AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ON-LINE FRAUD AND CRIME: ARE CONSUMERS SAFE?

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

MAY 23, 2001

Serial No. 107–37

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE
72–823PS WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

NATHAN DEAL, Georgia
Vice Chairman
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ED BRYANT, Tennessee
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

EDOLPHUS TOWNS, New York
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

ON-LINE FRAUD AND CRIME: ARE CONSUMERS SAFE?

WEDNESDAY, MAY 23, 2001

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Upton, Deal, Shimkus, Bryant, Terry, Bass, Tauzin (ex officio), Towns, DeGette, and Harman.

Staff present: Ramsen Betfarhad, policy coordinator and majority counsel; Brian McCullough, professional staff; David Cavicke, majority counsel; Kelly Zerzan, majority counsel; Shannon Vildostegui, professional staff; and Will Carty, legislative clerk.

Mr. STEARNS. Good morning. Welcome to the Commerce, Trade and Consumer Protection Subcommittee hearing on cyber fraud and crime. I want to thank all of our witnesses for appearing before the committee this morning and I am especially pleased that we have four of our top Federal law enforcement agencies charged with combatting cyber fraud and crime present this morning.

I understand that as I speak, the FBI, in conjunction and coordination with the Secret Service, the IRS, the U.S. Customs and U.S. Postal Service and a myriad of State and local law enforcement agencies are arresting as many as 90 suspects as part of a nationwide sweep combatting fraud. The breadth and scope of this operation is very impressive. I commend the FBI and all the other Federal and local law enforcement agencies for undertaking such an important law enforcement action.

The Internet fraud schemes exposed as part of this investigation represent over 56,000 victims nationwide who suffered cumulated losses in excess of $117 million. I know we'll hear more about that this morning.

I believe that effective enforcement in tandem with greater consumer education and awareness and industry action spells out an effective recipe for protecting against and combatting cyber fraud and crime. It is no great revelation that fraudulent and criminal activities have colored the human experience throughout history. With any major technological development, new types or forms of fraud and crime make their debut as older forms are adapted to

take advantage of this new technology, that is, no telemarketing fraud without a telephone network.

One cannot argue that fraud or crime lacked from a want of innovation of creativity. The Internet, as a sweeping new technology, is no exception. With the advent of the Internet, a global ubiquitous communications network offering virtual anonymity, old-style fraudulent and criminal activities have made their way into the Internet as new frauds have evolved to take advantage of the Internet's unique properties.

The Internet fraud schemes highlighted today by the FBI nationwide sweep and FTC's top Internet scam list indicate that most of the scams are old fashioned, but there are some that are new and enabled by the Internet.

Although both the old-fashioned scams as executed on-line and the new on-line specific scams pose difficult challenges for law enforcement, today's testimony clearly suggests that those challenges are definitely surmountable. Yet, combatting these new challenges may require new thinking on the part of law enforcement in conjunction with substantially greater cooperation between Federal, local and indeed international law enforcement agencies.

A more significant deterrent to cyber fraud and crime is consumer education and awareness. As our knowledge as on-line users increases, the risk of us being taken by fraudulent activity decreases dramatically.

Today's hearing is an important step in informing the American consumer as to what is transpiring on-line. The hearing highlights the types of fraud being propagated without the fanfare which some of the media outlet provide and this is good. The testimony today is a good source of straight facts.

And finally, my colleagues, industry has an important role in undertaking security measures to protect their on-line systems from fraudulent and criminal activities. Today's testimony merely highlights a snapshot of all efforts undertaken by industry to protect and make secure their on-line system. They clearly recognize that preservation and enhancement of on-line security is good for business.

I very much look forward to the testimony and again want to congratulate the FBI and the other law enforcement agencies who are undertaking nationwide sweep combatting cyber fraud and crime.

And at this point I'll ask the distinguished ranking member from New York for his statement.

Mr. TOWNS. Thank you very much, Mr. Chairman. I want to thank you for holding this important hearing.

This committee has a special responsibility to protect consumers against fraudulent commercial practices wherever they occur. Clearly, Internet transactions present unique opportunities for those who want to take advantage of consumers. In many ways, the Internet makes an on-line retailer anonymous to a consumer. The seller's actual location may not be known. Representation the seller makes are largely unverifiable. The quality of goods or services that are being sold may not be identifiable. Information the consumer divulges in the course of conducting an Internet transaction may be used in ways the consumer does not approve and the

consumer may have no idea of how to obtain recourse for harm he or she suffers.

It is clear to me that unless we satisfy consumer concerns about these and other problems, consumers will limit their Internet transactions and Internet will not realize its full and proper potential. This would be truly unfortunate. Many of us understand the tremendous benefits consumers stand to gain from on-line retailing and other transactions, especially today as the attention of more and more of us is being directed to the need to conserve energy in as many ways as possible. On-line shopping offers the potential for real energy savings that are too attractive to ignore.

In addition, on-line shopping can provide the consumer with a far greater range of choices than traditional retailing can provide.

I therefore look forward to hearing from our witnesses about what action this subcommittee should be considering to help make the consumer secure and confident about his or her on-line transactions.

Many have taken a wait and see attitude on the need of protecting phone line transactions. My personal view is that we have seen enough at this time. It is time now for action. In much the same way this committee acted not too many years ago to protect consumers against telemarketing fraud, it is now time to act against on-line fraud. This is not a partisan issue. No one is safe. There have been reports of on-line fraud, identity and other wrongful acts affecting virtually every member of our society including CEOs of major corporations. Towhead must stop. And I would hope that this subcommittee will take the lead in bringing the fraudulent practices that occur on-line to an end.

Mr. Chairman, again, I want to thank you for holding this hearing.

Mr. STEARNS. I thank my colleague, and now the distinguished Chairman of the full committee, Mr. Tauzin.

Mr. TAUZIN. Thank you, Mr. Chairman, and I want to thank you for this hearing today because we focus today on cyber fraud and cyber crime, on what it is and what the appropriate law enforcement agencies are doing about it. And I'm particularly pleased that will hear today from the agencies that are charged with enforcing the current law, like the identity thefts and the assumption of the Deterrence Act of 1998 that was authored by John Shadegg. Although similar to traditional fraud in many ways, Internet fraud poses rather unique problems. Just as privacy has always been an issue for us in the brick and mortar world, privacy poses unique problems on the Internet and so it is with fraud.

Fraud is nothing new, Mr. Chairman. You know, there have been sham artists and shake down artists who visited our homes as traveling salesmen or catalog frauds or mail order frauds of all types, but the Internet gives miscreants special capabilities because they can hide a lot better on the Internet and they can deceive a lot better on the Internet in many ways. Predators can mask their identifies. They can hide their locations and they can easily cover their tracks. Websites can be put up and then removed in seconds, allowing criminals to strike quickly and run even faster. Bonnie and Clyde would have loved this environment.

Internet fraud has taken many forms, many which we'll discuss here today, including on-line auction fraud, identity theft and pretexting and Internet fraud can reduce consumer confidence in the safety of on-line transactions. And if there's one thing I think we all need to be paying special attention to, it's how well we enforce the law, how well we prevent the fraud on the Internet from damaging its potential as a place for Americans and people in the world to do business.

This low consumer confidence ends up meaning fewer transactions, slower economic growth and you know the rest.

I'm pleased that the agencies charged with battling Internet fraud are here today and Eileen, I'm particularly pleased again to see you. You've been so helpful to us in all the work you've done with the FTC. I'm pleased that we have representatives from private companies here to tell us how they intend to battle on-line fraud. Private companies with an on-line presence know how dangerous this is because they see the enormous value in protecting information about their customers and protecting their customers from miscreants.

Security is a priority and businesses are responding. I'm going to have to leave right when I finish, Mr. Chairman, to go upstairs. We've got a hearing on the capacity to hack into the HICFA websites and the lack of security on those websites and the potential for harm and damage and fraud in our important Medicare fund systems.

The bottom line is with increasing technologies, the Internet world is increasingly less safe unless we are increasingly vigilant. And today, we'll learn about how we can be better enforcers of the law and more vigilant in protecting against fraud that would rob Americans of the great potential of the e-commerce.

I want to thank you, Chairman Stearns, for holding the hearing. As usual, you have prepared an informative and educational set of panels and as Chairman of the full committee I want to extend the appreciation of all the members of our committee for the fine work you're doing in this series of hearings.

Thank you and I yield back my time.

Mr. STEARNS. I thank the chairman. Now we will recognize Mr. Shimkus from Illinois.

Mr. SHIMKUS. One of the few times I get to go before Chairman Upton. I'm going to be very, very brief. Crooks are crooks and we just have to stay ahead of them or at least we have to stay equal to what their ability to get in. There's also an issue of the thrill of the challenge. I think that's all part of this, especially with our young. I always like when we have some young kids in the audience and there's two about halfway back, very young girls and that's the exciting age of computer activity that advances way past most of us policymakers. They're the ones who may get in the wrong crowd and start playing around and being able to do a lot more things. It's hard to get our generation, the old fogies up to speed to meet the challenge technologically of the software and the encryption and the keys and all the other stuff. Law enforcement and individuals are of a different generation than the generation today. So that's the challenge. The challenge is keeping pace with the bad guys and there's always going to be bad guys.

So I look forward to the hearing today to hear what we're doing as Federal agencies to try to keep pace with the bad guys and also, of course, the private sector is going to have a tremendous role because really, they've got to protect their bottom line. So they're going to be investing a lot of money to attempt to do that. Identity theft, pretexting and on-line consumer fraud are probably the big three. I look forward to the hearing today and with that, Mr. Chairman, I yield back my time.

Mr. STEARNS. I thank my colleague. Now the distinguished chairman of the Telecommunications Subcommittee, Mr. Upton.

Mr. UPTON. Thank you, Mr. Chairman, and I want to thank you also. We were hoping to have a witness from the State of Michigan and at the very last moment he was not able to come and I appreciate your willingness to include him as part of the second panel. This is an important hearing.

Last year, a resident of my District had her credit card and other sensitive materials stolen by a home improvement contractor installing tile at her house and the contractor used the information to order literally thousands of dollars worth of merchandise over the Internet. Because of quick police action, expertise and effectiveness of Michigan's high tech crime unit, just last week the perpetrator pled guilty. This story had a happy ending, but there are a lot of them out there that don't. Literally thousands of these crimes go unsolved and unfortunately high tech crimes are quickly becoming commonplace.

While we all can do more to protect ourselves from on-line crimes, we must also take preemptive action to make sure that law enforcement has the tools and the training that they need to catch the bad folks.

Currently, Michigan is one of only a handful of States that have a high tech crimes unit and according to the FBI cyber crimes perpetrated by individuals in Michigan already account for 3.2 percent of those committed in the United States. I've been told that since its establishment in 1999, the unit had over 1500 complaints and tried cases from the sale of date rape drugs over the Internet, an issue that I tried to take care of with legislation last year, to child pornography and yes, even murder. But the biggest obstacle faced by law enforcement agencies investigating alleged cyber crime is distance. Because these types of crimes are committed via the Internet, often the victim and the perpetrator are thousands of miles away from each other, even perhaps on the other side of the globe. For all the promise of new technology, there are also new dangers that most of us would never think of and that's why today's hearing is so important.

I look forward to hearing from the witnesses and interacting throughout the day and I yield back the balance of my time.

Mr. STEARNS. I thank the gentleman. The gentleman from Nebraska, Mr. Terry. No opening statement.

At this point we'll move to Panel 1. Mr. Bryant, the gentleman from Tennessee is interested in an opening statement before we begin. Pass. All right.

We have in Panel 1 Mr. Bruce Swartz, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice. We have Thomas Kubic, Deputy Assistant Director, Criminal Division,

Federal Bureau of Investigation; Ms. Eileen Harrington, Associate Director of Marketing Practices, Bureau of Competition, the Federal Trade Commission; and Mr. Bruce Townsend, Special Agent in Charge of Financial Crimes Division, United States Secret Service.

I welcome all of you and we'll just go from my left to the right and start with you, Mr. Kubic, for your opening statement.

STATEMENTS OF THOMAS T. KUBIC, DEPUTY ASSISTANT DIRECTOR, CRIMINAL DIVISION, FEDERAL BUREAU OF INVESTIGATION; BRUCE A. TOWNSEND, SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, UNITED STATES SECRET SERVICE; EILEEN HARRINGTON, ASSOCIATE DIRECTOR OF MARKETING PRACTICES, BUREAU OF COMPETITION, FEDERAL TRADE COMMISSION; AND BRUCE SWARTZ, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. KUBIC. Good morning, Mr. Chairman, and members of the subcommittee. In view of the limited time I have prepared a full statement which I submit for the record.

Mr. STEARNS. By unanimous consent, so directed.

Mr. KUBIC. Thank you. Today as you mentioned, the FBI and the Department of Justice announced the results of a series of investigations that have been on-going nationwide under the code name of "Operation Cyber Loss." These cases were based on information initially developed through the Internet Fraud Complaint Center. The effort was coordinated among our field offices, along with the active participation of the U.S. Postal Service, the U.S. Secret Service, the Internal Revenue Service, the U.S. Attorneys and numerous State and local law enforcement officials.

Internet fraud schemes exposed during these investigations involved more than 56,000 victims nationwide with losses exceeding $117 million. Some of the fraud schemes investigated during "Operation Cyber Loss" were those involving on-line auction fraud which was previously mentioned, the nondelivery of merchandise purchased over the Internet, as well as credit card fraud and identity fraud.

Ninety subjects have been charged with wire fraud, mail fraud, money laundering, bank fraud and software piracy. In all, there were 26 FBI field offices involved in these investigations.

The efforts today are, in fact, a response to the perceived rise in crime and fraud on the Internet. The Internet, as mentioned, is in fact a perfect medium for which the fraudsters can reach a large number of people and maintain a cloak of secrecy over their identity. As a point of reference, the FBI defines Internet fraud as any fraudulent scheme in which the Internet plays a significant role in either the offering of nonexisting goods or services or the payment for those goods and services on-line.

Recognizing this emerging crime problem, the FBI joined in some discussions with the National White Collar Crime Section, rather the White Collar Crime Center, and those discussions led to the May 8, 2000 opening of the Internet Fraud Complaint Center.

Over the past 12 months the Internet Fraud Complaint Center has developed as the central repository for Internet fraud complaints. This Center has advantages over the decentralized system

that previously existed. Often a complaint would be received in a particular police department, initially reviewed, and if it did not reach the standard for a formal criminal investigation, it was merely left there for no further analysis as to other similar and related incidents.

Today, suspected fraud schemes can be reported on-line as they occur by victims throughout the United States and in fact, worldwide. What happens at the Internet Fraud Complaint Center is the supervisory Special Agents, along with Internet fraud specialists review those complaints when they come in and they link those complaints with others that may have been previously received. This information is then quickly disseminated to law enforcement agencies on both the Federal, State and local level.

Let me give you some idea as to the extent of the Center's operation. Over the past year, there were 36,410 complaints that were received at the Center. An analysis of those complaints led to 30,000 validated complaints and referrals to many law enforcement jurisdictions throughout the United States.

The IFCC has done further research and developed a formalized reporting system called an Internet Investigative Report which does, in fact, link the cases, put in the identities of subjects as known and submits that information to law enforcement officers throughout the U.S.

Let me wrap up with making a couple of quick points. Similar in nature to the Neighborhood Community Watch, the Internet Fraud Complaint Center serves as a cyber neighborhood watch where 24 hours a day, 7 days a week, individuals who are victimized by these fraudsters can make a report. That report is then processed and quickly disseminated to the respective jurisdictions.

Second, all of these complaints are very important. One complaint standing alone may not appear to be related, but as demonstrated from the investigations and the arrests made today, a small dollar amount can quickly escalate with the victims' number in the thousands.

In conclusion, the IFCC was an important first step in addressing the threat of Internet fraud. The end result of this effort, I believe will be an Internet where everyone is safe, but the fraudsters.

Thank you.

[The prepared statement of Thomas J. Kubic follows:]

PREPARED STATEMENT OF THOMAS T. KUBIC, DEPUTY ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Good morning, Chairman Stearns, and members of the Subcommittee on Commerce, Trade and Consumer Protection. I am pleased to appear today on behalf of the Federal Bureau of Investigation and share with your subcommittee the FBI's perspective on the Internet fraud crime problem.

Let me begin by emphasizing that the FBI places a high priority on investigating Internet fraud matters and is committed to working with this subcommittee and all of Congress to ensure that law enforcement and the private sector have the necessary tools and protections to combat these crimes. It is only with the valuable cooperation of private sector companies such as those represented here today that efforts to combat Internet fraud will succeed. The FBI recognizes and appreciates the interest and efforts of these and other companies in preventing Internet fraud as well as their willingness to work with law enforcement to address the problem.

I would like to first discuss results of a series of investigations against Internet fraud announced today by the FBI and department of justice, followed by an FBI perspective as to the extent of the Internet fraud crime problem along with the

unique challenges faced by law enforcement in addressing it, and then give you an overview of what the FBI is doing to address the problem including details concerning the Internet fraud complaint center.

As noted above, today, the FBI and the Department of Justice is announcing a nationwide sweep into Internet fraud, code named "Operation Cyber Loss," initiated by the FBI's Internet Fraud Complaint Center (IFCC) and coordinated by FBI offices, U.S. Postal Inspection Service (USPIS), Internal Revenue Service-Criminal Investigative Division, U.S. Customs Service, United States Secret Service, and numerous state and local law enforcement entities. The Internet fraud schemes exposed as part of this investigation represent over 56,000 victims nationwide who suffered cumulative losses in excess of $117 million. Among the Internet fraud schemes highlighted by operation cyber-loss were those involving on-line auction fraud, systemic non-delivery of merchandise purchased over the Internet, credit/debit card fraud, identity theft, various investment and securities frauds, multi-level marketing and ponzi/pyramid schemes. Approximately 90 subjects have been charged as a result of operation cyber-loss for wire fraud, mail fraud, conspiracy to commit fraud, money laundering, bank fraud, and intellectual property rights (software piracy). Twenty-six different FBI field offices throughout the country have been involved in the cyber loss investigation. As is true of Internet fraud in general, subjects and victims involved in this operation were scattered throughout the world. Action taken this week in connection with this operation represents only a small fraction of cases referred by the IFCC and only represent cases culminating in significant prosecutive action.

The schemes identified as part of Operation Cyber-Loss vary widely in type and complexity. They tend to be multi-jurisdictional with subjects and victims scattered across the United States and the world. While many of the schemes involved an element of on-line auction fraud, this was often only one aspect of a subject's fraudulent activities. The cases reflect the nature of fraudsters to migrate from one fraudulent scheme to another, and is indicative of criminal behavior that would only continue to expand if left unaddressed. We will attach to our statement for the record summaries of some of the fraud schemes exposed as part of this operation. It should be pointed out that these summaries do not reflect all of the cases included as part of Operation Cyber Loss since a number of these cases are ongoing and details cannot be provided at this time due to matters being under seal and/or so as not to compromise the investigation.

The IFCC is a joint operation with the FBI and the National White Collar Crime Center (NW3C). The NW3C is a non-profit organization which is partially funded by the Department of Justice. The mission of NW3C is to provide a nationwide support system for the prevention, investigation and prosecution of economic crimes.

A little over a year ago, on May 8, 2000, the IFCC opened its doors to combat the growing problem of fraud over the Internet. The Internet is changing the world as we know it, and promises to change how we buy things, how we communicate, where we get entertainment, news, and weather, where we work, and much, much more while bringing enormous benefits to society. The growth and utilization of the Internet as a communications and commerce tool is unsurpassed in modern history. Current trends reflect this remarkable growth:

- Internet users in the U.S. reached 65 million in 1998, over 100 million in 1999, and is expected to exceed 200 million this year [1]
- Business-to-business e-commerce totaled over $100 billion in 1999 (more than doubling from 1998) and is expected to grow to over one trillion dollars by 2003. Worldwide net commerce, both business-to-business and business-to-consumer, will hit an estimated $6.8 trillion in 2004.[2]

The vast majority of communication and commerce conducted via the Internet is for lawful purposes. However, the Internet is increasingly utilized to foster fraudulent schemes. Just as prior technological advances have brought dramatic improvements for society, they have also created new opportunities for wrongdoing. As worldwide dependence on technology increases, high-tech crime is becoming an increasingly attractive source of revenue for organized crime groups, as well as an attractive option for them to make commercial and financial transactions that support criminal activity. Criminal activity in the cyber world presents a daunting challenge at all levels of law enforcement. In the past, a nation's border acted as a barrier to the development of many criminal enterprises, organizations and conspiracies. Over the past five years, the advent of the Internet as a business and communica-

[1] New York Times, November 12, 1999
[2] Source: Forrester Research, Inc., <http://www.Forrester.com>

tion tool has erased these borders. Cyber criminals and organizations pose significant threats to global commerce and society.

The use of the Internet for criminal purposes is one of the most critical challenges facing the FBI and law enforcement in general. Understanding and using the Internet to combat Internet fraud is essential for law enforcement. The fraud being committed over the Internet is the same type of white collar fraud the FBI has traditionally investigated but poses additional concerns and challenges because of the new environment in which it is located. Internet fraud is defined as any fraudulent scheme in which one or more components of the Internet, such as web sites, chat rooms, and e-mail, play a significant role in offering non-existent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims' funds, access devices, or other items of value to the control of the scheme's perpetrators. The accessability of such an immense audience coupled with the anonymity of the subject, require a different approach. The Internet is a perfect vehicle to locate victims and provide the environment where the victims don't see or speak to the fraudsters. The Internet environment often creates a false sense of security among users leading them to check out opportunities found on the Internet less thoroughly than they might otherwise. Anyone in the privacy of their own home can create a very persuasive vehicle for fraud over the Internet. The expenses associated with the operation of a "home page" and the use of electronic mail (e-mail) are minimal. Con artists do not require the capital to send out mailers, hire people to respond to the mailers, finance and operate toll free numbers. This technology has evolved exponentially over the past few years and will continue to evolve at a tremendous rate.

