special section with advice about telemarketing fraud targeting older consumers. From the NFIC web site, consumers can link to dozens of government agencies and organizations for even more information and assistance. The NFIC web site has garnered 12 Internet awards, including the *USA Today* "Hot Site" and a "Best of '96 Award" from *HomePC Magazine*.

Consumers can report suspected telemarketing or Internet fraud to law enforcement agencies through the NFIC and IFW. The easiest ways are calling the hotline or using the fraud reporting form on the web site. Telemarketing and Internet fraud reports are transmitted daily to a database for law enforcement agencies maintained by the Federal Trade Commission and the National Association of Attorneys General. They are also relayed to over 150 agencies at all levels of government in the United States and Canada. Through this "early warning system," law enforcement agencies are alerted to emerging scams and provided with the information they need about con artists and their victims.

National Fraud Information Center
PO BOX 65868
Washington, DC 20035
<http://www.fraud.org>

Law Enforcement Assistance: (202) 835-0618
Fax: (202) 835-0767
Consumer Assistance: (800) 876-7060
TDD: (202) 835-0778

Statistics Show Internet Fraud Rising

The blurry computer screen gradually comes into focus while an Internet advertisement flashes across the screen. The message reads: "HUNDREDS of unclaimed scholarships, 100 percent guaranteed! Or, make MILLIONS in ...is multilevel marketing plan!"

As more consumers gain access to the Internet, fraud will only continue to rise as crooks prey on unsuspecting cyberspace users, according to the National Consumers League's National Fraud Information Center. The number of fraud reports that consumers made to NFIC rose sharply last year.

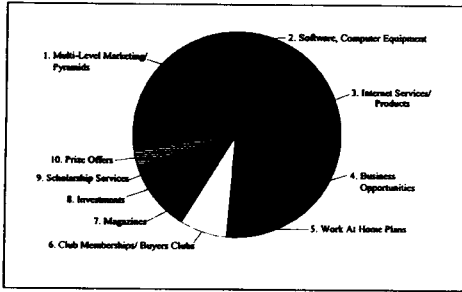
"Con artists are using the same pitches on the Internet that they have long made by mail or on the phone," NFIC Director Susan Grant said.

"The same pitches -- whether on-line or on the telephone, require the same advice," she said. "Be wary

of promises of great profits or earnings, wonderful bargains, and free gifts or prizes. They could just be vapor in cyberspace."

Grant said that pyramids and bogus multilevel marketing plans led the list of Internet fraud reports made to NFIC in 1996. Those scams are also among the top 10 telemarketing fraud complaints that consumers make to the center.

NCL established NFIC in 1992 to give consumers advice concerning telephone solicitations and to route reports of fraud to law enforcement agencies. With a grant from



Statistics show incidences of fraud on the web are growing. Source: NFIC

MasterCard International in 1996, the League created Internet Fraud Watch, which enabled NFIC to expand its services to cover fraud on the World Wide Web. NationsBank became the official bank sponsor last year, and MCI and NYNEX also help sponsor NFIC's Internet program.

NFIC receives about 300 e-mail

messages daily from consumers who want information about Internet promotions -- up from 20 per day last February. And more than 90,000 people visit the NFIC web site at <http://www.fraud.org> each week to read the latest news on scams and browse through the educational information that it provides.

According to NFIC statistics, some of the top 1996 Internet scams were technology specific, targeting computer users. For instance, the second most frequent cyberfraud involved sales of computer

Please See **Internet**, Page 2



Internet, from Page 1

equipment and software, while number three was sales of Internet services and products.

"Consumers paid in advance for equipment or services they either did not get or didn't do what was promised," said Grant. "That isn't to say consumers should avoid internet commerce, only they need to be extremely careful. And they need to do their homework today on a company they plan to do business with on the Internet, or they may regret it tomorrow."

The remaining top ten cyberscams were:

4. business opportunities and franchises;
5. work-at-home schemes;
6. club memberships and buyers clubs;
7. magazine subscription sales;
8. investments;
9. scholarship services;
10. sweepstakes and prize offers.

Consumers can ask questions or make fraud reports through NFIC's toll-free hotline, **(800) 876-7060**, or via its web site. Nearly 400 reports of suspected Internet fraud were processed from February to December in 1996.

The reports are downloaded daily to the telemarketing and Internet fraud database maintained by the Federal Trade Commission and the National Association of Attorneys General. Reports are also provided to other law enforcement agencies to alert them to scams and "give them the ammunition they need to take action against fraud," Grant said.

NFIC's web site has won 12 Internet awards for the quality of consumer information it provides. A new Internet Fraud Watch section will appear on the site soon, featuring tips on how to avoid fraud, articles on government agencies and private sector attempts to combat abuses, bulletins about the latest scams, and information about protecting one's privacy in cyberspace. •