Internet fraud does not have traditional boundaries as seen in the traditional schemes. No one knows the full extent of the fraud being committed on the Internet. Not all victims report fraud, and those who do, do not report it to one central repository. For traditional fraud schemes the FBI has systems in place to identify and track fraud throughout the country. For example, a con man opens up shop in Chicago, finds a location, obtains phones, hires personnel, and begins to defraud people. When victims don't receive what they were promised and realized that they have been defrauded, they will contact their local field office of the FBI, and provide the complaint information, which will be forwarded to the chicago office (where the fraud is occurring). The FBI in Chicago receives a number of these complaints and initiates an investigation. Fraud over the Internet does not need a physical location, nor personnel, nor telephones. Internet fraud is disjointed, and spread throughout the country. The traditional methods of detecting, reporting, and investigating fraud fail in this virtual environment. Victims of fraud have been unsure of how or where to report what they see or what they have experienced on the Internet. Law enforcement agencies have received complaints in a piecemeal fashion, most not reaching a level to advance the complaint to an investigation. Another problem is venue, without some technical investigatory steps it is difficult to identify the location of a website or the origin of an e-mail.

What makes Internet fraud even more of a concern for law enforcement authorities is the changing demographics of Internet users. In general, according to a recent study, the online population tends to be younger, more affluent, and better educated than the general adult population.[3] But while the 18-34 age group is the largest single age group online—representing 39 percent of the world wide web population[4]—the consensus is that the 50-and-older age group is the fastest-growing age group online.[5] Moreover, according to a recent survey, the 50-and-older group surfed the web 19 percent longer than all web users combined.[6] If older adults spend more time on the Internet, and have more assets than younger adults that are available for discretionary uses such as investment opportunities, they may be more likely to be sought out by online fraudulent schemes, as law enforcement authorities have found with traditional telemarketing fraud schemes. It should therefore not be sur-

---

[3] *See* Rebecca Fairley Raney, "Studies Reach Contradictory Conclusions About the Internet Population," N.Y. Times on the Web, May 10, 1998, <http://www.nytimes.com/library/tech/98/05/cyber/articles/10race.html>.

[4] *See* Matthew Broersma, *supra* note 4.

[5] *See* Erin Kelly, "Mom's Online!," Time, <http://www.pathfinder.com/time/reports/50plus/mother.html> (printed May 12, 1998). Since 1994, surveys have shown that the percentage of 50-and-older Internet users in the United States has increased from 13 percent in 1994 to 16 percent in 1997. *See* Amy Harmon, "Guess Who's Coming Online," N.Y. Times on the Web, March 26, 1998, <http://www.nytimes.com/library/tech/98/03/circuits/articles/26geez.html> (printed April 23, 1998).

[6] *See* "Older Netizens," Los Angeles Times, May 11, 1998, <http://latimes.com/HOME/NEWS/CUTTING/t000044218.1.html>.

prising that a number of older adults who use the Internet are concerned about such schemes preying on their age group.[7]

The Internet provides criminals with a tremendous way to locate numerous victims at minimal costs. The victims never see or speak to the subjects, and often don't know where the subjects are actually located. Crimes committed using computers as a communication or storage device have different personnel and resource implications than similar offenses committed without these tools. Electronic data is perishable—easily deleted, manipulated and modified with little effort. The very nature of the Internet and the rapid pace of technological change in our society result in otherwise traditional fraud schemes becoming magnified when these tools are utilized as part of the scheme. The Internet presents new and significant investigatory challenges for law enforcement at all levels. These challenges include: the need to track down sophisticated users who commit unlawful acts on the Internet while hiding their identities; the need for close coordination among law enforcement agencies; and the need for trained and well-equipped personnel to gather evidence, investigate, and prosecute these cases. Victims are often scattered around the country in different jurisdictions or countries than the subject(s). Subjects located in other countries are increasingly targeting victims in the U.S. utilizing the Internet. Evidence can be stored remotely in locations not in physical proximity to either their owner or the location of criminal activity. In addition, losses suffered by victims in individual jurisdictions may not meet prosecutive thresholds even though total losses through the same scheme may be substantial. In order to subpoena records, utilize electronic surveillance, execute search warrants, seize evidence and examine it in foreign countries, the FBI must rely upon local authorities for assistance. In some cases, local police forces do not understand or cannot cope with technology. In other cases, these nations simply do not have adequate laws regarding cyber crime and are therefore limited in their ability to provide assistance. Our legal attache program provides critical contributions in these matters.

Cyber crime exists across FBI program boundaries and without regard to international borders. Among the FBI program areas impacted by cyber crime are: securities and commodities transactions, prime bank schemes, telemarketing schemes, online banking frauds, government program and private health care fraud schemes, online pharmacy schemes, online auction frauds, identity theft, intellectual property theft, business-to-business frauds, non-delivery of services, Nigerian letter solicitations, credit card fraud, e-commerce and trading, e-commerce and government procurement, online gambling, organized crime/drugs, terrorism, fugitives, purchase and sale of stolen/counterfeit merchandise, child pornography, denial of service attacks, intrusions, money laundering, and as a business tool to transact criminal activity.

To this point, we have discussed in general the potential threat posed by cyber crime, why it has become and will continue to be one of the most significant crime problems, and briefly described some of the myriad facets of cyber crime. I would like to now focus the discussion on the Internet fraud schemes and what the FBI is doing to address this area of cyber crime.

INTERNET FRAUD COMPLAINT CENTER (IFCC)

The development of a proactive strategy to investigate Internet fraud through the establishment of an Internet Fraud Complaint Center (IFCC) as a central repository for complaints was essential. The IFCC was necessary to adequately identify, track, and prosecute new fraudulent schemes on the Internet on a national and international level. It serves as a clearinghouse for the receipt, analysis, and dissemination of complaints concerning frauds perpetrated over the Internet. IFCC personnel collect, analyze, evaluate, and disseminate Internet fraud complaints to the appropriate law enforcement agency. The IFCC provides a mechanism by which the most egregious schemes are identified and addressed through a criminal investigative effort.

The IFCC provides a central analytical repository for complaints regarding Internet fraud, and it acts as a resource for enforcement agencies at all levels of government to include regulatory agencies. It provides analytical support, and aids in the development and provides training modules to address Internet fraud. The FBI and the national white collar crime center (nw3c) cosponsor the IFCC. This partnership is mutually beneficial for both entities in that it allows both agencies to share staffing responsibilities and, by forwarding complaints to FBI field divisions, utilize the FBI's investigative resources to address this new techno crime.

---

[7] *See* Erin Kelly, *supra* note 17.

The IFCC identifies current crime problems, and develops investigative techniques to address newly identified crime trends. The information obtained from the data collected is providing the foundation for the development of a national strategic plan to address Internet fraud.

IFCC's mission is to develop a national strategic plan to address fraud over the Internet, and to provide support to law enforcement and regulatory agencies at all levels of government for fraud that occurs over the Internet. IFCC's purpose is the following:

- To develop a national strategy to address Internet fraud;
- To develop criminal Internet fraud cases and refer for criminal prosecutions companies and individuals responsible;
- To reduce the amount of economic loss by Internet fraud throughout the United States;
- To provide an analytical repository for Internet fraud complaints;
- To receive, analyze and refer all fraudulent activity identified on the Internet;
- To identify current crime trends over the Internet;
- To develop investigative techniques to address those identified crime problems;
- To track fraud facilitated by the Internet and provide analytical support of Internet crime trends;
- To act as an investigative resource for Internet fraud;
- To develop training modules to investigate Internet fraud;
- To develop information packets from complaints generated and forward that information to the appropriate law enforcement agencies.

Public awareness of the existence and purpose of the IFCC is paramount to the success of this effort. The IFCC provides a convenient and easy way for the public to alert authorities of a suspected criminal activity or civil violation. Victims of Internet crime are able to go directly to the IFCC web site (WWW.IFCCFBI.GOV) to submit their complaint information, relieving considerable frustration for the victim in trying to decide which law enforcement agency should receive the complaint. The FBI web page also aids in this effort. A detailed explanation of the complaint center, its purpose and contact numbers, is provided so that consumers can report Internet fraud. The FBI web page provides victims with a hyperlink to the IFCC web page. Many other consumer protection web sites which provide information on fraud matters contain links to the IFCC web site.

The FBI has also established an Internet fraud council working group consisting of federal and state law enforcement agencies, international law enforcement agencies, federal and state enforcement agencies, and representatives of the private business sector. The group's purpose is to create a network to share information, discuss pertinent issues, recommend legislative solutions, and obtain the maximum benefit for all participating members.

During the start-up phase of IFCC, the entire staff processed incoming complaints and forwarded them to law enforcement agencies. In its first year of operation, the IFCC received 36,410 complaints, of those complaints, 5,907 were invalid, incomplete or duplicative, resulting in 30,503 valid criminal complaints. Those complaints were referred to an average of two to three law enforcement agencies. This referral process has spawned hundreds of criminal investigations throughout the country. The FBI staff at the IFCC have begun to use the data to identify multiple victims, various crime trends and same subject cases thus initiating the investigative phase of the center's operations. This process wasn't fully functional until January 1, 2001. Utilizing this process in which the IFCC staff draft Internet investigative reports and forwards those reports to multiple law enforcement agencies, the IFCC has investigated and referred 545 investigative reports encompassing over 3,000 complaints to 51 of 56 FBI field divisions and 1,507 local and state law enforcement agencies. IFCC has also referred 41 cases encompassing over 200 complaints to international law enforcement agencies. The IFCC has received complaints of victims from 89 different countries.

Auction fraud is by far the most reported Internet fraud, comprising nearly two-thirds of all complaints. Payment for merchandise that was never delivered accounts for 22% of complaints, and credit and debit card fraud makeup almost 5% of complaints. Another 5% of complaints stem from various types of investment frauds and confidence fraud schemes such as home improvement scams and multi-level marketing schemes. It has been the experience of the FBI that further investigation into these complaints often reveals a variety of frauds being perpetrated by subjects. Subjects engaged in one type of fraud scheme such as on-line auction fraud are frequently involved in other types of fraud schemes such as bank fraud, investment frauds and/or ponzi/pyramid schemes.

Businesses that conduct a significant amount of commerce over the Internet are exposed to losses in the millions of dollars due to various fraud schemes. With as-

sistance from the private sector, the IFCC is developing a business-friendly system for rapid data transfer of multiple complaints in an effort to better serve these crime victim-companies' needs. This process will permit the Internet companies that are experiencing these losses to file bulk complaints and those complaints will then be distributed by IFCC to the appropriate law enforcement agencies.

In effect, the IFCC operates as part of a cyber community watch in which the self policing efforts of honest and vigilant Internet users and Internet service providers result in potential fraudulent activity over the Internet being brought to the attention of law enforcement through the IFCC. The IFCC does much more than just collect complaint information. It ensures that the information, along with additional investigative information developed by IFCC personnel, is disseminated to the appropriate agencies, and that identified fraud schemes can be prevented or mitigated. The IFCC processes all complaints it receives regardless of the alleged dollar loss. Many of the complaints received do not allege losses which meet minimum dollar thresholds for federal prosecution, but they can often be successfully worked by local law enforcement agencies. At a minimum, they form part of a database which enables IFCC to potentially connect them with a widespread fraud scheme and/or organized criminal group. In this light, all complaints alleging fraud over the Internet are important. No victim should feel like any loss they suffered is too insignificant to report. It is only by victims and businesses reporting potentially fraudulent activity that law enforcement becomes aware of it and can take action. This point is made clear by action taken today by the FBI and other law enforcement agencies.

OPERATION CYBER-LOSS

The success of the IFCC was demonstrated through IFCC's key role in operation cyber-loss.

The FBI recognizes that the IFCC and initiatives such as operation cyber loss, while important first steps in addressing Internet fraud, represent merely the tip of the iceberg when it comes to the threat posed by cyber crime. They are a piece of a developing comprehensive FBI strategic plan addressing all aspects of cyber crime which will allow the FBI and law enforcement to effectively and efficiently maintain a high level response capability and prosecutorial success in areas where either: (1) a computer system and/or the Internet are used in furtherance of a crime; or (2) a computer system is the victim of a crime. The use of a computer system or the Internet in furtherance of crime is not limited to one FBI program area but is increasingly found in criminal investigative division and national infrastructure protection center cases. In many instances where a computer system is seriously targeted, the purpose of the attack is to facilitate ongoing criminal activity.

The FBI is committed to ensuring the safety and security of those who use the Internet while maintaining an appreciation of the Internet as an important medium for commerce and communication. Focused law enforcement efforts will promote greater consumer confidence and trust in the Internet as a safe and secure medium of commerce and communication. The IFCC serves as an example of an innovative approach to an emerging crime problem. It provides the benefits of community policing, forging an effective partnership between law enforcement at all levels, ordinary citizens, consumer protection organizations such as the NW3C, and the business community. Addressing the emerging and dynamic threat of Internet fraud requires contributions from all segments of our society. The FBI serves to facilitate and coordinate this collaborative effort. Thank you.

Mr. STEARNS. Thank you.

Mr. Townsend.

STATEMENT OF BRUCE A. TOWNSEND

Mr. TOWNSEND. Mr. Chairman, members of the subcommittee, thank you for the opportunity to address the subcommittee on the subject of on-line fraud and associated crimes and the Secret Service's efforts to combat this problem.

I've prepared a comprehensive statement for the record and with the subcommittee's permission I will summarize it at this time.

Mr. STEARNS. By unanimous consent, so entered.

Mr. TOWNSEND. In addition to providing the highest level of physical protection to our Nation's leaders, the Secret Service exercises broad, investigative jurisdiction over a variety of financial

crimes. As the original guardian of our Nation's financial payment systems, the Secret Service has a long history of pursuing those who victimize our financial institutions and law abiding citizens.

In recent years, the combination of the information technology revolution and the effects of globalization have caused the investigative mission of the Secret Service to evolve in a manner which cannot be overstated.

Mr. Chairman, we in the Secret Service applaud your efforts in convening this hearing today. We stand ready to work with you and all the members of the subcommittee in addressing this issue.

It is our belief that hearings such as this will be the catalyst to bring together the resources of the State and Federal Governments in addition to the private sector in the unified response to this issue.

Burgeoning use of the Internet and advanced technologies has promoted greater competition within the financial sector. Although this provides benefits to the consumer through readily available credit and consumer-oriented financial services, it also creates a rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders.

Information collection has become a common by-product of the newly emerging e-commerce. Internet purchases, credit card sales and other forms of electronic transactions are being captured, stored and analyzed by entrepreneurs intent on increasing their market share. The result is an entirely new business sector being created which promotes the buying and selling of personal information.

With the advent of the Internet, companies have been created for the sole purpose of data mining, data warehousing and brokering of this information. These companies collect a wealth of information about consumers, including information as confidential as their medical histories.

Consumers routinely provide personal, financial and other types of information to companies engaged in business on the Internet. Consumers may not realize that the information they provide in credit card applications, loan applications or with merchants they patronize is a valuable commodity in this new age of information trading.

The Internet provides the anonymity all criminals desire. In the past, fraud schemes required false identification documents and necessitated some face to face exchange of information. Now with a laptop and modem, criminals are capable of perpetrating a variety of financial crimes without identity documents through the use of stolen personal information.

The Secret Service has investigated cases where cyber criminals have hacked into Internet merchant sites and stolen personal information and credit card account numbers of their customers. These account numbers are then used with supporting personal information to order merchandise which can be sent throughout the world. Many account holders are not aware that their credit card account has been compromised until they receive their billing statement.

Today, we are faced with another new challenge, that of identity theft. Time and time again criminals have demonstrated the ability to obtain information from businesses conducting business on the

Internet. The information has been used to facilitate account take-over schemes and other similar frauds.

It has become a frightening reality that one individual can literally take over another individual's financial identity without the true victim's knowledge. Using compromised financial identities of people from all walks of life, criminals purchase everything from cars to computers to homes. Presently, Secret Service Agents are investigating an identity theft case involving fraudulent credit card purchases. During the course of the investigation, agents have determined that the suspects used a stolen identity of an innocent party to obtain a $400,000 mortgage to purchase a home. Further investigation has determined that the suspects were in the process of obtaining seven additional home loans, using other identities with an aggregate value of $2.1 million.

The Secret Service has a long history of conducting investigations into various fraud schemes and high tech crimes, from hackers, freakers and carders in the mid-1980's to the masters of deception group in the early 1990's, to the New York busboy CEO identity theft case in recent weeks. The Secret Service has been among those at the forefront of cyber crime investigations.

We in the Secret Service pledge to continue to work with the Congress, with our domestic and global law enforcement partners and with the private sector to stay abreast of emerging high tech threats to the citizens we serve.

Mr. Chairman, this concludes my prepared statement. I'd be happy to answer any questions that you or other members of the subcommittee may have.

Thank you.

[The prepared statement of Bruce A. Townsend follows:]

PREPARED STATEMENT OF BRUCE A. TOWNSEND, SPECIAL AGENT IN CHARGE-FINANCIAL CRIMES DIVISION, U.S. SECRET SERVICE

Mr. Chairman, members of the Subcommittee, thank you for the opportunity to address the Subcommittee on the subject of on-line fraud and associated crimes and the Secret Service's efforts to combat this problem.

In addition to providing the highest level of physical protection to our nation's leaders, the Secret Service exercises broad investigative jurisdiction over a variety of financial crimes. As the original guardian of our Nation's financial payment systems, the Secret Service has a long history of pursuing those who would victimize our financial institutions and law abiding citizens. In recent years, the combination of the information technology revolution and the effects of globalization have caused the investigative mission of the Secret Service to evolve in a manner that cannot be overstated.

Mr. Chairman, we in the Secret Service applaud your efforts in convening this hearing today. We stand ready to work with you and all the members of the subcommittee in addressing this issue. It is our belief that hearings such as this will be the catalyst to bring together the resources of the state and Federal Governments, and the private sector in a unified response to this issue.

Burgeoning use of the Internet and advanced technologies has promoted greater competition within the financial sector. Although this provides benefits to the consumer through readily available credit, and consumer oriented financial services, it also creates a rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders.

Information collection has become a common byproduct of the newly emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by entrepreneurs intent on increasing their market share. The result is a growing business sector for promoting the buying and selling of personal information.

With the advent of the Internet, companies have been created for the sole purpose of data mining, data warehousing, and brokering of this information. These compa-

nies collect a wealth of information about consumers, including information as confidential as their medical histories.

Consumers routinely provide personal, financial, and health information to companies engaged in business on the Internet. Consumers may not realize that the information they provide in credit card applications, loan applications, or with merchants they patronize, is a valuable commodity in this new age of information trading.

The Internet provides the anonymity all criminals desire. In the past, fraud schemes required false identification documents, and necessitated a "face to face" exchange of information and identity verification. Now with just a laptop and a modem, criminals are capable of perpetrating a variety of financial crimes without identity documents through the use of stolen personal information.

The Secret Service has investigated several cases where cyber criminals have hacked into Internet merchants' sites and stolen the personal information and credit card account numbers of their customers. These account numbers are then used with supporting personal information to order merchandise that is then shipped throughout the world. Most account holders are not aware that their credit card accounts have been compromised until they receive their billing statement.

In an investigation conducted in April 2001, Secret Service Agents from the Lexington, Kentucky, Resident Office, along with their local law enforcement partners from the Richmond, Kentucky, Police Department, arrested a suspect who was operating an on-line auction selling counterfeit sports memorabilia. During this investigation it was learned that the suspect had fraudulently opened a number of credit card accounts utilizing the personal information of individuals with whom he had dealt over the Internet.

Cyber criminals are also using information hacked from sites on the Internet to extort money from companies. It is not unprecedented for international hackers to hack into business accounts, steal thousands of credit card account numbers along with the accompanying personal identifiers, then threaten the companies with exposure unless the hackers are paid a substantial amount of money.

Today we are faced with another new challenge—that of identity theft. Time and time again, criminals have demonstrated the ability to obtain information from businesses conducting commerce on the Internet. This information has been used to facilitate account takeover schemes and other similar frauds. It has become a frightening reality that one individual can literally take over another individual's financial identity without the victim's knowledge.

We in the Secret Service view identity theft as a disturbing combination of old schemes and abuse of emerging technologies. However, it should be clear—this crime is about more than the theft of money or property. This crime is about the theft of something that cannot be so easily replaced—a person's good name, a reputation in the community—years of hard work and commitment to goals. Make no mistake about it, this crime is a particularly invasive crime that can leave victims picking up the pieces of their lives for months or years afterward.

In an investigation that illustrates the potential for significant losses to the public, agents of the Secret Service Los Angeles International Fraud Task Force recently arrested four suspects for their role in a scheme that involved fraudulently opening lines of credit for six different businesses. Further investigation revealed that the businesses were fictitious, and the individual identities associated with them had been fraudulently taken over by the suspects. It was also discovered that the suspects had used the personal identifiers of these supposed company officers to obtain auto and business loans, student loans, and open credit card accounts, resulting in an actual loss of more than $1.4 million. Pursuant to the execution of several seizure warrants, more than $360,000 cash and three luxury vehicles were seized from the suspects for forfeiture. A fifth suspect could not be located, and it has since been determined that he has fled to Nigeria.

Congress has already taken an important step in providing increased protection for the victims of identity theft through the enhancements made to Title 18, United States Code, Section 1028 by the Identity Theft and Assumption Deterrence Act, which was signed into law in October of 1998.

This law accomplished four things simultaneously. First, it identified people whose credit had been compromised as true victims. Historically with financial crimes such as bank fraud or credit card fraud, the victim identified by statute, was the person, business or financial institution that lost the money. All too often the victims of identity theft whose credit was destroyed, were not recognized as victims. This is no longer the case.

Second, this law established the Federal Trade Commission (FTC) as the one central point of contact for these victims to report all instances of identity theft. This collection of data on all ID theft cases allows for the identification of systemic weak-

nesses and the ability of law enforcement to retrieve investigative data from one central location. It further allows the FTC to provide people with the information and assistance they need in order to take the steps necessary to correct their credit records.

Third, this law provided increased sentencing potential and enhanced asset forfeiture provisions. These enhancements help to reach prosecutorial thresholds and allow for the return of funds to victims.

Lastly, this law closed a loophole in Title 18, United States Code, Section 1028 by making it illegal to steal another person's personal identification information with the intent to commit a violation. Previously, under Section 1028 only the production or possession of false identity documents was prohibited. With advances in technology such as E-Commerce and the Internet, criminals today do not need actual documents to assume an identity.

We believe this legislation is an important factor in bringing together the Federal and state governments in a focused and unified response to the identity theft problem. Today, law enforcement, regulatory and community assistance organizations have joined forces through a variety of working groups, task forces, and information sharing initiatives to assist victims of identity theft. Victims no longer have to feel abandoned, with no where to turn.

A case in point concerns the investigation recently conducted by our New York Field Office's Electronic Crimes Task Force and the New York City Police Department concerning the compromised credit accounts of high profile businessmen. The investigation originated in December of 2000, when the office was notified that an Assistant United States Attorney for the Southern District of New York had a personal credit card account compromised. In February, the office was contacted again by a private party investigating the identity takeover and attempted brokerage account theft of a prominent corporate CEO in California. A subsequent joint investigation by the Secret Service Field Office and the New York Police Department determined that the credit card accounts of many of America's wealthiest Chief Executive Officers, as well as many other citizens, had also been compromised. This investigation determined that by utilizing the Internet and cellular telephones, the perpetrators were able to obtain the account numbers and had then established fictitious addresses for the corporations in order to conduct fraudulent transactions. Furthermore, attempts were also made to transfer approximately $22 million from legitimate brokerage and corporate accounts belonging to the victims, into fraudulently established accounts for conversion to the perpetrators' own use.

The Secret Service continues to attack identity theft by aggressively pursuing core violations. It is by the successful investigation of criminals involved in financial and computer fraud that we are able to identify and suppress identity theft.

Using compromised financial identities of people from all walks of life, criminals purchase everything from cars to computers to homes. Agents in our Birmingham Field Office are working an identity theft case involving $40,000 in fraudulent credit card purchases. During this investigation, agents have determined that the suspects used the stolen identity of an innocent party to obtain a $400,000 mortgage to purchase a home in the Birmingham area. Further investigation has determined that the suspects were in the process of obtaining seven additional home loans using other identities, with an aggregate value of $2.1 million.

As stated earlier, identity theft, and the use of false identification has become an integral component of most financial criminal activity. In order to be successful in suppressing identity theft, we believe law enforcement agencies should continue to focus their energy and available resources on the criminal activities that incorporate the misuse or theft of identification information. The Secret Service has achieved success through a consistent three -tiered process of aggressive pro-active investigations, identification of systemic weaknesses, and partnerships with the financial sector.

Our investigative program focuses on three areas of criminal schemes within our core expertise. First, the Secret Service emphasizes the investigation of counterfeit instruments. By counterfeit instruments, I am referring to counterfeit currency, counterfeit checks—both commercial and government—counterfeit credit cards, counterfeit stocks or bonds, and virtually any negotiable instrument that can be counterfeited. Many counterfeiting schemes would not be possible without the compromise of the financial identities of innocent victims. Second, the Secret Service targets organized criminal groups that are engaged in financial crimes on both a national and international scale. Again we see many of these groups, most notably the Nigerian and Asian organized criminal groups, prolific in their use of stolen financial and personal information to further their financial crime activity.

Finally, we focus our resources on community impact cases. The Secret Service works in concert with the state, county, and local police departments to ensure our

resources are being targeted to those criminal areas that are of a high concern to the local citizenry. Further, we work very closely with both federal and local prosecutors to ensure that our investigations are relevant, topical and prosecutable under existing guidelines. No area today is more relevant or topical than that of identity theft.

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement who generally respond first to criminal activities. By working closely with other federal, state, and local law enforcement, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries.

This partnership approach to law enforcement is exemplified by our financial crimes task forces located throughout the country. Each of these task forces pools the personnel and technical resources to maximize the expertise of each participating law enforcement agency.

In addition to our interdependent working relationship with law enforcement on all levels, our partnership with the private sector has proved invaluable. Representatives from numerous commercial sectors, including the financial, telecommunications, and computer industries, have all pledged their support for finding ways to ensure consumer protection while minimizing corporate losses. The Secret Service has entered into several cooperative efforts with representatives of the financial sector to address challenges posed by new and emerging technologies.

In conjunction with these technological advances, the Secret Service is actively involved in a number of government sponsored initiatives. At the request of the Attorney General, the Secret Service joined an Identity Theft Subcommittee of the Attorney General's White Collar Crime Council.

This group, which is made up of federal and state law enforcement, regulatory, and professional agencies, meets regularly to discuss and coordinate investigative and prosecutorial strategies as well as consumer education programs.

The Secret Service has a long history of conducting investigations into hi-tech crimes. From "hackers," "freakers," and "carders," in the mid 1980s to the "Masters of Deception" group in the early 1990s, to the New York "Busboy" CEO identity theft case described above, the Secret Service has been among those at the forefront of cybercrime investigations.

We in the Secret Service pledge to continue to work with the Congress, with our domestic and global law enforcement partners, and with the private sector, to stay abreast of emerging hi-tech threats to the citizens we serve.

Mr. Chairman, this concludes my prepared statement. I would be happy to answer any questions that you or any other member of the subcommittee may have. Thank you.

Mr. STEARNS. I thank you.

Ms. Harrington?

STATEMENT OF EILEEN HARRINGTON

Ms. HARRINGTON. Thank you, Mr. Chairman. I am Eileen Harrington of the FTC's Bureau of Consumer Protection. The Commission's full statement has been submitted for the record and I will summarize.

We have a 6 point strategy at the FTC for combatting on-line fraud. First, know and analyze the problem. Second, use targeted law enforcement actions to halt egregious fraud. Third, give consumers easy access to fraud prevention information and a simple way to tell law enforcement when they fall victim to on-line or off-line fraud. Fourth, share complaint data with U.S. and worldwide law enforcers. Fifth, provide onsite, hands on Internet investigation training for our law enforcement partners. And last, strengthen working relationships throughout the international consumer protection law enforcement network to address the increasing trend toward cross border on-line fraud.

Here is how we are implementing this strategy. In 1995, the Commission held several weeks of hearings to explore the impact

of new technologies and globalization on competition and consumer protection. We gathered the best minds from every sector to share their expertise as we set about developing a plan to attack what we already saw as a boom in high tech fraud.

From those hearings we developed our plan and set about our work. And since those first hearings, the FTC has held numerous follow-up workshops bringing together law enforcers, regulators, policymakers and business and consumer groups to study and make recommendations on specific on-line issues such as pretexting and identity theft.

As the Nation's leading consumer protection agency, the FTC is committed to the on-going work of study and analysis of the enormous benefits and worrisome problems that flow from e-commerce.

The FTC brought the first Federal law enforcement action against a scam using the Internet. That was in 1994 before there was even a worldwide web. Since then, we have brought over 150 additional actions to stop almost 600 defendants who are engaged in fraud and deception using the Internet. In these cases Federal courts have ordered more than $180 million in restitution to victims and at the FTC's request, have frozen millions and millions of dollars of additional proceeds in cases still in litigation.

In addition, the FTC has organized and led nine enforcement sweeps targeting various kinds of on-line fraud and deception and these sweeps have resulted in hundreds of other actions by our enforcement partners. For example, in 2000, the FTC organized topten.com, the first international law enforcement targeting Internet fraud. In this year-long effort, law enforcers from five Federal agencies, nine other countries and 23 States brought 251 enforcement actions against on-line scammers.

In 1997, the FTC established its Consumer Response Center to provide consumers with immediate access to fraud prevention and other consumer information and a one stop shop for filing consumer complaints. Consumers can reach the FTC's Consumer Response Center by calling our toll free number, by going on-line to file a complaint or by using traditional means like fax and letters. Today, the FTC handles 50,000 complaints and inquiries from consumers each month.

Also, in 1997, the Commission launched the Consumer Sentinel which is a web-based fraud complaint data base. The FTC provides free real-time access to this fully searchable data base which with over 300,000 fraud complaints is the largest of its kind in North America. Every law enforcement agency in the United States and Canada and over 300 agencies now use Consumer Sentinel.

The data base and the analytical tools that come with it enable law enforcers to know immediately when consumers in their jurisdictions complain of fraud or when subjects in their jurisdictions are complained of. And it also enables law enforcers to alert one another to on-going investigations and to pool other investigational resources. In short, Consumer Sentinel uses the Internet technology to give law enforcement a leg up in catching Internet crooks.

Since 1999, the FTC has operated the National Clearinghouse for ID Theft complaints and just last year alone we received about 50,000 complaints about ID theft. Consumers can call our toll-free ID Theft Hotline for information about what to do if they fall vic-

tim to ID theft and they immediately receive expert counseling about steps that they should take. Their complaints are also made available immediately through Consumer Sentinel.

The Commission has pioneered new investigative techniques to track down those responsible for fraud on the Internet and FTC staff conducts Internet training, Internet investigation training, throughout the country and in other parts of the world on an ongoing basis. For example, in the past year, we provided training to enforcers in Illinois, in Tennessee, in California and today, Mr. Chairman, coincidentally, our trainers are in Tallahassee conducting a training session.

We've also trained authorities from our law enforcement partner agencies throughout the world. Twenty-three other countries have received Internet investigation training from the FTC.

In 1996, we developed the law enforcement surf protocol and since then we have organized and led 27 law enforcement surfs, looking at particular problems on the Internet and sending the warning message to on-line crooks that law enforcement is there and will follow-up with tough enforcement.

The FTC's Internet Rapid Response Team uses all of these tools to respond quickly when we see particularly egregious high tech fraud. For example, last October in the space of a few days, we received hundreds of complaints about a sophisticated on-line billing scam, and within a matter of weeks, fully investigated it, went to court, got an order halting the scam and located the perpetrators in Great Britain and Australia and used our international enforcement network to get service on them and freeze their assets.

We continue to work closely at the FTC with other enforcement agencies. At present we have an Inspector from the United States Postal Inspection Service on detail who is the manager of our Consumer Sentinel project and we are very pleased that we are being joined at the FTC by an Agent on detail from the Secret Service to work exclusively on the ID theft area which we commend the Secret Service for taking the lead in.

We are a small agency with a big mission. As we often say, we live in a target rich environment and only by working collaboratively can enforcers here and throughout the world give their citizens the confidence and protection they deserve as they increasingly turn to the Internet to conduct their life's business.

Thank you, Mr. Chairman.

[The prepared statement of Eileen Harrington follows:]

PREPARED STATEMENT OF EILEEN HARRINGTON, ASSOCIATE DIRECTOR, DIVISION OF MARKETING PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. Chairman, I am Eileen Harrington, Associate Director of the Division of Marketing Practices in the Federal Trade Commission's Bureau of Consumer Protection.[1] At the Committee's request, my remarks will focus primarily on the FTC's efforts to combat fraud on the Internet. I will also touch on two other specific areas of concern both to the Committee and the Commission, namely, identity theft and "pretexting."

Fraud—whether on the Internet or in the "brick and mortar" world—probably needs little explanation, but it may be useful to clarify what the terms "identity

[1] The views expressed in this statement represent the views of the Commission. My responses to any questions you may have are my own and are not necessarily those of the Commission or any Commissioner.

theft" and "pretexting" signify. Identity theft is use by a thief, unbeknownst to his victim, of the victim's name, social security number or other personal identifying information, to open accounts and rack up huge debts for goods and services. Identity theft certainly predates the Internet, and although identity thieves are finding ways to exploit this new tool, often this pernicious practice utilizes rather primitive low-tech means, such as intercepting a victim's mail, or scavenging personal information from a victim's trash. "Pretexting" is a term coined by the private investigation industry, and refers to the practice of obtaining personal information under false pretenses. For example, an investigator who obtains a bank account balance by posing as the account holder would be engaged in pretexting. This tactic is perhaps as old as the private investigation industry itself. But it appears to be gaining in popularity—especially in the burgeoning Internet marketplace—because of the booming market for comprehensive personal information.

I. INTRODUCTION AND BACKGROUND

A. The FTC and its Law Enforcement Authority

The FTC is the federal government's primary consumer protection agency. While most federal agencies have jurisdiction over a specific market sector, the Commission's jurisdiction extends over nearly the entire economy, including business and consumer transactions on the Internet.[2]

Under the Federal Trade Commission Act,[3] the agency's mandate is to take action against "unfair or deceptive acts or practices" and to promote vigorous competition in the marketplace. The FTC Act authorizes the Commission to halt deception through civil actions filed by its own attorneys in federal district court, as well as through administrative cease and desist actions.[4] Typically these civil actions seek preliminary and permanent injunctions to halt the targeted illegal activity, as well as redress for injured consumers. Where redress is impracticable, Commission actions generally seek disgorgement to the U.S. Treasury of defendants' ill-gotten gains. As discussed below, these tools have proven to be effective in fighting a broad array of fraudulent schemes on the Internet, in spite of the sheer size and reach of the Internet.

In addition, the FTC has specific statutory authority with respect to identity theft and pretexting. Under the Identity Theft Assumption and Deterrence Act of 1998 the agency is charged, among other things, with responsibility to create and maintain a central clearinghouse for identity theft complaints. The Gramm-Leach-Bliley Act charges the FTC and other agencies with responsibility to ensure that financial institutions protect the privacy of consumers' personal financial information.[5]

B. The Growth of Ecommerce and Internet Fraud.

The growth of the Internet and ecommerce has been explosive. The number of American adults with Internet access grew from about 88 million in mid-2000 to more than 104 million at the end of the year.[6] The Census Bureau of the Department of Commerce estimated that in the fourth quarter of 2000, not adjusted for seasonal, holiday, and trading-day differences, online retail sales were $8.686 bil-

---

[2] The FTC has limited or no jurisdiction over specified types of entities and activities. These include banks, savings associations, and federal credit unions; regulated common carriers; air carriers; non-retail sales of livestock and meat products under the Packers and Stockyards Act; certain activities of nonprofit corporations; and the business of insurance. *See, e.g.,* 15 U.S.C. §§ 44, 45, 46 (FTC Act); 15 U.S.C. § 21 (Clayton Act); 7 U.S.C. § 227 (Packers and Stockyards Act); 15 U.S.C. § 1011 *et seq.* (McCarran-Ferguson Act).

[3] 15 U.S.C. § 45(a). The Commission also has responsibilities under more than 45 additional statutes, *e.g.,* the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.,* which establishes important privacy protections for consumers' sensitive financial information; the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.,* which mandates disclosures of credit terms; and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et. seq.,* which provides for the correction of billing errors on credit accounts. 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.

[4] 15 U.S.C. §§ 45(a) and 53(b).

[5] 15 U.S.C. §§ 6801-6809. In addition to the FTC, the Federal banking agencies, the National Credit Union Administration, the Treasury Department, and the Securities and Exchange Commission have responsibilities under the Gramm-Leach-Bliley Act.

[6] Pew Internet and American Life Project, *More Online, Doing More* (reported at http://www.pewinternet.org/reports/toc.asp?Report=30) (comparison of tracking survey data in May and June with data from Thanksgiving and Christmas indicates that the number of American adults with Internet access grew fr

lion, an increase of 67.1 percent from the 4th quarter of 1999.[7] Total ecommerce sales for 2000 were an estimated $25.8 billion, .8 percent of all sales.[8]

Unfortunately, but not surprisingly, the boom in ecommerce has created fertile ground for fraud. The Commission's experience is that fraud operators are always among the first to appreciate the potential of a new technology to exploit and deceive consumers. Long-distance telemarketing attracted con artists when it was introduced in the 1970's. They swarmed to pay-per-call technology when it became available in the late 1980's. Internet technology is the latest draw for opportunistic predators who specialize in fraud. The rapid rise in the number of consumer complaints related to online fraud and deception bears this out: in 1997, the Commission received fewer than 1,000 Internet fraud complaints; a year later, the number had increased eight-fold. In 2000, over 25,000 complaints—roughly 26 percent of all fraud complaints logged into the FTC's complaint database, "Consumer Sentinel," by various organizations that year—related to online fraud and deception. The need—and challenge—is to act quickly to stem this trend while the online marketplace is still young.

C. The FTC's Response to Protecting Consumers in the Online Marketplace

Stretching its available resources to combat the growing problem of Internet fraud and deception, the Commission has targeted a wide array of online consumer protection problems. This effort has produced significant results. Since 1994 , the Commission has brought 182 Internet-related cases against over 593 defendants. It obtained injunctions stopping the illegal schemes, and ordering more than $180 million in redress or disgorgement,[9] and obtained orders freezing millions more in cases that are still in litigation. Its federal district court actions alone have stopped consumer injury from Internet schemes with estimated annual sales of over $250 million.[10]

II. CHALLENGES POSED BY INTERNET FRAUD

The Commission faces a host of novel challenges in its efforts to combat fraud and deception online. Traditional scams—such as pyramid schemes and false product claims " thrive on the Internet. Moreover, the architecture of the Internet itself has given rise to new high-tech scams that were not possible before development of the Internet. Both traditional scams and and the innovative ones exploit the global reach and instantaneous speed of the Internet. In addition, the Internet enables con artists to cloak themselves in anonymity, which makes it necessary for law enforcement authorities to act much more quickly to stop newly-emerging deceptive schemes before the perpetrators disappear. And because the Internet transcends national boundaries, law enforcement authorities must be more creative and cooperative to successfully combat online fraud. These novel challenges are discussed in greater detail below.

A. Combating Internet Fraud Requires New Methods of Collecting and Analyzing Information.

The Commission is developing new methods of collecting and analyzing information about both the offline and online marketplace, drawing upon the power of new technology itself. A central part of this effort is Consumer Sentinel, a web-based consumer complaint database and law enforcement investigative tool.[11] Consumer Sentinel receives complaints about all sorts of transactions, whether on the Internet or in the "brick and mortar" world. The complaints come into Consumer Sentinel from the FTC's Consumer Response Center ("CRC"), which processes both telephone and mail inquiries and complaints.[12] For those consumers who prefer the online environment, an electronic complaint form at www.ftc.gov, first available in May of

---

[7] Reported at www.census.gov/mrts/www/current.html).

[8] *Id.*

[9] To date the Commission has collected more than $55 million in redress for victims of Internet fraud and deception.

[10] These figures are based on estimated annual fraudulent sales by defendants in the twelve months prior to filing the complaint. Fraudulent sales figures are based on, among other things, financial statements, company records, receiver reports, and deposition testimony of company officials.

[11] *See* www.consumer.gov/sentinel.

[12] The CRC now receives over 12,000 inquiries and complaints per week. They cover a broad spectrum—everything from complaints about get-rich-quick telemarketing scams and online auction fraud, to questions about consumer rights under various credit statutes and requests for educational materials. Counselors record complaint data, provide information to assist consumers in resolving their complaints, and answer their inquiries.

1998, permits consumers to channel information about potential scams directly to the CRC and the fraud database.

Consumer Sentinel also benefits from the contributions of many public and private partners. It receives data from other public and private consumer organizations, including 64 local offices of the Better Business Bureaus across the nation, the National Consumers League's National Fraud Information Center, and Project Phonebusters in Canada. Additionally, a U.S. Postal Inspector has served for the past year as the program manager, and the U.S. Postal Inspection Service just signed an agreement to begin sharing consumer complaint data from its central fraud database with Consumer Sentinel.

The Commission provides secure access to this data over the Internet, free of charge, to over 300 U.S., Canadian, and Australian law enforcement organizations—including the Department of Justice, U.S. Attorneys' offices, the Federal Bureau of Investigation, the Securities and Exchange Commission, the Secret Service, the U.S. Postal Inspection Service, the Internal Revenue Service, the offices of all 50 state Attorneys General, local sheriffs and prosecutors, the Royal Canadian Mounted Police, and the Australian Competition and Consumer Commission. Consumer Sentinel is a dynamic online law enforcement tool to use against all types of fraud, especially online fraud.[13]

The central role that Consumer Sentinel plays in the Commission's law enforcement is exemplified by "Operation Top Ten Dot Cons," the Commission's latest broad "sweep" of fraudulent and deceptive Internet scams. In a year-long law enforcement effort, the FTC and four other U.S. federal agencies,[14] consumer protection organizations from 9 countries,[15] and 23 states[16] announced 251 law enforcement actions against online scammers. The FTC brought 54 of the cases.[17] The top 10 Internet or online scams, identified through analysis of complaint data in the Consumer Sentinel database, were:

- Internet Auction Fraud
- Internet Service Provider Scams
- Internet Web Site Design/Promotions ("Web Cramming")[18]
- Internet Information and Adult Services (unauthorized credit card charges)
- Pyramid Scams
- Business Opportunities and Work-At-Home Scams
- Investment Schemes and Get-Rich-Quick Scams
- Travel/Vacation Fraud
- Telephone/Pay-Per-Call Solicitation Frauds (including modem dialers and videotext)[19]
- Health Care Frauds

The Consumer Sentinel data enabled the FTC and the other enforcement agencies that joined us in this project both in the U.S. and abroad to identify not only the top ten types of scams, but also the specific companies generating the highest levels of complaints about each of those types of scams. These companies became the tar-

---

[13] In 1998, the Interagency Resources Management Conference Award recognized Consumer Sentinel as an exceptional initiative to improve government service.

[14] U.S. agencies participating included the Commodity Futures Trading Commission, the Department of Justice, the Securities and Exchange Commission and the United States Postal Inspection Service.

[15] Participants in "Operation Top Ten Dot Cons" included consumer protection agencies from Australia, Canada, Finland, Germany, Ireland, New Zealand, Norway, the United Kingdom and the United States.

[16] Cases were brought by the Attorneys General of Arizona, Colorado, Florida, Illinois, Iowa, Indiana, Louisiana, Maryland, Massachusetts, Michigan, Missouri, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, Tennessee, Texas, and Washington. Consumer protection offices in West Virginia, and Wisconsin also took action, as did the Louisiana Department of Justice, the Oklahoma Department of Securities, and the Washington State Securities Division.

[17] The SEC's contribution to this project consisted of 77 cases.

[18] "Web cramming" is a type of unauthorized billing scam. Web crammers call their victims—often small businesses—and offer a "free" Web page; then they start billing the victims, typically on their monthly telephone statements, without authorization. In many cases the small business victims are not even aware that they have a web site or are paying for one.

[19] Telephone/Pay-Per-Call Solicitation Frauds are schemes that exploit the telephone billing and collection system to charge consumers for telephone-based entertainment programs ("audiotext" in industry parlance) or other so-called "enhanced services" that are not telecommunications transmission but are often billed on consumers' telephone bills. Modem dialers and videotext schemes, like the operation attacked in *FTC v. Verity International,* No.00 Civ. 7422(LAK) (S.D.N.Y. 2000), described infra, are ones that, unbeknownst to a consumer, cause his or her computer modem to disconnect from his or her usual Internet service provider, dial an expensive international telephone number, and reconnect to the Internet at a remote location overseas, charging the consumer as much as $5.00 or more per minute for as long as the consumer remains online.

gets for the law enforcement actions that comprised Operation Top Ten Dot Con. Finally, Consumer Sentinel data enabled the Commission and its partners to obtain and develop evidence against these targets from individual consumers whose complaints had been included in the database.

Consumer Sentinel first went online in late 1997. Since then, the Commission has upgraded the capacity of the Consumer Sentinel database and enhanced the agency's complaint-handling systems by creating and staffing a new toll-free consumer helpline at 1-877-FTC-HELP, and adding several new functions to Consumer Sentinel. The first of these new functions, the "Top Violators" report function, allows a law enforcement officer to pull up the most common suspects and schemes by state, region or subject area. The second new function, "Auto Query," enables an investigator to create an automatic search request. This automatic search can be set to run daily, weekly, or monthly, and if new complaints come into Consumer Sentinel that match the search criteria, Consumer Sentinel will automatically alert the investigator via email. Third, the "Alert" function enables law enforcers to communicate with each other and minimize duplication of their efforts, and a fourth new function performs a search of Commission court orders online. In 2000, Consumer Sentinel received over 100,000 consumer complaints. Currently the database holds over 300,000 consumer complaints.[20]

Consumer Sentinel has particular relevance to identity theft, because the Commission has expanded Consumer Sentinel to encompass the Identity Theft Data Clearinghouse. Victims of identity theft can call the FTC's toll-free telephone number, 1-877-ID THEFT (438-4338), to report the crime and receive advice on what to do. CRC counselors enter the victims' information about their experience into the Identity Theft Data Clearinghouse, which immediately makes the information available, through the Consumer Sentinel web site, to174 participating domestic law enforcement agencies. The Clearinghouse data is used to spot patterns of illegal activity. For example, the Clearinghouse database may facilitate identification of organized or large-scale identity theft rings. The Clearinghouse is a tool that has begun to enable the many agencies involved in combating identity theft to share data, and to work more effectively to track down identity thieves and assist consumers.[21] In this regard, starting this month, the U.S. Secret Service has detailed an agent to the Commission's Identity Theft Clearinghouse program to help develop and refer case leads from the Clearinghouse to law enforcers throughout the nation to facilitate investigation and prosecution of identity theft.

The Commission's efforts to improve consumer complaint collection and analysis through the Consumer Response Center and Consumer Sentinel are complemented by a proactive program to uncover fraud and deception in broad sectors of the online marketplace through "Surf Days." Surf Days use new technology to detect and analyze emerging Internet problems. While Consumer Sentinel provides data on broad trends and the volume of complaints prompted by particular Internet schemes, Surf Days allow the Commission to take a "snap shot" of a market segment at any given time. The Commission also uses Surf Days to reach new entrepreneurs and alert those who unwittingly may be violating the law.

On a typical Surf Day, Commission staff and personnel from our law enforcement partners—often state attorneys general, sister federal agencies or private organizations like the Better Business Bureau—widely "surf" the Internet for a specific type of claim or solicitation that is likely to violate the law. When a suspect site is identified, the page is downloaded and saved as potential evidence, and the operator of the site is sent an email warning that explains the law and provides a link to educational information available at www.ftc.gov. Shortly thereafter, a law enforcement team revisits the previously warned sites to determine whether they have remedied their questionable claims or solicitations. The results vary, depending on the targeted practice of the particular Surf Day. Between 20 and 70 percent of the Web site operators who received a warning come into compliance with the law, either by

---

[20] The FTC recently signed an agreement with the Department of Defense to collect consumer complaints from men and women serving in the military through a project called "Soldier Sentinel."

[21] The Commission has been working closely with other agencies to establish a coordinated effort to identify the factors that lead to identity theft, to minimize those opportunities, to enhance law enforcement efforts and help consumers resolve identity theft problems. The first such event was the Commission's April 1999 meeting with representatives of approximately a dozen federal agencies as well as the National Association of Attorneys General to discuss the implementation of the consumer assistance provisions of the Identity Theft Act. FTC staff works with the Identity Theft Subcommittee of the Attorney General's Council on White Collar Crime to coordinate law enforcement strategies and initiatives. FTC staff also coordinates with staff from the Social Security Administration's Inspector General's Office on the handling of social security number misuse complaints, a leading source of identity theft problems.

taking down their sites or modifying their claims or solicitations. Sites that continue to make unlawful claims are targeted for possible law enforcement action.

To date, the Commission has conducted 27 different Surf Days targeting problems ranging from "cure-all" health claims to fraudulent business opportunities and credit repair scams.[22] More than 250 law enforcement agencies or consumer organizations around the world have joined the Commission in these activities; collectively, they have identified over 6,000 Internet sites making dubious claims. The law enforcement Surf Day has proven so effective that it is now widely used by other government agencies, consumer groups and other private organizations.

B. Traditional Scams Use the Internet to Expand in Size and Scope.

Out of the 170 cases brought by the Commission against Internet fraud and deception, over half have targeted old-fashioned scams that have been retooled for the new medium. For example, the Commission has brought 28 actions against online credit repair schemes, 25 cases against deceptive business opportunities and work-at-home schemes, and 11 cases against pyramid schemes.

It is no surprise that the Internet versions of traditional frauds can be much larger in size and scope than their offline predecessors. A colorful, well-designed Web site imparts a sleek new veneer to an otherwise stale fraud; and the reach of the Internet allows an old-time con artist to think—and act—globally, as well.

Pyramid schemes are the most notable example of a fraud whose size and scope are magnified by the Internet.[23] By definition, these schemes require a steady supply of new recruits. The Internet provides an efficient way to reach countless new prospects around the world, and to funnel funds more efficiently and quickly from the victims to the scammers at the top of the pyramid. As a result, the victims are more numerous, the fraud operator's financial "take" is much greater, and the defense is typically well-funded and fierce when the FTC brings suit to stop a pyramid scheme operating online.

Despite the extensive resources required to pursue an online pyramid case, the Commission has asserted a strong enforcement presence, obtaining orders for more than $70 million in redress for victims,[24] and pursuing millions more in ongoing litigation. In one case, FTC v. Fortuna Alliance, the Commission spent two years in litigation and negotiations and finally obtained a court order finding the defendants in contempt, and a stipulated final order enjoining the defendants from further pyramid activities and requiring them to pay $5.5 million in refunds to over 15,000 victims in the U.S. and 70 foreign countries.[25] More recently, in FTC v. Five Star Auto Club, Inc.,[26] the Commission prevailed at trial against another pyramid scheme that

---

[22] The FTC has coordinated or co-sponsored the following Surf Days, listed by date of their announcements: Pyramid Surf Day (Dec. 1996), Credit Repair Surf (April 1997), Business Opportunity Surf Day (April 1997), Coupon Fraud Surf Day (Aug. 1997), North American Health Claims Surf (Oct. 1997), HUD Tracer Surf Day (Nov. 1997), International Surf Day (Oct. 1997), Kids Privacy Surf Day (Dec. 1997), Junk E-mail Harvest (Dec. 1997), Privacy Surf (March 1998), Textile and Wool Labeling Surf (Aug. 1998), Y2K Surf (Sept. 1998), International Health Claims Surf (Nov. 1998), Investment Surf Day (Dec. 1998), Jewelry Guides Surf (Jan. 1999), Pyramid Surf Day II (March 1999), Green Guide Surf (April 1999), Coupon Fraud II Surf Day (June 1999), Jewelry Guides Surf II (January 2000), Scholarship Services Surf (January 2000), GetRichQuick.con Surf (March 2000), False or Unsubstantiated Lice Treatment Claims Surf (April 2000), Credit Repair Surf II (Aug. 2000), Childrens' Online Privacy Protection Act Compliance Surf (Aug. 2000), False Claims of Authenticity for American Indian Arts and Crafts Surf Day (Oct. 2000), TooLate.Com [Surf of Online Retailers' Compliance with the Mail or Telephone Order Merchandise Rule] (Nov. 2000), and Operation Detect Pretext [Surf of more than 1,000 web sites (coupled with a review of more than 500 advertisements in the print media) for firms offering to conduct financial searches, in order to identify potential violators of the Gramm-Leach-Bliley Act, which specifically prohibits obtaining, or attempting to obtain, another person's financial information by making false, fictitious or fraudulent statements to financial institutions].

[23] Pyramid operators typically promise enormous earnings or investment returns, not based on commissions for retail sales to consumers, but based on commissions for recruiting new pyramid members. Recruitment commissions, of course, are premised on an endless supply of new members. Inevitably, when no more new recruits can be found, these schemes collapse and a vast majority of participants lose the money they invested.

[24] To date, the Commission has collected about $42.6 million in these cases.

[25] *FTC v. Fortuna Alliance, L.L.C.,,* No. C96-799M (W.D. Wash. 1996). *See also, FTC v. JewelWay International, Inc.,* No. CV97-383 TUC JMR (D. Ariz. 1997) ($5 million in redress for approximately 150,000 investors); *FTC v. Nia Cano,* No. 97-7947-CAS-(AJWx) (C.D. Cal. 1997) (approximately $2 million in redress); *FTC v. FutureNet,* No. 98-1113GHK (AIJx) (C.D. Cal. 1998) ($1 million in consumer redress). *FTC v. Five Star Auto Club, Inc.,* 97 F. Supp. 2d 502 (S.D.N.Y. 2000). ($2.9 million in consumer redress); *FTC v. Equinox International Corp.,* No CV-S-990969-JBR-RLH (D.Nev. 1999) (pyramid promoted through many devices, including some use of the Internet; $50 million in consumer redress).

[26] *FTC v. Five Star Auto Club, Inc.,* 97 F. Supp. 2d 502 (S.D.N.Y. 2000).

lured online consumers to buy in by claiming that an annual fee and $100 monthly payments would give investors the opportunity to lease their "dream vehicle" for "free" while earning up to $80,000 a month by recruiting others to join the scheme. The court issued a permanent injunction shutting down the scheme, barring for life the scheme's principals from any multi-level marketing business, and ordering them to pay $2.9 million in consumer redress.

C. Scams Are Increasingly High-Tech.

Although most Internet fraud stems from traditional scams, the number of schemes uniquely and ingeniously exploiting new technology is multiplying. These are the most insidious schemes because they feed on the public's fascination with—and suspicion of—new technology. Their ultimate effect can only be to undermine consumer confidence in the online marketplace. To combat this type of high-tech fraud, the Commission has supported staff training and given its staff the tools to be effective cyber-sleuths.

Recognizing that most of its attorneys and investigators need to be Internet savvy, the Commission has hosted beginner and advanced Internet training seminars and held sessions on new technology, investigative techniques, and Internet case law. The Commission also makes this training available to personnel of other law enforcement agencies. In the past year, the Commission has presented Internet training seminars in seven U.S. cities and in Toronto, Canada, and Paris, France. In addition to FTC staff, these sessions trained approximately 800 individual participants from other law enforcement agencies. These participants represented twenty different countries including the U.S., twenty-six states, twenty-two federal agencies, and fourteen Canadian law enforcement agencies. Among those who have participated are representatives from the offices of state Attorneys General, the Department of Justice and U.S. Attorneys, the Securities and Exchange Commission, the FBI, and the Postal Inspection Service.

In addition to providing regular Internet training, the Commission also provides its staff with the tools they need to investigate high-tech fraud. The FTC's Internet Lab is an important example. With high speed computers that are separate from the agency's network and equipped with current hardware and software, the Lab allows staff to investigate fraud and deception in a secure environment and to preserve evidence for litigation.

1. Modem Hijacking—The Commission has used its training and tools to stop some of the most egregious and technically sophisticated schemes seen on the Internet. For example, the FTC's lawsuit against Verity International, Ltd.,[27] was prompted by the influx of hundreds of complaints in the last week of September 2000 through the CRC and logged in Consumer Sentinel. Investigation showed that high charges on consumers' phone lines were being initiated by "dialer" software downloaded from teaser adult web sites. Many line subscribers had no idea why they received bills for these charges. Others discovered that a minor in their household—or another person who did not have the line subscriber's authorization—accessed the Web sites and downloaded the dialer software. The dialer program allowed users to access the "videotext" adult content without any means of verifying that the user was the line subscriber, or was authorized by the line subscriber to incur charges on the line for such service. Once downloaded and executed, however, the program actually hijacked the consumer's computer modem by surreptitiously disconnecting the modem from the consumer's local Internet Service Provider, dialing a high-priced international long distance call to Madagascar, and reconnecting the consumer's modem to the Internet from some overseas location, opening at an adult web site. The line subscriber—the consumer responsible for paying phone charges on the line—then began incurring charges on his or her phone lines for the remote connection to the Internet at the rate of $3.99 per minute. The court has ordered a preliminary injunction in this matter, and litigation continues.[28]

2. "Pagejacking" and "Mousetrapping"—Earlier, in *FTC v. Carlos Pereira d/b/a atariz.com*,[29] the Commission attacked a world- wide, high-tech scheme that allegedly "pagejacked" consumers and then "mousetrapped" them at adult pornography sites. "Pagejacking" is making exact copies of someone else's Web page, including the imbedded text that informs search engines about the subject matter of the site. The defendants allegedly made unauthorized copies of 25 million pages from other

[27] *FTC v. Verity International, Ltd.,* No. 00 Civ. 7422 (LAK)(S.D.N.Y. 2000).

[28] Other modem hijacking cases include *FTC v. Audiotex Connection, Inc.,* No. CV-97-0726 (DRH) (E.D.N.Y. 1997) (final stipulated injunction halting the unlawful practice and ordering that 27,000 victims receive full redress totaling $2.14 million); *FTC v. RJB Telcom, Inc.,* No.CV 00-2017 PHX SRB (D. Az. 2000); *FTC v. Ty Anderson,* No. C 00-1843P (W.D. Wa. 2000).

[29] *FTC v. Carlos Pereira d/b/a atariz.com,* No. 99-1367-A (E.D. Va. 1999).

Web sites, including those of Paine Webber and the Harvard Law Review. The defendants made one change on each copied page that was hidden from view: they inserted a command to "redirect" any surfer coming to the site to another Web site that contained sexually-explicit, adult-oriented material. Internet surfers searching for subjects as innocuous as "Oklahoma tornadoes" or "child car seats" would type those terms into a search engine and the search results would list a variety of related sites, including the bogus, copycat site of the defendants. Surfers assumed from the listings that the defendants' sites contained the information they were seeking and clicked on the listing. The "redirect" command imbedded in the copycat site immediately rerouted the consumer to an adult site hosted by the defendants. Once there, defendants "mousetrapped" consumers by incapacitating their Internet browser's "back" and "close" buttons, so that while they were trying to exit the defendants' site, they were sent to additional adult sites in an unavoidable, seemingly endless loop.

Using the new tools available in the Internet Lab, the Commission was able to capture and evaluate evidence of this "pagejacking" and "mousetrapping." In September 1999, the Commission filed suit in federal court and obtained a preliminary order stopping these activities and suspending the Internet domain names of the defendants. Since then, the Court has entered default judgments against two defendants and a stipulated permanent injunction against a third, baring them from future law violations. A fourth defendant, Carlos Pereira, has evaded law enforcement authorities in Portugal.

3. Internet-based Facilitation of ID Theft—The Commission has brought one law enforcement action that directly confronted identity theft, *FTC v. Jeremy Martinez d/b/a Info World.*[30] Jeremy Martinez allegedly facilitated identity theft by offering over the Internet fake ID templates for which there was absolutely no legitimate use. The FTC complaint alleged that Jeremy Martinez, doing business as Info World, maintained Web sites, including one located at a site called "newid" that sold 45 days of access to fake ID templates for $29.99. The site contained "high quality" templates to use in creating fake drivers licenses from ten states.[31] It also offered a birth certificate template, programs to generate bar codes—required in some states to authenticate drivers licenses—and a program to falsify Social Security numbers.

The complaint alleged that Martinez was deliberately marketing his site to consumers who were surfing the net to find fake ID documents. Web sites use Meta-tags—hidden words that help search engines identify and index Web site content. Martinez's Meta-tags included "illegal id," "fake id fraud," and "forging documents" according to the FTC complaint.

The Commission charged that selling the fake ID templates violated Section 5 of the FTC Act and that by providing false identification templates to others, Martinez provided the "means and instrumentalities" for others to break the law—a separate violation of Section 5. Immediately upon the Commission's filing of the complaint, the Court issued a Temporary Restraining Order (TRO) halting the alleged illegal activity, and soon thereafter a stipulated preliminary injunction continuing the relief granted in the TRO. On May 17, 2001 the Court approved Martinez' stipulated settlement with the FTC that permanently bans him from selling false identification documents or identification templates, or assisting others in doing so. The settlement also permanently bars Martinez from providing others with the means and instrumentalities with which to make any false or misleading representations that conceal or alter a person's identity, or that falsely signify that a fake document is real. The stipulation also requires Martinez to disgorge illegal earnings from the scheme in the amount of $20,000. The settlement provides an "avalanche" clause making Martinez liable for more than $105,000 in the event that he misrepresented his financial condition to the Commission.

4. Pretexting by Internet-based Information Brokers.—Last month, the Commission filed lawsuits against three Internet-based information brokers who used false pretenses, fraudulent statements or impersonation to obtain consumers' confidential fi-

---

[30] *FTC v. Jeremy Martinez d/b/a Info World,* No. 00 Civ 12701 (C.D. Cal. Dec. 5, 2000). *See, also, FTC v. J.K. Publications, Inc., et al,* 99 F. Supp.2d. 1176 (C.D. Cal. Apr. 10, 2000)(granting summary judgment for the FTC in case alleging that defendants obtained consumers' credit card numbers without their knowledge and billed consumers' accounts for unordered or fictitious Internet services), later proceedings at *FTC v. J.K. Publications, Inc., et al,* 99 Civ 00044 (C.D. Cal. Aug. 30, 2000)(final order awarding $37.5 million in redress); *FTC v. Rapp,* No. 99-WM-783 (D. Colo. filed Apr. 21, 1999) (alleging that defendants obtained private financial information under false pretenses)(Stipulated Consent Agreement and Final Order entered June 23, 2000).

[31] Info World offered templates for California, Georgia, Florida, Maine, Nevada, New Hampshire, New Jersey, Utah, Wisconsin and New York drivers licenses.

nancial information.[32] The practice " known as 'pretexting'" is illegal under the Gramm-Leach-Bliley Act.[33] The three complaints, filed in federal courts in Maryland, New York and Texas, alleged that defendants represented on their Web sites that they could obtain customer financial information and used pretexting to obtain bank account balances.

The Commission staff first identified the defendants as possible pretexters when it conducted a "surf" of information broker Web sites. As part of "Operation Detect Pretext," the staff screened more than 1,000 Web sites and reviewed more than 500 print media advertisements to identify approximately 200 firms that offered to obtain and sell asset or bank account information to third parties. The Commission staff sent notices to most of these firms advising them that their practices must comply with the anti-pretexting provisions of the Gramm-Leach-Bliley Act. At the same time, the staff set up a sting operation to confirm that the three defendants were actually providing the illegal pretexting services they advertised on their Web sites. Based primarily upon evidence uncovered by the sting, the FTC filed complaints alleging that the defendants—for fees ranging from $100 to $600—would obtain bank account balances by calling a bank and pretending to be the customer.

The courts in all three cases immediately entered TROs to halt the illegal activity, freeze certain of the defendants' assets, and require the defendants to produce their financial and business records to the Commission. Shortly thereafter, all three defendants stipulated to preliminary injunctions continuing the relief granted in the TROs. The Commission's goal is an order permanently barring defendants' illegal pretexting practices and disgorging the money defendants earned from them.

E. Online Scams Spread Quickly and Disappear Quickly.

One hallmark of Internet fraud is the ability of perpetrators to cover their tracks and mask their locations and identities. Using anonymous emails, short-lived Web sites, and falsified domain name registrations, many fraud operators are able to strike quickly, victimize thousands of consumers in a short period of time, and disappear nearly without a trace.

To stop these swift and elusive con artists, law enforcement must move just as fast. The FTC's Internet Rapid Response Team was created for this very purpose. It draws heavily upon complaints collected by the FTC's Consumer Response Center and the Consumer Sentinel system. The team constantly reviews complaint data to spot emerging problems, conduct quick but thorough investigations, and prepare cases for filing in federal courts. Based on such data review, FTC staff had completed its investigation and was in court successfully arguing for an *ex parte* temporary restraining order and asset freeze in *FTC v. Verity International, Ltd.* within a little more than a week after the first complaints began coming in to the Consumer Response Center.

In another exemplary effort, *FTC v. Benoit,*[34] the Rapid Response Team quickly moved against defendants who allegedly used deceptive emails or "spam" to dupe consumers into placing expensive international audiotext calls.[35] The defendants allegedly sent thousands of consumers an email stating that each recipient's "order" had been received and that his or her credit card would be billed $250 to $899. The email instructed consumers to call a telephone number in the 767 area code if they had any questions. Most consumers did not realize that 767 was the area code for Dominica, West Indies. When consumers called the number expecting to reach a customer representative, they were connected to an audiotext entertainment service with sexual content and charged expensive international rates.

Even though a string of telephone carriers could not identify who operated the audiotext number in question, the Internet Rapid Response Team constructed a compelling case in about three weeks. The Commission quickly obtained a federal

---

[32] *FTC v. Information Search, Inc. and David Kacala,* Civil Action No. AMD-01-1121 (D. Md. April 17, 2001); *FTC. v. Victor L. Guzzetta d/b/a Smart Data Systems,* Civil Action No. CV 01 2335 (E.D.N.Y. April 17, 2001); *FTC v. Paula L. Garrett d/b/a Discreet Data Systems,* Civil Action No. H 01- 1225 (S.D. Tex. April 17, 2001). The Commission determined to file the complaints by a vote of 3-2, with Chairman Pitofsky, Commissioner Anthony, and Commissioner Thompson voting in the affirmative and Commissioner Swindle and Commissioner Leary voting in the negative.

[33] Subtitle B of the Gramm-Leach-Bliley Act provides for both civil and criminal penalties for pretexting or for soliciting others to pretext. 15 U.S.C. §§ 6821. et seq. The Commission only has civil enforcement authority. Subtitle B also directs the Commission to report annually to Congress on the disposition of all enforcement actions. The Commission issued its first annual report on January 12, 2001, before the three complaints were filed.

[34] *FTC v. Benoit (previously FTC v. One or More Unknown Parties),* No. 3:99 CV 181 (W.D.N.C. 1999). In the course of the litigation, Commission attorneys were able to identify the operators of the scheme.

[35] "Audiotext" services are telephone-based entertainment or information services.

court order to stop the scheme and freeze any proceeds of the fraud still in the telephone billing system.

F. Effective Remedies Are More Difficult to Achieve in the Global Online Market.

The globalization of the marketplace poses new and difficult challenges for consumer protection law enforcement. Anticipating this development, the Commission held public hearings in the fall of 1995 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, and the Commission published a two-volume report summarizing the testimony and the role of antitrust and consumer protection law in the changing marketplace. As reported in, "Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace," there was a broad consensus that 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.[36] These principles have guided FTC policy regarding the Internet ever since.

In addition to gathering information through hearings and workshops, the FTC has gained practical knowledge about the effects of globalization and ecommerce through its litigation. In this respect, the Commission has found that pursuing Internet fraud often involves a difficult and costly search for money that has been moved off-shore. For example, in *FTC v. J.K. Publications,*[37] the defendants, who had made unauthorized charges of $19.95 per month on consumers' credit or debit cards for purported Internet services, moved much of their ill-gotten gains off-shore. The Commission ultimately won a $37.5 million verdict in this matter, but in the course of litigation, the receiver appointed in this case reported that the defendants had moved millions of dollars to the Cayman Islands, Liechtenstein, and Vanuatu in the South Pacific. However, to date, despite substantial litigation costs, the monies have not been fully repatriated.[38]

In addition to fraud proceeds moving off-shore quickly, fraudulent online operators may be beyond the reach of the Commission and U.S. courts, practically if not legally. There is now limited recognition of civil judgments from country to country. Even if the Commission were to bring an action and obtain a judgment against a foreign firm that has defrauded U.S. consumers, the judgment might be challenged in the firm's home country, and the ability to collect any consumer redress might be frustrated. In light of this possibility, U.S. law enforcement must look for more effective cross-border legal remedies, and must work more cooperatively with law enforcement and consumer protection officials in other countries.

To meet this challenge, the Commission is increasingly cooperating with international counterparts in a number of venues. One is the International Marketing Supervision Network (IMSN), a group of consumer protection agencies from the 30 countries that are members of the Organization for Economic Cooperation and Development (OECD). The FTC has also executed cooperation memoranda with agencies in Canada, the United Kingdom, and Australia.

The FTC has also taken a stride forward in cross-border cooperation with a project called econsumer.gov. The FTC, agencies from twelve other countries, and the OECD unveiled this new international joint effort to gather and share cross-border e-commerce complaints at last month's IMSN meeting in New York. The project has two parts: a public Web site at www.econsumer.gov, and a restricted access law enforcement site. The public site provides—in English, French, German, and Spanish—an online consumer complaint form and various other consumer protection information. The law enforcement site, using the FTC's existing Consumer Sentinel network, will provide the econsumer.gov complaints and other investigative information to participating enforcers.

---

[36] *See* Bureau of Consumer Protection, Federal Trade Commission, *Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace,* iii (May 1996); *See also, Looking Ahead: Consumer Protection in the Global Electronic Marketplace* (September 2000).

[37] *FTC v. J.K. Publications,* No. 99-000-44ABC (AJWx)(C.D. Cal. 1999).

[38] Similarly, in *FTC v. Fortuna Alliance,* the Commission found that the defendants had transferred $2.8 million to Antigua, West Indies. With the assistance of the U.S. Department of Justice's Office of Foreign Litigation, the Commission obtained an order from an Antiguan court freezing those funds and a stipulated final judgment in U.S. court that required the defendants to repatriate that money for consumer redress. In the process, however, it cost $280,000 in fees alone to litigate the case in foreign court. In this case, the Department of Justice's Office of Foreign Litigation paid $50,000 up front, and the U.S. court ordered the defendants to pay the remaining $230,000 in fees. In other cases, the Commission may have to bear all or most of the cost of litigating in foreign court.

The Commission's actions in *FTC v. Pereira* represent significant strides in the right direction. In that case, the Commission realized that the defendants' "pagejacking" and "mousetrapping" scheme had operated through Web sites registered with a U.S.-based company. Thus, in its request for a temporary restraining order and preliminary injunction, the Commission asked that the registrations for these Web sites be suspended, thereby effectively removing the defendants and their deceptive Web sites from the Internet, pending a full trial. At the same time, the Commission reached out to its international colleagues in Portugal and Australia. The Australian Competition and Consumer Commission (ACCC) proved especially helpful in providing information about the defendants and their business operations in Australia. The ACCC also began its own investigation, executed a number of search warrants, and began pursuing potential legal action against the defendants in that country.

III. CONSUMER AND BUSINESS EDUCATION

Law enforcement alone cannot stop the tide of fraudulent activity on the Internet. Meaningful consumer protection depends on education as well. Consumers must be given the tools they need to spot potentially fraudulent promotions, and businesses must be advised about how to comply with the law. The FTC's consumer and business education program uses the Internet to communicate anti-fraud and educational messages to reach vast numbers of people in creative and novel ways quickly, simply and at low cost. As more consumers and businesses come online, use of the Internet to disseminate information will grow.

A. Fraud Prevention Information for Consumers

More than 200 of the consumer and business publications produced by the FTC's Bureau of Consumer Protection are available on the agency's Website in both text and .pdf format. Indeed, the growth in the number of our publications viewed online between 1996 and 1999 (140,000 vs. 2.5 million) tells the story of the Internet's coming of age as a mainstream medium and highlights its importance to any large-scale dissemination effort. Those 2.5 million page views are in addition to the 6 million print publications the FTC distributes each year to organizations that disseminate them on the FTC's behalf.[39]

B. Link Program

In addition to placing publications on its own Web site, the FTC actively encourages partners " government agencies, associations, organizations, and corporations with an interest in a particular subject " to link to its information from their sites and to place banner public service announcements provided by the FTC on their sites. Links from the banners allow visitors to click through to the FTC site quickly to get the information they're looking for exactly when they want it. Examples of the varied organizations that have helped drive traffic to the valuable consumer information on www.ftc.gov are Yahoo!, American Express, Circuit City, AARP, North American Securities Administrators Association, the Alliance for Investor Education, the Better Business Bureau, CBS, motleyfool.com, the U.S. Patent and Trademark Office, Shape Up America!, the National Institutes of Health, and the Arthritis Foundation.

---

[39] With respect to identify theft, the Commission also conducts an extensive multi-media education campaign including print materials, media mailings and interviews and a website, located at www.consumer.gov/idtheft. The FTC's consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name,* covers a wide range of topics, including how identity theft occurs, how one can protect one's personal information and minimize their risk, what steps to take immediately upon finding out one is a victim, and how to correct credit-related and other problems that may result from identity theft. It also describes federal and state resources that are available to consumers who have particular problems as a result of identity theft. The FTC has distributed directly more than 230,000 copies of the booklet through April 2001. Another 425,000 copies have been printed and are being distributed by the Social Security Administration. The identity theft website includes the booklet, descriptions of common identity theft scams, and links to testimony, reports, press releases, identity theft-related state laws, and other resources. The site also has a link to a web-based complaint form, allowing consumers to send complaints directly to the Identity Theft Data Clearinghouse. The website had received almost 350,000 hits by the end of April 2001 and more than 7,300 complaints had been submitted electronically.

As part of "Operation Detect Pretext," in January the Commission published a Consumer Alert entitled "Pretexting: Your Personal Information Revealed" that offers practical tips on how consumers can protect their pers

C. "Teaser" Pages

Too often, warning information about frauds reaches consumers *after* they've been scammed. For the FTC, the challenge is reaching consumers *before* they fall victim to a fraudulent scheme. Knowing that many consumers use the Internet to shop for information, agency staff have developed teaser sites that mimic the characteristics that make a site fraudulent and then warn the reader about the fraud. Metatags embedded in the FTC teaser sites make them instantly accessible to consumers who are using major search engines and indexing services as they look for products, services and business opportunities online. The teaser pages link back to the FTC's page, where consumers can find practical, plain English information. The agency has developed more than a dozen such teaser sites on topics ranging from fraudulent business opportunities and wealth-building scams to weight loss products, vacation deals and investments.[40] Feedback from the public has been overwhelmingly positive: visitors express appreciation—not only for the information, but for the novel, hassle-free and anonymous way it is offered.

D. Consumer.gov.

Following its vision of the Internet as a powerful tool for consumer education and empowerment, the FTC organized a group of five small federal agencies in 1997 to develop and launch a Web site that would offer one-stop access to the incredible array of federal consumer information. On the theory that consumers may not know one federal agency from another, the information is arranged by topic area. Federal agencies have responded well to consumer.gov. The site now includes contributions from 170 federal agencies. Consumers also find it useful, with over 182,500 visits to the site recorded in the first half of FY 2001.

Visitors to consumer.gov find special initiatives, too: The President's Council on Y2K Conversion asked the FTC to establish a Y2K consumer information site; the Quality Interagency Coordination Task Force requested a special site on health care quality; and the U.S. Postal Inspection Service asked that consumer.gov house the site to support the **kNOw Fraud** initiative, an ongoing public-private campaign initiated with the sending of postcards about telemarketing fraud to 115 million American households in the fall of 1999.[41] The FTC continues to maintain the site.

E. Business Education for Online Marketers

As part of its mission, the FTC provides guidance to online marketers on how to assure that basic consumer protection principles apply online. Many of these entrepreneurs are small, start-up companies that are new to the Internet and to marketing in general and are unfamiliar with consumer protection laws. The Commission's publication, *Advertising and Marketing on the Internet: Rules of the Road,* is designed to give practical, plain-English guidance to them.[42] FTC also has used a variety of other approaches to get its messages out to the business community, from posting compliance guides, staff advisory letters and banner public service announcements on the Web to speaking at industry and academic meetings and conferences, using the trade press to promote the availability of information on the agency site, and holding workshops on online issues and posting the transcripts. Most recently, on January 30 of this year, the Commission, in cooperation with the Electronic Retailing Association, presented "Etail Details," a case-driven Internet marketing seminar for Internet retailers, marketers, and suppliers on applying offline rules and regulations online. The seminar was designed to ensure etailers understand and comply with FTC rules regarding etailing.

---

[40] The titles of the teaser sites are: Looking for Financial Freedom?; The Ultimate Prosperity Page; Nordicalite Weight Loss Product; A+ Fast Ca$h for College; EZTravel: Be an Independent agent; EZTravel: Certificate of Notification; EZToyz Investment Opportunity; HUD Tracer Association; CreditMenders Credit Repair; NetOpportunities: Internet is a Gold Mine; National Business Trainers Seminars; VirilityPlus: Natural Alternative to Viagra; ArthritiCure: Be Pain-Free Forever.

[41] The original consumer.gov team received the Hammer Award, presented by the Vice President to teams of federal employees who have made significant contributions to reinventing government. than 1,000 Internet fraud complaints; a year later, the number had increased eightfold. In 2000, over 25,000 complaints—roughly 26 percent of all fraud complaints logged into the FTC's complaint database, "Consumer Sentinel," by various organizations that year—related to online fraud and deception. The need—and challenge—is to act quickly to stem this trend while the online marketplace is still young.

[42] There has been an astonishing growth in page views of this publication in the past year: from 33,448 views in FY 1999 to 110,473 in FY 2000 .

IV. CONCLUSION

The Commission has been involved in policing the electronic marketplace for more than six years " before the World Wide Web was widely used by consumers and businesses. The Commission has strived to keep pace with the unprecedented growth of the electronic marketplace by targeting our efforts, making innovative use of the technology, and leveraging our resources to combat fraud on the Internet. In addition, the Commission has taken the necessary steps to fulfill its responsibilities under both the Identity Theft Assumption and Deterrence Act of 1998 and, with respect to pretexting, the Gramm-Leach-Bliley Act to promote protection of consumers' personal financial information by financial institutions. We have done this within the framework of limited resources, and without retreating from our important consumer protection work in traditional markets.

The Commission greatly appreciates the opportunity to describe its efforts to combat fraud on the Internet, and its activities against identity theft and pretexting.

Mr. STEARNS. I thank the gentlelady.

Mr. STEARNS. Mr. Swartz.

STATEMENT OF BRUCE SWARTZ

Mr. SWARTZ. Thank you, Mr. Chairman. Mr. Chairman, members of the subcommittee, the Department of Justice thanks you for inviting the Department of Justice to testify this morning about the important issue of Internet fraud and the closely related issue of identity theft. With the subcommittee's permission I will submit my full statement for the record and simply summarize it this morning.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. SWARTZ. As the subcommittee members have noted, and as the prior witnesses have stated, Internet fraud is one of the most pervasive and one of the fastest growing types of fraud we face.

I'd like to turn first this morning to the Department's strategy for dealing with Internet fraud. That strategy has three significant components. The first of those components is interagency and international coordination. Mr. Kubic this morning has already mentioned one of the fruits of that cooperation and coordination, "Operation Cyber Loss", a significant take down of Internet fraudsters.

My written statement also details a number of other recent significant prosecutions that have been undertaken by Federal law enforcement with regard to Internet fraud.

Beyond Cyber Loss, the Department of Justice also fosters coordination through its chairing of the interagency Telemarketing and Internet Fraud Working Group. All of the law enforcement agencies at the table this morning, as well as the Postal Inspection Service, the FTC, the SEC and other law enforcement agencies, are represented on this working group. The working group meets quarterly and is able to examine and work toward responding to developing trends in Internet fraud.

Internationally as well, the Department of Justice is in the lead in attempting to coordinate responses to Internet fraud, particularly through the Lyon Group of the G-8, a senior experts group on transnational organized crime. The Department has worked to ensure that we have a global response to what is clearly a global problem.

The second component of the Department's response to Internet fraud is intelligence and analysis. We've heard this morning already from other witnesses about the importance of the Internet Fraud Complaint Center, which the Department of Justice has

strongly supported. That Center has allowed for centralization of complaints and for packaging of investigative materials to be sent out to prosecutors. The FTC's Consumer Sentinel program has also been an important development in the intelligence and analysis field.

Legal analysis is also an important part of this, and in that regard, the Department of Justice has developed a brief bank of legal materials and pleadings which it has been able to provide to Federal prosecutors throughout the United States. Similarly, we've worked on developing an Intranet on the Internet, a means of speeding communication among and between Federal prosecutors engaged in Internet fraud prosecutions.

The third component of our strategy is training and outreach. The Department of Justice, through the Fraud Section and through its Computer Crime Section, has taken the lead in providing specialized training on Internet fraud at the National Advocacy Center. That training has been provided to Federal, State and local prosecutors and law enforcement agencies. Significantly, it also has been provided to international prosecutors and law enforcement agency members—again, recognizing the global dimensions of this project.

Our outreach programs also extend beyond law enforcement agencies. We're looking to develop ways to increase public education and knowledge about Internet fraud, with appropriate collaboration between the public and private sector. These measures include public websites produced by the Department and other law enforcement agencies and regulatory agencies. These act as electronic fora for discussing detailed ways to prevent becoming a victim and also how to respond if one does become a victim.

With the subcommittee's permission, I would like now to turn briefly to the related issue of identity theft. Identity theft of course can be perpetrated on the Internet, and is frequently perpetrated on the Internet, but can be perpetrated in other ways as well. Here, also the Department of Justice has followed a policy and a strategy of coordination, intelligence analysis and training and outreach.

A major vehicle for implementation of this strategy has been the Attorney General's White Collar Crime Council and in particular, its Identity Theft Subcommittee. That subcommittee includes all of the major Federal law enforcement agencies. It has provided guidance memoranda and other materials about identity theft and distributed them not only to Federal, but also to State and local, prosecutors and investigative agencies. It has also worked with the FTC and other agencies to provide educational materials.

In addition, in the field, the Department has supported the creation and establishment of identity theft task forces. I'm pleased to report that this coordination has resulted in an increasing number of prosecutions under the new identity theft statute, with over 92 prosecutions reported by the United States Attorneys' offices over the past 2 years.

Thank you, Mr. Chairman. I would welcome any questions the subcommittee might have.

[The prepared statement of Bruce Swartz follows:]

PREPARED STATEMENT OF BRUCE SWARTZ, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, UNITED STATES DEPARTMENT OF JUSTICE

Good morning, Mr. Chairman and Members of the Subcommittee. I am pleased to appear before you this morning to testify about the problem of Internet fraud and the closely related problem of identity theft, and what the Department of Justice is doing to combat them. I will first discuss Internet fraud and then identity theft.

As a preliminary matter, Mr. Chairman, today the Department of Justice and the FBI are announcing a major enforcement operation targeting Internet fraud, one of the fastest-growing and most pervasive forms of white-collar crime. The threat of Internet fraud calls for forceful action, and today, the Department and the FBI, in partnership with the U.S. Postal Inspection Service, the Internal Revenue Service-Criminal Investigative Division, the U.S. Customs Service, and numerous state and local law enforcement agencies, are responding with a national "sweep" of coordinated enforcement actions against approximately 90 subjects. In a few moments, Mr. Thomas Kubic, Deputy Assistant Director in the FBI's Criminal Investigative Division, will provide details of the sweep, "Operation Cyber Loss."

I. INTERNET FRAUD

Internet fraud, in all of its forms, is one of the fastest-growing and most pervasive forms of white-collar crime. Criminals, both here and abroad, have recognized that the very features of the Internet that many people find appealing—its global reach, its ability to communicate instantaneously with millions of people at virtually zero cost, and the relative anonymity that its users have while online—can be turned to their advantage for fraudulent purposes. Regrettably, criminal exploitation of the Internet now encompasses a wide variety of securities and other investment schemes, online auction schemes, credit-card fraud, financial institution fraud, and identity theft. If law enforcement does not move aggressively to respond to this threat, there are significant indications that the threat will become more severe and more pervasive over time.

A January 2001 study by Meridien Research, for example, reports that with the continuing growth of e-commerce, payment-card fraud on the Internet will increase worldwide from $1.6 billion in 2000 to $15.5 billion by 2005. The Securities and Exchange Commission staff reports that it receives 200 to 300 online complaints a day about Internet-related securities fraud. Foreign law enforcement authorities also regard Internet fraud as a growing problem. Earlier this year, the European Commission reported that in 2000, payment-card fraud in the European Union rose by 50 percent to $553 million in fraudulent transactions, and noted that fraud was increasing most in relation to remote payment transactions, especially on the Internet. Similarly, the International Chamber of Commerce's Commercial Crime Service reported that nearly two-thirds of all cases it handled in 2000 involved online fraud.

To ensure an effective and coordinated response to the problem of Internet fraud, the Department has been pursuing a comprehensive six-part strategy. The elements of that strategy are as follows.

A. Interagency Coordination

First, the Department has taken a number of steps to provide enhanced coordination on Internet fraud prosecutions between law enforcement and regulatory agencies at regional, national, and even international levels. On the national level, for example, the Department has been proactive in maintaining contact with United States Attorneys' offices throughout the country about their Internet fraud cases, and working to develop coordinated actions wherever possible.

United States Attorneys have been compiling a record of significant accomplishments in prosecuting major Internet fraud schemes. The following are but a few of the more recent successful Internet fraud prosecutions by United States Attorneys:

- On May 10, 2001, a federal jury in the District of Colorado found Daniel Ketelsen guilty of charges relating to Internet fraud. Ketelsen received money for computer components he auctioned under false identities but never delivered via eBay. After receiving numerous complaints from victims, Ketelsen filed a fraudulent claim with his insurance company, alleging that the computer components had been stolen from his garage. An investigation by U.S. Postal Inspectors revealed that Ketelsen never had the computer components auctioned on eBay, and was attempting to obtain money illegally from an insurance company.
- On March 8, 2001, a federal jury in the Southern District of New York convicted Fred Moldofsky, on securities fraud charges for distributing over the Internet a series of fake press releases regarding Lucent Technologies. The evidence at trial showed that on March 22-23, 2000, Moldofsky, a self-described securities day trader living in Houston, used the Internet to distribute a series of 19 fake

press releases purporting to announce that Lucent expected its earnings for the second quarter of its fiscal year 2000 to fall short of analysts' expectations. After Moldofsky's posting of these messages on a Yahoo! message board, on the morning of March 23, 2000, the price of Lucent's common stock declined by as much as 3.6 percent, resulting in losses of millions of dollars by investors who sold Lucent stock at artificially depressed prices. Later that morning, when Bloomberg News announced that Lucent had confirmed the release to be fake, Lucent's common stock price rose by approximately $5 per share in less than eight minutes.

- On December 27, 2000, a federal judge in the Central District of California sentenced two defendants in a business opportunity fraud scheme to 27 months' imprisonment and more than $100,000 in restitution to fraud victims. The defendants in this case had pleaded guilty to fraud-related charges stemming from their sending out more than 50 million "spam" e-mails, fraudulently soliciting money. The e-mails, which targeted students, the elderly, and others, promised enormous returns from a "work-at-home" scheme in exchange for the payment of a so-called "processing fee" of $35. The scheme resulted in approximately 12,405 victims sending money to the defendants. (It should be noted that the cost of sending these 50 million spam e-mails was less than $100. By contrast, sending the same number of messages by first-class mail, at 34 cents per envelope, would have cost the defendants approximately $17 million in postage alone.)

  To misdirect people who wanted to complain about the solicitations or the lack of action after the "fees" were paid, the defendants' "spam" included a forged return address, making it appear that the point of origin was an Internet service provider, BigBear.Net. Irate Internet users sent approximately 100,000 e-mails in response, mistakenly believing that BigBear.Net had sent the spam. This flood of messages led to the "crash" of BigBear.Net's Internet computer file servers. The company that operated BigBear.Net also had to hire three temporary workers for nearly six months to respond to these complaints. Ultimately, the court's restitution order included not only individual victims but the victimized company.

The Department also fosters national-level coordination through its chairing of the interagency Telemarketing and Internet Fraud Working Group. This Working Group, which meets quarterly, brings together representatives of numerous United States Attorneys' offices, the FBI, the Secret Service, the Postal Inspection Service, the Federal Trade Commission, the Securities and Exchange Commission, and other law enforcement and regulatory agencies. The Working Group meetings enable agencies to share information about trends and patterns in Internet fraud schemes, to brief members on noteworthy legal and policy developments, and otherwise to encourage closer and more active communication on Internet and telemarketing fraud matters.

At the international level, the Department of Justice has played a leading role in initiating discussions about Internet fraud at subgroup meetings of the G8's Senior Experts Group on Transnational Organized Crime (also known as the "Lyon Group"). These discussions have led to the G8 Ministers of Justice identifying Internet fraud as a significant threat to the growth and development of e-commerce, and committing to adopt a comprehensive response to the problem that includes investigation, prosecution, and prevention. Discussions on followup measures on Internet fraud are being pursued in the Projects and High-tech Subgroups of the Lyon Group.

B. Support and Advice on Prosecutions

Second, the Department provides continuing support and advice on Internet fraud prosecutions to federal prosecutors. As a result of its continuing contact with Assistant United States Attorneys who handle Internet fraud cases, the Department has compiled a substantial "brief bank" of pleadings and other legal materials that prosecutors may find useful. The Department makes these materials readily available to United States Attorneys' offices throughout the country. The Department is now working to establish an Intranet on Internet fraud to improve communication and information-sharing among its prosecutors. The Department, through the Fraud Section and the Computer Crime and Intellectual Property Section of the Criminal Division, also routinely provides legal and practical advice to federal prosecutors working on Internet fraud cases.

C. Training for Prosecutors and Agents

Third, the Department has demonstrated its commitment to ensuring that prosecutors and agents receive appropriate training to conduct Internet fraud investiga-

tions and prosecutions effectively. At its National Advocacy Center, the Department has established basic and advanced training courses on Internet fraud. The Center has a basic Cybercrimes course, presented several times a year, that now includes a track on Internet fraud. The Center has also conducted two advanced Internet fraud courses for more than 180 federal, state, and local prosecutors, FBI agents, and even foreign prosecutors from Canada, Germany, Hong Kong, and the United Kingdom. The Department has taken affirmative steps to invite foreign prosecutors to these courses, because it regards Internet fraud as a global problem that will require increased understanding of how U.S. and foreign prosecutors can work together more effectively. The Department has also provided expert speakers on Internet fraud issues for training sessions at the FBI Academy and other law enforcement and regulatory training programs.

D. Investigative and Analytical Resources

Fourth, the Department has recognized the need to develop investigative and analytical resources, so that agents and prosecutors can more quickly identify Internet fraud schemes while they are still underway and develop effective enforcement responses. To that end, it has supported the establishment of the Internet Fraud Complaint Center (IFCC), a joint project of the FBI and the National White Collar Crime Center. The IFCC receives complaints from members of the public in nearly 90 countries about various types of Internet frauds and other Internet-related crimes. It then analyzes the fraud-related complaints for patterns, develops additional information on particular cases, and sends investigative packages to law enforcement authorities in the jurisdiction that appears likely to have the greatest investigative interest in the matter.

E. Education and Prevention

Fifth, the Department has been actively pursuing new measures for public education about, and prevention of, Internet fraud, with appropriate collaboration between government and the private sector.

F. Nature and Scope of the Problem

Finally, the Department continues to work closely with other agencies to develop better information about the nature and scope of Internet fraud. The IFCC's data compilations are expected to be increasingly useful in identifying longer-range trends and patterns of Internet fraud schemes, including statistical data that law enforcement and regulatory agencies may find useful in allocating resources and devising enforcement strategies. The Department has also worked closely with the Federal Trade Commission (FTC) to enhance the quality and availability of data from complaints about Internet-related consumer fraud that the FTC receives for inclusion in its Consumer Sentinel database.

This summary of the Department's efforts against Internet fraud should help to demonstrate that the Department is wholeheartedly committed to an aggressive strategy for combating Internet fraud, and that this strategy is based on fostering improved cooperation and coordination at all levels of government.

II. IDENTITY THEFT

With your permission, Mr. Chairman, I would like to turn to the issue of identity theft. Identity theft, and the crimes that it furthers, can take advantage of the Internet, but can be committed online or offline.

Law enforcement has made remarkable strides in dealing with identity theft as a crime problem over the last two years. One of the first steps that needed to be taken was to ensure that identity theft is clearly identified as a serious crime. Before October 30, 1998, when the Identity Theft and Assumption Act of 1998 (18 U.S.C. § 1028(a)(7)) became law, there was no federal statute that made identity theft a crime, and state statutes on identity theft were few and far between. Only two years later, federal prosecutors are making substantial use of the statute. To date, we have identified at least 92 cases in which U.S. Attorneys' offices throughout the country have made use of that section in prosecuting cases that involved identity theft. Here are some examples of federal identity theft prosecutions that the Department has been pursuing this year:

- In California, a defendant was sentenced to 27 months' imprisonment and five years' supervised release after pleading guilty to identity theft and related charges. The defendant stole private bank account information about an insurance company's policyholders and used that information to deposit approximately 4,300 counterfeit bank drafts, totaling more than $764,000, and withdraw funds from the accounts of the policyholders. *United States v. Johnson* (C.D. Cal.).

- In Delaware, two defendants were sentenced to terms of imprisonment after pleading guilty to identity theft. The defendants obtained names and Social Security numbers of high-ranking military officers on the Internet and used them to apply for credit cards and bank and corporate credit in the officers' names. One defendant was sentenced to 33 months' imprisonment, three years' supervised release, $160,910.87 in restitution, and a $100 special assessment; the other was sentenced to 41 months' imprisonment, three years' supervised release, $126,298.79 in restitution, and a $100 special assessment. *United States v. Christian* (D. Del.).
- In Texas, a man was indicted on identity theft and related charges, after allegedly creating false identification documents in the name of his deceased brother-in-law and twice applying for a U.S. passport in the brother-in-law's name. *United States v. Ipi* (S.D. Tex.).
- In the State of Washington, a defendant pleaded guilty to identity theft, after using the date of birth and Social Security number of another individual (with the same first and last names and middle initial) to obtain credit cards and an automobile loan. *United States v. Wahl* (W.D. Wash.). Another defendant pleaded guilty to identity theft and related charges, after participating in a conspiracy to use the identities and names of others to obtain credit cards, open banking and investment accounts at numerous locations, and negotiate fraudulent and counterfeit checks. *United States v. Tomaszewski* (W.D. Wash.).

Approximately 40 states have now enacted statutes to prohibit identity theft, and other states are considering such legislation. Moreover, to ensure that persons convicted under the federal identity theft provisions receive appropriate sanctions, the United States Sentencing Commission has issued Sentencing Guidelines for identity theft. The new Guidelines establish a two-level enhancement, in addition to the offense level dictated by the amount of loss, where the identity thief has used "breeder documents," such as Social Security cards. Even if there is no loss, the Guidelines will set a "floor"—that is, a minimum offense level—of 12, which would ensure a jail sentence that could be as high as 10-16 months, even for someone with no prior criminal convictions. The Guidelines also invite upward departures for more severe sentences in cases where egregious conduct seriously affects individuals (for example, where the criminal "takes over" a victim's identity).

Until recently, victims of identity theft had no single national point of contact to report instances of identity theft or get advice on how to deal with identity theft, and law enforcement had no single place to which they could go to find and review complaints from identity theft victims in their jurisdictions. Under the 1998 Act, the Federal Trade Commission established a national toll-free number [1-877-ID-THEFT] for victims to call, and has made the identity theft complaints available to law enforcement through its Consumer Sentinel data base.

Similarly, until recently federal, state, and local law enforcement had no means by which they could coordinate their efforts and resources to deal more effectively with identity theft. We now understand that identity theft—while it may appear in any one case to be a comparatively minor violation—is a crime problem of significant proportions, and one that calls out for genuine and sustained cooperation among federal, state, and local law enforcement.

Today, law enforcement is vigorously pursuing two distinct approaches to improved coordination. First, soon after the enactment of the Identity Theft and Assumption Deterrence Act in 1998, the Attorney General's Council on White Collar Crime established a Subcommittee on Identity Theft. This Subcommittee is intended to provide appropriate coordination and coherence in the fight against identity theft.

The Subcommittee, which includes all of the major federal law enforcement agencies, operates to foster closer coordination among all levels of government. Its growing list of accomplishments includes preparation and distribution of guidance memoranda about the identity theft offense to United States Attorneys' offices, federal, state, and local law enforcement agencies, and numerous government agencies, such as the Social Security Administration's Office of Inspector General, the FTC, the SEC, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Federal Reserve Board, and the Department of the Treasury. The Subcommittee also has assisted the FTC and other agencies in preparing and distributing educational and other materials directly to consumers and victims of identity theft, in an effort to prevent or ameliorate the effects of this crime. Much of this progress is due to the leadership of the Criminal Division's Fraud Section, which continues to devote significant resources to the work of the Subcommittee.

Second, in the field, law enforcement agencies are establishing closer working arrangements, such as identity theft task forces, to investigate and prosecute appropriate cases more efficiently:

- In the Western District of Washington, a Special Assistant U.S. Attorney, employed by the Social Security Administration, has been instrumental in the development of an Identity Theft Working Group. The group includes representatives from the U.S. Attorney's Office, the U.S. Department of Agriculture, the Veterans Administration, the FBI, the Immigration and Naturalization Service, the IRS Criminal Investigation Division, the Postal Inspection Service, local law enforcement, county prosecutors, the Washington State Department of Health and Social Services, and the Washington State Attorney General. The Working Group is addressing training on fraud and identity theft, coordination of statistics on identity theft, and outreach.
- In the District of Maryland, investigators have set up a multiagency task force on identity theft that includes representatives of the U.S. Secret Service and local police.
- Other informal arrangements or task forces are now established or being established in Cleveland, Detroit, St. Louis, and Los Angeles.

Only two years ago, there was no nationwide program to educate and warn the public and law enforcement about identity theft. To date, we have taken a number of significant steps to inform the public about the seriousness of the problem. The FTC has an extensive collection of online resources and materials about identity theft, available through the Web site at www.consumer.gov/idtheft. In addition, the Fraud Section of the Department's Criminal Division has a series of Web pages on identity theft that are posted on the Department's Web site, www.usdoj.gov. These Web pages include information about the nature of identity theft, what the Department is doing about it, and how consumers can better protect themselves from identity theft. These Web pages are linked to the FTC Identity Theft Web site, and other law enforcement Web sites, to help consumers immediately contact other agencies that can assist them in addressing their personal problems resulting from identity theft.

Furthermore, last year the Treasury Department, the FTC, the Social Security Administration, the Secret Service, and the Department of Justice sponsored a series of events to highlight the problem of identity theft. The Treasury-sponsored Identity Theft Summit, which was open to the public, included panel discussions on victims' experiences; federal and state prevention programs; private sector prevention programs; federal, state, and local investigative and prosecutive actions in response to identity theft; public and private sector remediation programs; possible future trends to be anticipated in identity theft; and identifying areas for enhanced cooperation between governmental and private sector. As a followup to the Summit, three workshops on identity theft were held focusing separately on remediation (FTC), prevention (Social Security Administration) and law enforcement (Department of Justice) strategies.

We have made a good beginning to combat identity theft in a more coordinated and effective fashion. We must, however, continue the efforts we have begun in order to have a lasting impact on the identity theft threat.

Mr. Chairman, that concludes my prepared statement. I would be pleased to respond to any questions that you or other Members of the Subcommittee may have at this time.

Mr. STEARNS. I thank you. I say to my colleagues we have here in front of us the Justice Department, the FBI, the FTC and the Secret Service and we have within each of these agencies they have talked about this new sense of cyber crime. And as this committee goes forward, I think what we're hearing from you is that it's often rolling, this cyber crime, even as we speak, the FBI is talking about 56,000 victims that these crimes have been perpetrated on at a cost of $117 million. That's roughly, if you take the 90 people that are going to be arrested, I guess as we speak, you're talking a little over $1,300,000 per person who perpetrated those crimes. So it's quite, as you said, Ms. Harrington, target rich. These people are out there. And the thing we have to realize is that this is perhaps just the tip of the iceberg. What each agency is talking about, the FBI talks about their complaints that they set. They've got 36,410, of which 30,000 were validated. The FTC—each of you folks have talked about the complaints and how you're trying to go through it. So we might be talking about something much larger

than even you have identified and the thing that worries Members of Congress, I think, is do you have the resources to deal with this? If you take a GS-5 and GS-9 and bring he or she over, can that individual have the capability to handle this?

So I would like to—let's start out with Mr. Kubic, do you have the resources in place to handle this, the technology or when the consumer goes out there and dealing with the industry, is the person who has the technology at an advantage or do you have resources to even identify and be comprehensive with the problem?

Mr. KUBIC. Mr. Chairman, I'd like to answer that question in the context of the overall law enforcement effort rather than just the FBI's commitment because we recognize that it would be extremely difficult to address the problem of 56,000 victims nationally just based on FBI Agents knocking on doors, doing interviews. So we have to be aware of what tools are available.

For instance, at the Internet Fraud Complaint Center, that whole process results in the first steps at obtaining the required evidence that we need to take to the U.S. Attorney's Office to present a case. So if we take advantage of the technology that's available and use the on-line reporting, for example, we get a step up, an advantage in making those cases.

Second, I think what's going on through the National White Collar Crime Center is a major effort at education and training for State and local law enforcement officers with these new tools, techniques, they become much more efficient and effective at conducting those investigations. So I'd say that while it's extremely difficult to commit the 2400 Agents who work white collar crime nationally to this one particular area of fraud, by partnering up with the Secret Service, the FTC, also the Postal Inspectors and IRS, we have somewhat of a multiplier effect as the Agents and Police Officers and Detectives who are well-trained, move forward to address these complaints.

Mr. STEARNS. So Mr. Kubic, you're saying this morning that you have the resource to combat future Internet cyber crime?

Mr. KUBIC. It would depend on the growth of the problem as well, Mr. Chairman. I mean if we see the effect of the law enforcement effort is to reduce the instance of some of these crimes, I think that we may be able to dampen the overall amount of crime that occurs.

I'd also point out that the private sector is very aggressive in protecting their intellectual property rights, as well as their assets in their commercial activity. As it was previously mentioned, there is a strong bottom line profit motive, don't want to lose customers.

Mr. STEARNS. Mr. Townsend, what are the most common ways in which ID information is stolen? Can you just give us an example?

Mr. TOWNSEND. Certainly, I believe Mr. Swartz referred to the fact that frequently the crime of identity theft is one that is perpetrated via the Internet, but we also see low tech means of identity theft. In the Secret Service, we view identity theft really as a disturbing combination of old schemes and new technology. Frequently, we see criminals that will hack into Internet merchant sites and steal credit card numbers and accompanying personal data about those customers and begin to use that, not only across

this country, but in a trans-national fashion. We have seen cases where a hacker in Moscow broke into a system located in the United States, sent that personal information and credit card numbers to a co-conspirator in Buenos Aires where merchandise is purchased and transshipped to Miami for sale on the street. It raises a lot of interesting questions. Where's the venue for that prosecution? Who's going to step up and investigate a case like that?

So as I mentioned in my opening statement, the effects of the IT revolution, combined with globalization have really changed the whole landscape of law enforcement.

The Internet provides the criminal with access to victims, literally an unlimited pool of victims. In low tech schemes one had to have some physical access to his or her victims. Well, the Internet has changed all that.

Mr. STEARNS. My time has expired, but Ms. Harrington, what is your toll free number?

Ms. HARRINGTON. 1-877-FTC-HELP.

Mr. STEARNS. Okay, the ranking member?

Mr. TOWNS. Thank you very much, Mr. Chairman. Let me begin with you, Mr. Swartz. You said today the Department of Justice and the FBI are announcing a major enforcement operation targeting Internet fraud, one of the fastest growing and pervasive forms of white collar crime.

The threat of Internet fraud calls for forceful action and today the Department and the FBI in partnership with the United States Postal Inspection Service, the Internal Revenue Service, the Criminal Investigative Division and Customs Service and you go on and on, you said States and local enforcement and all of that.

Let me ask the question, is coordination and cooperation enough? Should there be some new statutes? Or can you do it just with coordination and cooperation?

Mr. SWARTZ. Mr. Towns, thank you for that question. I think that the question as to whether or not legislation is sufficient is always a critical one and one that we're constantly reevaluating at the Department of Justice. Certainly the identity theft statute of 1998, was an important development.

At the current time we believe that we have the legislative tools for dealing with matters such as "Operation Cyber Loss". Of course, it is a matter that we will continue to consider and analyze, particularly as Mr. Kubic suggests, as we analyze how Internet fraud is developing and increasing. But for now and pending, of course, any decisions made by the new administration, I believe that we do have the legislative tools in hand to deal with this problem.

Mr. TOWNS. Let me switch over. I don't want to start a fight, but I just want to go to you, Mr. Kubic in something that you said that in some way or another ties into this. You indicated let me begin by emphasizing that the FBI places a high priority on investigating Internet fraud matters and is committed to working with this subcommittee and all of Congress to ensure that law enforcement and the private sector, have the necessary tools and protections to combat these crimes.

Now are you saying more needs to be done? I just want to make certain this is clear. I'm not trying to start a fight.

Mr. KUBIC. No, no, that's a good question. I think we're saying the same thing. Basically, what I was suggesting was that as we delve into the problem, as we understand the operations of some of these criminal organizations, there may come a time when we need to come back and identify some flaws in the current legislation that they are exploiting. That being the case, that was the genesis of my initial comment, that we would like to have the opportunity, that as these investigations progress, should there be a need for additional legislation, we'd work with the Department of Justice certainly and the committee to make some recommendations.

At this time, the laws are quite adequate to address this particular problem.

Mr. TOWNS. You mentioned the working group. Thank you, Mr. Kubic. You mentioned the working group. Would the working group consider these kind of matters as well?

Mr. KUBIC. Yes, that would be the kind of matter that would be before the working group, not only the trends in Internet crime, but what steps, if necessary, to take with regard to seeking additional legislation. But that's exactly the kind of forward looking problem that they try to deal with.

Mr. TOWNS. Thank you. Ms. Harrington, you mentioned the Commission has conducted 25 different surf days targeting problems ranging from cure-all health claims to fraudulent business opportunities and credit repair scams.

More than 250 law enforcement agencies or consumer organizations are around the world have joined the Commission in these activities. Collectively, they have identified over 6,000 Internet sites making dubious claims.

First of all, my question would be what happened, No. 1, and how many sites were corrected, and of course, I guess the other part of the question would be were they corrected voluntarily or in other context?

Ms. HARRINGTON. Thank you for that question. Internet surf days are a way for law enforcement to let operators of sites that make these dubious claims know that law enforcement is on the beat. We focus on a specific problem. We organize our law enforcement partners to visit specific parts of the web during a time period, download for evidentiary purposes, what they find that is suspect and then several things happen. No. 1, a message goes out to those site operators from law enforcement. It might say we're the FTC and we visited your web site today and we want you to know what the law requires. And we tell them what the law is. Or our partner tells them what the relevant law is in the United States, in Norway, in Finland, wherever it is that our surf partners are located.

So first we send basically a warning message with information about what the law requires.

Second, some time later we go back and do a follow-up surf on those sites that we found in the first instance that raise problems to see whether they're still engaged in the behavior that caused us to be concerned. And what we find there really has varied from problem area to problem area. We find in a significant percentage of instances that either the site has been taken down or the claims

that we were concerned about in the first place have been corrected, where we find evidence that they're still doing the same thing, then that site operator becomes a prime target for follow-up investigation and enforcement. And we at the FTC and our enforcement partners have brought many enforcement actions to stop those bad practices.

Can we get them all? No. But by being on the beat, by giving the information needed to know how to comply with the law and interestingly, we find whenever we do a surf that there are some site operators who are engaged in illegal behavior and they don't know that it's illegal. They're copying what they see others do and because they've seen someone else do it, they think well, this must be all right. And when we tell them that it's not all right, they not only stop it, but we get thank you notes from people who almost ran afoul of the law.

Mr. STEARNS. The gentleman from Illinois, Mr. Shimkus, you're recognized.

Mr. SHIMKUS. Thank you, Mr. Chairman. Under the Gramm-Leach-Bliley Act, pretexting was allowed to be enforceable under the law and I know the FTC has about three cases seeking—my first question is to Mr. Swartz. Your testimony does not address pretexting and the question is has the DOJ taken any pretexting cases up yet?

Mr. SWARTZ. If you allow me to consult with my colleague for a moment?

Mr. SHIMKUS. I can give you the answer.

Mr. SWARTZ. At the present time I am informed while there are investigations that are on-going, there are no pending prosecutions.

Mr. SHIMKUS. And the law on pretexting has been in effect for about 18 months, is that correct? Do you expect to address the pretexting issue in the future or why have you not been more vigilant in this one area?

Mr. SWARTZ. We certainly hope that the investigations will bear fruit and they will lead to criminal prosecutions, but it is a matter that is being pursued through investigations.

Mr. SHIMKUS. Let me and it will be an area that will be vigilant and watching the Department of Justice in their good offices, address this issue.

The concern that I have and there's very good diligence being done by the different agencies, with all the different agencies' finger in the pie, is that helpful or is that harmful? In other words, where do we get a better bang for our buck and more streamlining of the process if we had one agency take the lead on all these issues and without the—because there is some collaboration and I listened to the opening testimonies and some of the questions and answers. There's collaboration being done. But all the things falling through the cracks because we have sliced up aspects of who's doing what and I'd like for each agency,if you would just go down the table, starting with Mr. Kubic and address that concern that we would have as policymakers about the efficiency of the multitaskings with the different agencies?

Mr. KUBIC. It's my opinion that each one of the agencies represented at the table here brings a particular unique expertise to the problem. For example, with regard to the Bureau's investiga-

tions of these matters, our primary focus is the determination as to whether or not there's a criminal enterprise that's engaged in this particular type of fraudulent activity so that the result of our investigation is not one particular individual, but it's thorough enough to get to the full understanding of that organization and how they're using the Internet to defraud people.

I think that as you hear from my associates to the left of me, each has a particular thing that they can bring to a task force investigation or a civil enforcement action that is somewhat unique. Absent that, I think what we'd see is the development of an organization which would be pretty large and cumbersome and not particularly nimble and able to respond to the emerging crime problem that we see.

Mr. TOWNSEND. If I could address my comments to the issue of identity theft. In the Secret Service, although I don't want to speak for Mr. Kubic, I think he would agree, enforcement agencies are about criminal case,s about getting people indicted and getting them locked up.

Identity theft is a crime that is a particularly invasive crime. I have had the opportunity to interview victims of identity theft who after being victimized repeatedly over time showed the symptoms of almost someone who was physically assaulted, so this is a crime that is about more than the theft of money or property, although that's important. It's about the theft of one's good name, reputation in the community, years of hard work and commitment to goals. In the enforcement world we have a limited ability, once we get the criminal locked up to help that victim. We want to help them, but we have limited ability and mandate with regard to victim witness. Now we do have some mandate in that area which we carry out with regard to helping victims and witnesses, but we're not equipped, frankly, to go on once that guilty verdict hopefully comes in. The Federal Trade Commission is and they are about making those victims whole which is, I think, a critical aspect of this and as Ms. Harrington stated in her opening testimony, we have detailed a full-time Secret Service Special Agent to the FTC to make sure that there is not a dropping of the ball, if you will, between that criminal prosecution and getting these victims made whole again.

So your point is well taken. We, in the Federal Government, we in law enforcement because of our law enforcement system have to be very vigilant about coordination because we're a country with so many different law enforcement agencies.

Do some things fall through the crack, probably so, but I think we're getting better. The Attorney General's White Collar Crime Council, the Identity Theft Subcommittee of all the ones that we participate in, and you know about them, in my view is among the most effective. Out of that group, that subcommittee has come at least two and maybe three identity theft white collar crime summits where real people and real law enforcement officers came in for an exchange of ideas.

Ms. HARRINGTON. Mr. Shimkus, I think that one of the most important ways to keep things from falling between the cracks is to share two kinds of information. One, who's doing what and two, what are the complaints? The good news is that computers in the

Internet enable law enforcement at all levels to do that better than ever before. We no longer have to rely on somebody picking up the telephone to call an agency to say hey, we're looking at so and so, do you have anything? And that's one of the reasons that we developed Consumer Sentinel and make it available for free to every law enforcement agency in the United States and Canada. Agencies can put alerts on Sentinel to let one another know who's looking at what, who needs more information and it's critical that all of the complaint data be central sourced and immediately available to all law enforcement and so that's why we have Consumer Sentinel and I think it goes a long way toward preventing that kind of problem that we have when things fall between the cracks.

Mr. SWARTZ. Certainly the question is an important one, but given the nature of Internet crime, generally, and Internet fraud, in particular, both its scope and diversity as a type of crime and its global reach, we believe it's inevitable that numerous Federal law enforcement agencies will be involved—and we believe because of the expertise they bring, as Mr. Kubic has suggested, they should be involved. But the Department of Justice considers its primary charge in this regard to be attempting to coordinate the response and ensuring, as you say, that cases do not fall through the cracks. We think we've gained from the cooperation of the different law enforcement agencies, but we recognize this is an on-going task that we have to continue.

Mr. STEARNS. Thank you. Ms. DeGette?

Ms. DEGETTE. Thank you, Mr. Chairman. One of the intriguing aspects, I think, about cyber crime is just that, that it's cyber crime and by nature much more ephemeral than something like a guy running into the local 7-11 and holding it up. It's a lot harder, sometimes, to find the perpetrators and I know several of the witnesses alluded both in their oral and written testimony to some of the international efforts that we're making to address cyber crime which I think is essential, a really essential component to beginning to address this, much more essential than traditional law enforcement challenges that we face. I know you're all nodding in agreement.

I'd like to talk a little bit more about that. In particular, about G-8 efforts and other efforts. Now Mr. Swartz, I know you talked in your written testimony about the G-8 efforts and nations agreeing to take action to criminalize certain computer abuse, designating a high tech point of contact to respond quickly to computer-related crimes and so on. Apparently, there's some follow-up discussions going on.

I wonder if you could tell me what the status of the efforts are, either at the G-8 or in EU context, other kinds of international cooperation?

Mr. SWARTZ. The G-8 senior experts group, commonly known as the Lyon Group has been for the United States one of the leading means of dealing with cyber crime issues. Its on-going standing sub-group in the high tech crime area, continues to meet to try and develop, as you suggest, the 24-7 network, that is the 24 hours, 7 days a week network to deal with computer crime and to address the future trends in this criminal area.

In addition, the United States works closely with the EU through the new trans-Atlantic agenda. We have met frequently with our EU partners to discuss cyber crime issues. The EU itself has issued recently a cyber crime communique or declaration on which the United States has commented. And then finally, there are negotiations on-going now with regard to a cyber crime convention with the Council of Europe, in which the United States is an observer but has played a role in attempting to ensure that United States interests are advanced by that convention.

Ms. DEGETTE. I think it's great that we're having meetings and discussions and so on. What kind of timeframe are we looking at for developing guidelines and what kinds of enforcement efforts are being taken in the EU countries or in the G-8 countries, I mean having talks is great and developing protocols is super, but until countries have laws that mirror ours, I'm not sure how effective it's going to be and once you finish, I see Ms. Harrington has a response.

Mr. SWARTZ. Certainly a number of our G-8 partners and EU partners have taken steps to ensure that they can prosecute these cases. The cyber crime convention being developed by the Council of Europe would require that legislation be enacted in signatory countries to deal with the issue. We agree that the purpose of the Lyon Group is not only to ensure that there are, as you say, protocols and guidelines, but to encourage actual prosecution of Internet fraud cases.

Ms. DEGETTE. Ms. Harrington?

Ms. HARRINGTON. Ms. DeGette, in addition to the work that was just described, as you know, treaties and changing laws takes a long time. We've been working on some practical and immediate approaches. One is through the International Marketing Supervision Network which is an organization of consumer protection law enforcement authorities from OECD and other countries and through that group we have been able, for example, to organize these international surf days to work together with those enforcement authorities to take action against perpetrators in their own countries who are on the web and scamming consumers all over the world.

We just launched with the IMSN a project called e-consumer.gov which is the first worldwide website where consumers can go and make fraud complaints. There are 13 countries participating in this and these are very practical——

Ms. DEGETTE. I understand. How many of the countries we're talking about, how many of the EU countries or the G-8 countries or others actually have laws that are parallel to our law that are directed at stopping this kind of cyber crime? Do you know or somebody else?

Ms. HARRINGTON. There are 29 or 30 countries that are part of the International Marketing Supervision Network. And I believe that all or almost all of those have laws like the FTC Act that prohibit deception in commerce and give those authorities some remedies that are immediately available to stop that kind of scheme.

Now we're a civil law enforcement agency at the FTC and many of our counterparts are as well. On the criminal side, I'd have to defer to Mr. Swartz.

Mr. SWARTZ. We'd be glad to respond for the record on that, if we could, and give you a listing of the various statutes.

Ms. DEGETTE. I think that would be very useful for the committee.

Mr. STEARNS. If you would be so kind as to send it to the chair and then we'll give it to Ms. DeGette.

And I thank the gentle lady. Mr. Upton?

Mr. UPTON. Thank you, Mr. Chairman. As I sit back and listen to the testimony and I've talked to my folks at home, there's not a nightmare that anyone—this is a nightmare that no one wants to experience and particularly for my field office folks, the FBI, look at the Western Michigan Marshal Service and others, I guess wire fraud is the main hook that you go after these folks.

Let's say as you look at today's world, it's real easy to log on to your own bank account and get it on the Internet, find out exactly where you are. It's real easy to order a Chicago Cubs or a St. Louis Cardinals jersey and get it delivered or University of Michigan ball cap, something like that, but all of a sudden that information is out there and as they steal one's identity, we learned of a case where literally the employees of one business were shipped monthly their vacation days and what they had left for the balance of the year and next to their name was their Social Security Number and someone picked that information up and set up a false account on the other side of the State with a telephone company. Thousands of dollars of bills added up. Of course, they went to the collection agency, the individuals didn't know anything about it. Only until they moved away and they tried to get a mortgage and they found out that there was a lien on their account.

Now if they go to the—I come from a small town, 12,000 people. The Police Department there probably can't, doesn't have the expertise to handle a situation like that, unless it's compounded with all these—literally, I think there are more than 150 individuals in this one case. But what is the threshold that Secret Service or the FBI will begin to look at a case versus someone that's all on their own and maybe it's a few thousand dollars, maybe it's a little bit more. I know tom Siegel had a pretty big case, $10 million they took out of his account. Not a lot of people have $10 million, but they got him. There are a lot more that are considerably smaller and I'm wondering what level do you all begin to examine.

The other thing I'd like you to comment on as part of that is my friend, Mr. Shimkus, mentioned the hearings that he participated in last year. I was not on the Subcommittee on Encryption. Of course, the administration's view is really a paradox. They were opposed to stronger encryption technology being used, but as an individual that wants to purchase something, you'd think that if you allowed those, whether it would be a lending institution or a mail order hours, to in fact have the tools on encryption to better protect and build some firewalls so that that information, that type of personal information cannot be divulged, you wouldn't have the caseload that you have today. The administration, particularly, Mr. Freeh weighed in very heavily against allowing that technology to get out the door.

So I'd be interested in your thoughts on both and start with you, Mr. Kubic.

Mr. KUBIC. Let me start by answering your first question which is is there a dollar amount that triggers an investigation?

By way of example, in the last year we actually referred out a case that was at the $180 level and within a week of receiving the complaint, the Police Officer knocked on the door of this lady who was defrauded out of some tickets that she never got and gave her back the $180. Frankly, she was very surprised at the speed with which this particularly fraudster decided that he didn't want to have anything to do with violating a Federal law, nor did he want anything to do with having the cops knock on his door very often.

So we don't want to do a lot of $180 cases, but the fact is that for purposes of collection of information and linkages, we really need to do some of that and we need to do it at some fairly low dollar levels, things that we're not normally known to be engaged in in terms of investigative priorities.

So we'll look at those. The Miami case that's mentioned in my earlier testimony is basically a $300 loss. However, there are 46,000 victims, so quickly you're into the multi-millions of dollars of an investigative effort. So having said that, I think that the Department and all 96 U.S. Attorneys regularly take the lead from the White Collar Crime Subcommittee in terms of establishing investigative and prosecutorial guidelines. So some of those are unique, but some apply somewhat nationally.

With regard to the Director's opposition to encryption, I think the key factor in the Bureau's position on that was not so much a concern about protecting legitimate transactions, but having the ability to decrypt, if you would, those conversations where we have a court order and the authority to intercept. Some of this encryption technology is very robust and frankly is beyond the ability of many, certainly many law enforcement agencies to decrypt. So I would say or suggest that in a very short time the criminals who are actively exploiting the Internet would, in fact, use that to hide their conversations from each other, to hide the distribution of the monies that were stolen and that really was the basis for the concern of the Bureau as expressed in prior testimony.

Mr. UPTON. Mr. Townsend?

Mr. TOWNSEND. In the Secret Service, in an effort to best utilize the finite resources that we have, we have developed case classifications that our offices are required to select from when opening their cases. Among those case classifications is something we call community impact case. And in the Secret Service, we believe that we are a grass roots law enforcement organization.

While we have a mission and the ability to deal with transnational threats and the fact that we also have 19 Secret Service attaches fully assigned to embassies around the world full-time, the case that you describe someone in a small town in Michigan is one that we very well might find ourselves involved in. Unlike some other agencies, we do not have a policy prohibition against taking a case, a criminal case to a State prosecutor and do that regularly on a regular basis.

In a community impact case, if it's a problem to our local law enforcement partners in that jurisdiction, the city police, the Michigan State Police, we view it as part of our mission to work with them to provide them whatever resources we can in a case which

might under existing U.S. Attorney guidelines for that district might not be prosecuted.

Another case I would like to just very briefly tell you about is one that occurred in Grand Rapids, Michigan during March of this year. There was a homicide case in which a person was murdered. Three suspects came under suspicion. One of our electronic crimes special agents, a fully qualified Secret Service Special Agent who has special expertise in electronic and high tech crimes was requested by the State Prosecutor in that county to examine computers that had been taken from the suspect's residence. In that case, our Secret Service EXAP Agent, Electronic Crimes Agent, recovered 162 e-mails which the conspirators had discussed the case and he testified at jury trial. The suspects were convicted.

A little bit outside what one might think of as a Secret Service's traditional mandate, but an important case to the citizens of Michigan in that case and one that we undertook.

Mr. UPTON. Thank you. I know my time has expired. I yield back.

Mr. STEARNS. I thank the gentleman. The gentleman from Georgia—I would point out to my colleagues, I think we're going to another quick second round, if you had a follow-up question that you want to do before we start the second panel. So Mr. Deal?

Mr. DEAL. Thank you, Mr. Chairman. I realize that this is a multi-faceted problem and all of your testimony, of course has alluded to that. I would have an initial question. Is there anything else that statutorily you see needs to be addressed and is it something that needs to be addressed at the Federal level, local level, etcetera or do you have the statutory tools in place to define the offenses and to provide the mechanisms for the prosecution?

Mr. SWARTZ. Mr. Deal, that's an issue that we are constantly reassessing. We believe at the current time that we do have the statutory tools at the Federal level, particularly with the Identity Theft Act of 1998. But again, it's the kind of issue that our working groups and committees consider to see whether there are any gaps in the statutory protections that are now available.

We should say that we also, of course, work with States and encourage States to make sure that they also have legislative authorities available to help supplement and deal with the cases as well, and we are pleased that 43 States now have identity theft legislation in place. The Federal Government, the Department of Justice and my colleagues here at the table work closely with State and local prosecutors and law enforcement agencies in that regard.

Ms. HARRINGTON. Mr. Deal, the one area that we might commend for study is in the area of international information sharing and cross-border fraud complaint sharing. There might be some improvement or room for improvement with the law there to make it easier for law enforcement to share fraud complaint information across borders.

Mr. TOWNSEND. Sir, in the view of the Secret Service, the Identity Theft and Assumption Act of 1998 gave us the additional tools that we needed at that time. It defined identity theft in and of itself as a crime and frequently we're able now to make a plea outside the traditional prosecutive guidelines that talk about dollar

thresholds, about the fact that the identity theft had occurred in and of itself and it's defined in the statutes.

And as you know, the Internet False Identification Act of 2000 closed a loophole in that law, so in our view we do have the tools to go forward.

Mr. KUBIC. I agree basically with the position of the Department that the tools are currently adequate. We can certainly use a few more prosecutors in some of the districts, however.

Mr. DEAL. Well, that was going to be my next question is that obviously you can have the legislative tools in place as far as defining the offenses, but then the next step is what do you do in terms of manpower and the ability to prosecute and I notice in looking through the material that if you're talking about jurisdictional amounts, Beanie Babies seems to be one of the larger categories, but in total dollars is not large compared with many other categories. What has been the attitude of most of the prosecutorial offices in terms of willingness to accept these cases, and I realize, being a former prosecutor myself, that the nature of these crimes often makes it very difficult because witnesses are far removed, perhaps, from the location where the prosecution may occur.

What has been the general attitude of the prosecutors to accept these cases and to proceed to prosecute them and what other than additional resources might be necessary in that regard?

Mr. KUBIC. I'd say that the Bureau's experience has been very good with regard to the willingness to take on some of the cases. In our partnerships with some of the county DAs and so on, I mean those cases that are referred out to State and local authorities, it's generally positive. There's an interest. Certainly, there's the Beanie Baby example is one of those things that I think is a little bit of a strange situation, if you would, and there may be things that are less dramatic than criminal prosecutions in some of those matters.

So I think a balanced approach is necessary, but our experience overall has been very good.

Mr. TOWNSEND. I would agree with Mr. Kubic in that in approaching high tech crime prosecutions with the various U.S. Attorneys the response has been receptive. Like all of us they are faced with keeping up with the technology challenge to having qualified Assistant U.S. Attorneys to prosecute these very complex cases. In the Secret Service, we frequently send some of our experts to the DOJ Advocacy Center in Columbia, South Carolina so we can share some of our expertise and learn from the DOJ what is going to be required, what the elements of proof are going to be in these evolving cases so we can put those out to our field agents.

Ms. HARRINGTON. One thing I would ad don the Beanie Baby problem, the FTC for the last couple of years has run a program called Project Safe Bid. And that project has our investigators looking at the Internet auction fraud complaints constantly and really packaging up prosecution worthy matters, doing some additional investigation on them and getting them out to local prosecutors. That's been a successful program. We've referred out over 50 auction fraud matters that we've worked up for them and many of those have resulted in local prosecutors bringing action, so where the dollar threshold might not meet the interest or for some other reason there might not be an interest at the Federal level, we have

a network of mostly county DAs and sheriffs who we've worked with who are willing to take these cases on.

Mr. SWARTZ. Certainly from the Department of Justice's point of view coordination and encouragement of these cases is one of our main goals. We've done that, as I mentioned in my opening statement, both by trying to work together on major operations like "Operation Cyber Loss" but also through training of State and local prosecutors and provision of not only packaged cases as Ms. Harrington correctly points out, but also packaged materials, brief banks and other materials, that make prosecution more straightforward.

Mr. DEAL. Thank you.

Mr. STEARNS. I thank the gentleman. The gentleman from New Hampshire, Mr. Bass?

Mr. BASS. Thank you very much, Mr. Chairman. This is a wonderful hearing. I'm sorry I've been in and out during the course of it because the subject matter is so current and I want to start by asking a question that was suggested to me by my distinguished colleague from Michigan who obviously knows a lot—who has forgotten more about this issue than I know.

Mr. UPTON. It's the great State of Michigan, not just Michigan.

Mr. BASS. I didn't yield to the gentleman, Mr. Chairman. I just wanted to give him some credit.

The issue of identity theft and Social Security Numbers, it's my understanding that certain members of the Ways and Means Committee would be introducing legislation having to do with the controlling the proliferation of the use of Social Security Numbers in almost every facet of our lives, from driver's licenses to personal checks and so forth. Is it not true—isn't there a case to be made that the use of Social Security Numbers on Internet transactions are, on the Internet, might be narrowed or controlled in order to deal with the issue of identity theft?

Mr. TOWNSEND. I know that Mr. Hughes, the Inspector General of the Social Security Administration testified I believe yesterday on that matter and certainly I don't speak for the Treasury Department or the administration on the pending legislation, but clearly looking at some way to—let me back up. The Social Security Number is a gateway to identity theft, so looking at ways in which the private industry uses—can continue or can be amended in some way, but looking at a way that we can try to amend what we're doing now is a useful undertaking in our view.

Mr. BASS. What kind of amendments are you talking about?

Mr. TOWNSEND. Well, clearly, as Mr. Hughes stated, the Social Security Number is out of the box. It's used not as the government intended it to be. So while there would be a number of ways to limit that use, we would, of course, have to look at particular proposals and develop a position. But just the undertaking, the beginning of looking at ways to limit the use of the Social Security Number now, in our view, is a good undertaking.

Mr. TOWNSEND. I yield to the gentleman from Michigan.

Mr. UPTON. I just have a—Mr. Bass and I have been talking about this a little bit up here. I know, I think it was part of the Welfare Reform Act that passed several years ago as an effort to go after deadbeat parents, often Dads. The Social Security Number,

States are now required to log in the Social Security Number as part of the driver's license. I know in the State of Michigan, we've never had the Social Security Number literally on the face of the driver's license before. We are now, I believe, required to make that change. And I have been one, among those, that have thought that that was a bad idea. I know that they've been using Social Security Numbers in almost any transaction, a bank loan, buying and purchasing a car, all of that thing. You've got to rattle off that digit. It's got to be part of the application and I would think that it's fairly easily stolen. And as you suggested, it's a pretty easy gateway then to get into the personal information that might be accumulated with that particular individual, and so although I haven't seen this legislation either that's referred to in the National Journal today, I'm inclined to think that it's a good idea and would lend my support to it.

Mr. KUBIC. Mr. Upton, if I could just volunteer somewhat of different view. It seems to me that the problem that relates to the identity theft is that the individual whose identity has been stolen by a Social Security Number, for example, it takes so long for that—the fact that it had been stolen to work its way through the commercial system as well as through law enforcement.

I would think that a quick validation that somebody stole Tom Kubic's Social Security Number and his name would result in a reissue o fa new Social Security Number and basically a closing of those old accounts. So the suspect or the subject is immediately stopped or prohibiting from engaging in any transaction with that number because it's not valid. That would require some work with the Credit Bureaus, those people who are doing a lot of commercial transactions or logging by commercial activity as well as the banks. But it just seems to me that to try to prohibit the States who are using it as a form of identification, it might be the wrong way of trying to do it.

Mr. UPTON. We had a situation in Michigan a couple of years ago where some clandestine group went out and they literally went after virtually every public official within the county, township officials, postmaster, postmistress, I mean a whole number of folks and through their own kangaroo court exercised some judgment against them and because they had the Social Security Numbers they were able to affect all of their credit ratings, so when they went to refinance their mortgage because the rates came down, there was a block on it that literally took months and months and they had no idea that this had happened and it was because probably, I didn't see y our personnel sheet coming in that you were testifying today, but it may, in fact, have been your Social Security Number on that cover sheet, I don't know.

Mr. Stearns, is it on there?

Mr. STEARNS. I don't think so.

Mr. KUBIC. I'm pretty familiar with the process that you're talking about. Some of the right wing types were engaged in that where public officials were liened up based on some judgments that they held against them. Once again, I think the fix may be to kill my old Social Security Number and give me a new number, if in fact that can be validated through the Social Security Administration.

The account and the information would stay the same, how many quarters and so on.

Mr. BASS. Reclaiming my time. What's left of it. Even worse is the reason for this whole legislative effort to begin with which was the murder of one of my constituents due to a purchase of a Social Security Number for a nominal fee by an individual who wound up stalking her. These are very, very serious issues that need direction and control by policymakers in this country.

With that, I'll yield back to the chairman.

Mr. STEARNS. We have a second panel and I thought if the members would agree that we would just quickly take about a minute, maybe, and we could wrap around and follow up with anything that is curious to you.

I'll start with the first question to the FBI. Is information from the Internet Fraud Complaint Center shared with the FTC Consumer Sentinel program? If not, why not?

Mr. KUBIC. Yes, it is. It is shared. Currently it's not shared on-line, but we'd like to move to that. Currently it's a disk and transferred in that fashion.

Mr. STEARNS. Mr. Swartz, would you comment on the convention and cyber crime and how that's coming along and what impact will it have on cyber fraud and crime enforcement?

Mr. SWARTZ. Mr. Chairman, the administration has not yet taken a position on the Council of Europe's Cyber Crime Convention, although, of course, we are deeply engaged in the negotiation process as an observer to the Council of Europe. The timeframe is that we expect by the end of this year the convention will be in its final form.

Mr. STEARNS. To the FTC and Ms. Harrington, do key interested private sector parties such as credit agencies have access to the FTC's Consumer Sentinel?

Ms. HARRINGTON. They don't now, but we would certainly be willing to work with them. There are legal issues, particularly in the agreements that we have with the Department of Justice which is a participant in Consumer Sentinel. So we would need to make some modifications to those agreements in order to permit private security agents like those of the credit card companies to have access to Sentinel, but we would be willing to work with them on that.

Mr. STEARNS. Mr. Towns?

Mr. TOWNS. Thank you very much, Mr. Chairman. Ms. Harrington, you mentioned that the FTC had limited resources to deal with the on-line problem.

How much are you actually spending now on this kind of problem?

Ms. HARRINGTON. I can get back to you with that precise information, Mr. Towns, I don't have it. But as I said, we're a small agency, about 1100 staff members. And certainly a much smaller percentage of those would be focused on consumer protection of all sorts. One of the pieces of good news that we have for you is that by using the technology itself, we get a lot more bang for our buck than we used to get, but we'll get back to you with an answer to your question, specifically, for the record.

Mr. TOWNS. A follow-up, quite often now people are talking about setting up an office within the Agency just to deal with these kind of matters. Do you have any thoughts on that?

Ms. HARRINGTON. Well, we don't think that's the right approach, at least for us. Instead, we've trained our entire Consumer Protection staff, investigators, attorneys and others. The Internet is a medium. It's not an industry. So while there are new and technology-enabled frauds that we see because of this technology, we also see a lot of frauds as all of the witnesses have acknowledged, that are migrating from the off-line world.

The point for us is to No. 1, make sure that everyone who is doing this work understands the technology, how to conduct investigations of those who use the technology, what the legal issues are that the technology poses, how to present evidence in court that is taken from the Internet, those kinds of things. And so by broadly training everyone, we think that we've had a greater impact on the problem than we would have if we sort of cordoned off a group of our people and said you do Internet only.

Mr. TOWNS. Thank you. Thank you, Mr. Chairman.

Mr. STEARNS. Mr. Bass?

Mr. BASS. Thank you, Mr. Chairman. I'll just ask one quick question. It has to do with the issue of investigations. It's my understanding that the law enforcement community's ability to investigate suspects is somewhat dependent on the suspect's method of on-line access. For example, because of the different notification laws within the Cable Act and the Telecom Act, our ability to track suspects may be limited. I was wondering if any of the four of you have a comment on this as an example, at least, in any other similar cases that you might be aware of?

Ms. HARRINGTON. Mr. Bass, I know that we've been working closely with our colleagues at the Department of Justice to take a look at some of the statutory provisions concerning electronic privacy and the way in which those might frustrate investigation and I believe that down the line there will be some thoughts shared, recommendations forthcoming from that inter-agency effort.

Mr. SWARTZ. I would add simply that it still is at the consideration stage and if I may take a moment to clarify the record on the Council of Europe Cyber Crime Convention: the administration has not taken a final position because of course, the convention itself is not final at this time and is still under development.

Mr. BASS. If no one else has any other observation, I'll yield back.

Mr. STEARNS. Ms. DeGette?

Ms. DEGETTE. Thank you, Mr. Chairman. Following up on my earlier line of questioning, I'm wondering perhaps, Mr. Kubic or Mr. Swartz, if you could tell me if there's any statistical analysis of how many cases there are that are unsolvable because of international implications on cyber crime or how much more difficult it is, given the electronic nature of the crime?

Mr. KUBIC. I'm not sure they are necessarily unsolvable. I can use the telemarketing example. Over the years, there's been a series of investigations that have been very successful at addressing that problem. In the last few years we've seen a migration of some of the con men from the U.S. to Canada and they now use Canada as a base of operations. The investigative response from the Bu-

reau's perspective was then to join with the RCMP to see what we could do to assist them. That led to a particular development of some task forces where we have agents working with the RCMP today. So——

Ms. DEGETTE. Let me stop you. I agree with you they're not unsolvable and that's not the question I'm intending to ask. What I'm asking is do we have some sense of how many we are not able to solve versus traditional types of crime and do we have any sense of the ones that are more difficult to solve, how much more difficult? Obviously, if you have folks going to Canada, you've got international implications which from a law enforcement perspective does make it more easier. I'm just wondering if we have some sense of the extent of the international implications?

Mr. KUBIC. Within the last year there are approximately 1500 complaints that we received from the Internet, at the Internet Fraud Complaint Center from foreign individuals complaining about being defrauded by U.S. fraudsters. I'd have to get back to you with some specific numbers though in terms of cases not solved.

Ms. DEGETTE. You can help Mr. Swartz with his.

Mr. SWARTZ. We'll try to respond together. Thank you.

Ms. DEGETTE. Did you have a response to the question?

Mr. SWARTZ. I can certainly expand further on the problems of international cooperation. It's something that our Office of International Affairs in the Department of Justice, Criminal Division, works constantly to improve. One of the things we've tried to encourage our law enforcement partners and other countries to do is to ensure that they have the tools in place to allow for real time investigations in cyber crime matters, for instance, which is also an important predicate for them to be able to share that information with us after they obtain it.

I'm not aware of any statistics that would let us establish with any definitive knowledge how many cases are not being solved because of international lack of cooperation, but it is certainly one of the areas we consider most important at the Department of Justice to try and push in the future.

Mr. STEARNS. Mr. Deal?

Mr. DEAL. Just very quickly. I think as all of you recognize that sometimes we are confronted with conflicting issues here in the Congress as we deal with legislative matters. Obviously, the whole discussion today deals with issues relating to privacy in one form or another, but as you're also aware this committee is constantly being asked to ratchet down in the name of protecting individual privacy, the ability to share information whether it be in the commercial sector or in other sectors.

Does the current restriction on to the name of privacy or perceived future restrictions in the name of privacy have any detrimental effect in your investigations or does the general exclusion of a criminal investigation remove that obstacle?

Are you understanding what I'm saying? I have an idea that the next panel is probably going to be more appropriately one that I ask that question to, but in the public sector now, does the right of privacy of someone who has requested information and they say I cannot reveal this because it would violate the right of privacy

of the person you're inquiring about, are those impediments that you run into now?

Mr. KUBIC. Well, obviously, we're one of the law enforcement exemptions so we regularly exchange information among ourselves without much of a concern about the privacy issue. It's criminal information that we're exchanging. It is a constant complaint that we hear from the private sector about our inability to share specific information that is not in the public record, so to speak as a result of a criminal complaint being filed. And it's an issue that we'll probably need some additional thought.

Mr. DEAL. For example, I could imagine a situation where you have the dollar amount of the fraud is smaller per individual case, and many of the victims may not have actually filed a complaint, but they are victims. And you, in the process of investigating the pattern, would need to inquire about people who may not have filed a complaint, but who nevertheless may be victims. Are the privacy rules that we currently have impediments to that investigation or does the general criminal exclusion give you enough leverage to be able to get that information?

Mr. KUBIC. I think we have enough tools to get the information that we need at this point.

Mr. DEAL. Thank you, Mr. Chairman.

Mr. STEARNS. I want to thank the participants of the first panel. We're very appreciative of your time and efforts and now we'll bring up the second panel which is Mr. Scott Charney, Principal, Digital Risk Management and Forensics, PricewaterhouseCoopers; Ms. Susan Grant, Director of the Internet Fraud Watch, National Consumers League; and Mr. Mark MacCarthy, Senior Vice President, Public Policy, Visa U.S.A. Incorporated.

I want to thank the three of you for waiting patiently and we look forward to your opening statements and we'll start from left to right with Mr. MacCarthy.

STATEMENTS OF MARK MacCARTHY, SENIOR VICE PRESIDENT, PUBLIC POLICY, VISA U.S.A. INCORPORATED; SCOTT CHARNEY, PRINCIPAL, DIGITAL RISK MANAGEMENT AND FORENSICS, PRICEWATERHOUSECOOPERS; AND SUSAN GRANT, DIRECTOR OF THE INTERNET FRAUD WATCH, NATIONAL CONSUMERS LEAGUE

Mr. MACCARTHY. Chairman Stearns, Ranking Minority Member Towns, who is no longer here, and members of the subcommittee, my name is Mark MacCarthy. I am Senior vice President for Public Policy for Visa U.S.A. and I'm pleased to be here to testify before you on this very important topic.

I should say I'm especially pleased to be here today because in the 1980's I was a staff member of the Energy and Commerce Committee working with the then chairman of the Commerce Committee, so this is a little like coming home for me.

Mr. STEARNS. Welcome.

Mr. MACCARTHY. Thank you. The Visa Payment System is the largest consumer payment system in the world. Over 1 billion Visa-branded cards are accepted at over 20 million locations to buy $1.8 trillion in goods and services worldwide. In the U.S. alone, card-

holders use Visa-branded cards for over $800 billion worth of purchases every year.

Visa is also the leading consumer e-commerce payment system in the world. Payment cards now account for 95 percent of on-line consumer transactions and Visa accounts for 53 percent of these transactions. We expect 10 percent of Visa's overall transaction volume to come from Internet purchases by the 2003, up from 2 percent today.

Some suggest that on-line commerce is lagging because people are afraid to shop on-line. But more people are shopping on-line, and we expect comfort levels to grow, as more people use this new channel of commerce. This is what happened with mail order and telephone order transactions in the past.

Consumers should be comfortable using Visa cards to shop on-line. Fraud using Visa payment cards is at an all-time low. As a percentage of our total volume, fraud has declined from 2/10ths of 1 percent in the late 1980's to a mere 7/100ths of a percent today.

And Visa has taken many steps to promote consumer confidence in this new channel of commerce, including:

A zero liability policy for unauthorized use of Visa cards.

Guidance for consumers shopping on-line.

Programs designed to help Internet merchants reduce the risk of unauthorized card use.

A tough new security program to protect cardholder data that's held in web merchant data bases.

An effective system for resolving disputes with on-line merchants through our chargeback procedures.

And steps to ensure on-line privacy protections for electronic shoppers.

Let me spend a few minutes describing some of these steps. First, Visa goes well beyond the current legal requirements to ensure that cardholders are fully protected against monetary losses due to the fraudulent use of Visa payment cards. This zero liability policy covers all Visa consumer card products, including debit and credit cards and it applies to on-line transactions, as well as off-line transactions.

Second, the fact that unauthorized transactions take place on the Internet does not mean that the Internet itself is a risky place for consumers to shop. Account information can be stolen off-line and then used for unauthorized transactions on-line.

This is why Visa and its members have developed an arsenal of fraud control programs that help merchants reduce the incidence of unauthorized use of Visa payment cards in card-not-present environment like the Internet.

Third, some consumers express concern that information they provide to on-line merchants could later be improperly accessed. To address this concern, Visa has developed new security requirements for companies holding card data—including web merchants, gateways and Internet service providers. These security requirements prescribe how companies should store, encrypt and access cardholder data and these provisions include the installation of firewalls and the encryption of stored data.

Fourth, Visa can help resolve consumer disputes with on-line merchants through our chargeback system. The three most com-

mon categories of consumer complaints handled in our chargeback system can be described as "I didn't do it," "I didn't get it" and "I don't want it." Visa rules for such complaints are designed to protect consumers. Consumers do not have to pay if they didn't purchase an item, if they didn't get the item or if it wasn't what they ordered.

Fifth, Visa has taken steps to ensure that privacy notices are posted by on-line merchants who accept Visa payment cards. Violation of consumer privacy expectations on the Internet is simply bad business, and consumers object to the unwanted dissemination of information about their on-line activities. To respond to such privacy concerns, Visa adopted new policies that require web merchants that accept Visa cards to display prominently on their websites the merchant's privacy policies and a description of their on-line security capabilities. These requirements become effective next month.

I appreciate the opportunity to appear before you today and I'd be happy to answer any questions.

[The prepared statement of Mark MacCarthy follows:]

PREPARED STATEMENT OF MARK MACCARTHY, SENIOR VICE PRESIDENT, PUBLIC POLICY, VISA U.S.A. INC.

Chairman Stearns, Ranking Minority Member Towns, and Members of the Subcommittee, my name is Mark MacCarthy, and I am Senior Vice President for Public Policy for Visa U.S.A. Inc. Thank you for the invitation to participate in this hearing on Online Fraud.

The Visa Payment System is a membership organization comprised of 21,000 financial institutions licensed to use the Visa service marks. It is the largest consumer payment system in the world. Over 1 billion Visa-branded cards are accepted at over 20 million locations worldwide. Consumers use their Visa cards to buy over $1.8 trillion in goods and services worldwide. Visa U.S.A., which is part of the Visa Payment System, is comprised of 14,000 U.S. financial institutions. U.S. customers carry about 350 million Visa-branded cards and use them to buy over $800 billion worth of goods and services annually.

Electronic commerce is vital to the U.S. economy and to the prospects for our continued economic growth. The size of electronic commerce is difficult to measure and there are gaps of tens of billions of dollars in estimates between different consulting groups. There is no doubt that electronic commerce is a large, growing and permanent new channel for the sale of goods and services to consumers. The Department of Commerce estimates, for example, that online retail sales grew from less than $5.2 billion in the fourth quarter of 1999 to almost $8.7 billion in the same quarter one year later. Sales projections for the electronic commerce market range from $35 billion to $76 billion by the year 2002. By any measure, this counts as explosive growth.

Visa is the leading consumer electronic commerce payment system in the world. Payment cards now account for some 95 percent of online consumer transactions and Visa accounts for 53 percent of the payment card portion. We expect 10 percent of Visa's overall transaction volume to come from Internet purchases by 2003, up from 2 percent today.

There are some who suggest that online commerce is lagging because people are afraid to shop online. But increasing numbers of people are shopping online, and we expect that comfort levels will grow, as more people become familiar with this new channel of commerce. This is certainly what happened with mail order and catalog and telephone order transactions in the past.

In our view, consumers should continue to feel comfortable using their Visa payment cards to shop online. Fraudulent use of Visa payment cards is at an all-time low. Fraud as a percentage of our total volume has declined over time. In the late 1980s, fraud accounted for about 0.20 percent of total Visa card volume; in the early 1990s, it was about 0.15 percent; today it's a mere 0.07 percent.

Visa has taken steps to promote consumer confidence in this new channel of commerce. These steps include:

- A zero liability policy for unauthorized use of our payment cards.

- Guidance for consumers shopping online.
- A range of programs designed to help Internet merchants reduce the risk of unauthorized card use.
- A tough new security program that went into effect on May 1, 2001 to protect cardholder data housed in web merchant databases.
- An effective system for resolving consumer disputes with online merchants through our chargeback procedures.
- Steps to insure online privacy protections for electronic shoppers.

ZERO LIABILITY

Under Federal regulations, credit card issuers are required to limit liability for unauthorized use of credit cards to $50. Visa has chosen to go beyond this requirement to ensure that cardholders are fully protected against any monetary losses due to fraudulent use of their payment cards.

In April 2000, a new Visa operating regulation went into effect that eliminates consumer liability in cases of unauthorized use of Visa payment cards. This zero liability policy covers the use of all Visa consumer card products—including debit and credit cards. As a result of this new policy, a consumer will not be held liable for unauthorized use of any Visa consumer payment card.

This zero liability policy applies to online transactions as well as offline transactions. Customers are protected online in exactly the same way as when they are using their cards at a store, ordering from a catalog by mail, or placing an order over the phone. In case of a problem, Visa provides 100 percent protection against unauthorized card use, theft, or loss. If someone steals a payment card number from one of our cardholders while the cardholder is shopping, online or offline, our customers are fully protected—they pay nothing for the thief's fraudulent activity.

We took this step in part to make sure that our cardholders know that it is safe to shop online, despite all of the recent attention to Internet security. Although card fraud numbers are very small, Visa's zero liability policy takes away risk of unauthorized use that cardholders face shopping online.

FRAUD CONTROL PROGRAMS

One type of fraud occurs when someone uses a cardholder's account number to engage in an unauthorized transaction online. For example, a person may steal a consumer's credit card number and use it to order merchandise online. The theft might occur in a variety of ways —for example, by breaking into a merchant's database that contains consumer account numbers, or by intercepting a consumer's credit card billing statement sent to the consumer's home.

It is important to keep in mind that account information can be stolen offline, and then used to engage in an unauthorized transaction online. The fact that unauthorized transactions take place on the Internet does not mean that the Internet itself is a risky place for consumers to shop. If the thief has obtained a card account number, but does not actually have the card, it is only natural for him to use this account information in a channel of commerce, such as the Internet or mail order and telephone order, in which the card does not have to be present in order for the transaction to take place. For this reason, mail order and telephone order and Internet transactions show a higher incidence of unauthorized use. The fraud rate for all Visa transactions is about 0.07 percent. For card-not-present transactions it is 0.15 percent. This, of course, does not mean that it is more risky for consumers to use these channels of commerce. It simply means that those who gain unauthorized access to card information are more likely to try to use that information to engage in fraud in a card-not-present environment.

It is in the interests of Visa, consumers, merchants, and Visa's members to prevent fraud. Fraud prevention protects merchants from absorbing the costs of fraud and protects consumers from the higher prices that they would have to pay in order to cover fraud losses. Fraud prevention further protects consumers from the trouble of having to exercise their rights in connection with unauthorized transactions. For these and other reasons, preventing fraud involving Visa credit and debit cards is a top priority for Visa and its members. Fraud prevention also is essential to protecting the integrity of the Visa brand and maintaining the confidence of consumers and merchants that use the Visa system. Through significant investments in technology, cooperative efforts between Visa, its members, and law enforcement agencies, and a wide variety of educational initiatives, the incidence of Visa-system fraud in recent years is at an all-time low, even as the volume of Visa card transactions has grown dramatically.

Visa and its member financial institutions have developed a varied arsenal of fraud control programs that help merchants reduce the incidence of unauthorized

use of Visa payment cards. These programs are especially important in addressing fraud in a card-not-present environment like the Internet. These include the Address Verification Service, Cardholder Risk Identification Service, an Exception File, Card Verification Value, and a new pilot program for Payer Authentication.

- The Address Verification Service is a fraud prevention system that allows merchants to verify automatically that a shipping address provided by a cardholder at the time of purchase matches the cardholder's billing address and other information. This service helps merchants minimize the risk that they will accept fraudulent orders from persons using stolen cardholder information.
- Visa's Cardholder Risk Identification Service ("CRIS") is a transaction scoring and reporting service that employs advanced neural network technologies to develop artificial intelligence risk-scoring models that help identify fraudulent transaction patterns. Issuers can use CRIS as a stand-alone fraud detection system or together with their own internal fraud detection methods.
- Visa's Exception File is a worldwide database of account numbers of lost/stolen cards or other cards that issuers have designated for confiscation, referral to issuers, or other special handling. All transactions routed to Visa's processing system have their account numbers checked against the Exception File.
- The Card Verification Value (CVV) is not printed on the card itself, but can be found on the card's signature strip on the back of the card. These codes help merchants confirm that cardholders are in possession of the actual card. Online merchants and other merchants in situations where the card is not present at the merchant's premises during the transaction can verify that their customers have the actual card in their possession by requesting the customer to provide the CVV from the signature strip.
- Visa's Payer Authentication service is currently a pilot program. This service will enable issuers to confirm a cardholder's identity to the merchant during the virtual (on-line) checkout process. This process will be accomplished using a password that the cardholder registers with his or her issuer. The process will help reduce fraud by enabling merchants to confirm the cardholder's identity at the time of purchase.

GUIDANCE FOR CONSUMERS SHOPPING ONLINE

Visa provides consumers with information on how to protect their cardholder information online. Visa's website, for example, provides an Internet Shopping Guide for consumers, with suggestions for how consumers can shop safely on the Internet. Some of these suggestions are:

- Shop with merchants you know and trust and visit Better Business Bureau Online if you have questions about a particular merchant.
- Look for signs of security. Symbols like an unbroken lock or key, a URL that begins https://, or the words Secure Sockets Layer (SSL) mean that no one but you and the merchant can view your payment information.
- Never send payment information via e-mail. Information that travels over the Internet (like e-mail) is not fully protected from being read by outside parties.
- Shop with reputable merchant sites that use encryption technologies that will protect your private data from being read by others as you conduct an online transaction. When you pay online, make sure that you are using a secure browser.
- Make a point of reading a merchant's privacy policy to find out what type of information is captured and how it is used.

SECURITY REQUIREMENTS FOR CARDHOLDER DATA

Some consumers express concern that the account information they provide to merchants during online transactions might be subject to unauthorized access after the transaction is complete. The account information might be transmitted to web merchants in a secure fashion, but not maintained securely in the web merchant's database. Reports of intrusion by hackers into web merchant databases have increased this concern. It should be noted, however, that the security of merchant databases of account numbers is not related to whether a transaction is conducted over the Internet, rather it is related to the accessibility of the database from the Internet.

To address this concern about unauthorized access to merchant databases, Visa has developed new security requirements for cardholder data. These requirements apply to any entity holding card data—including web merchants, gateways and Internet service providers. These requirements prescribe how these companies should store, encrypt and grant access to cardholder data. For example, they require Internet merchants to install firewalls, to keep security systems up-to-date, to

encrypt stored data, and to use anti-virus software, among other things. These requirements became effective May 1, 2001.

Visa offers assistance to Internet merchants that accept Visa cards in meeting these requirements for safeguarding their customers' payment card data. We provide merchants with training sessions, interactive reviews, compliance and monitoring consultation and information on third-party firms specializing in testing and compliance.

The new program requires the top 100 e-commerce merchants—who account for 70 percent of Internet commerce in the Visa system—to have their online security procedures validated by an outside accounting or Internet security firm. Other online retailers will be subject to random security reviews by Visa.

The twelve requirements of the new security program are: Install and maintain a working network firewall to protect data accessible via the Internet. Keep security patches up-to-date. Encrypt stored data. Encrypt data sent across open networks. Use and regularly update anti-virus software. Restrict access to data by business "need-to-know." Assign a unique ID to each person with computer access to data. Do not use vendor-supplied defaults for system passwords and other security parameters. Track access to data by a unique ID. Regularly test security systems and processes. Maintain a policy that addresses information security for employees and contractors. Restrict physical access to cardholder information.

DISPUTE RESOLUTION

Visa has an effective way of resolving consumer disputes with online merchants through our chargeback system. Chargebacks are contractual ways of resolving transaction disputes involving payment cards between the Visa banks that serve cardholders (the issuers) and the Visa banks that serve merchants (the acquirers). A chargeback is the return of a transaction from the issuer to the acquirer. Our chargeback system can resolve transaction disputes, even if the merchant and the consumer are geographically dispersed. As a result, Visa's chargeback process provides practical and effective consumer protections for electronic commerce transactions.

Most chargebacks in the Visa system are for housekeeping reasons. In a system that handles 25.5 billion transactions a year, mistakes are bound to occur. These can include double billing, no billing, incorrectly entered amounts, failure to provide requested copies of transactions, mismatches among accounts and so forth. These errors constitute the vast majority of chargebacks.

In addition to these housekeeping chargebacks, there are chargebacks involving consumer complaints. The three most common categories of Internet consumer complaints handled in our chargeback system can be described by the phrases: "I didn't do it," "I didn't get it" and "I don't want it." Visa rules with respect to these complaints are designed to protect cardholders. Cardholders do not have to pay if they did not make the purchase, if they did not get what they ordered or if it was not what they ordered.

The "I didn't do it" dispute relates to situations where the cardholder claims that the transaction was processed without the cardholder's permission. This is the most common category of Internet disputes. It covers fraud, but it also covers situations where the cardholder does not recognize the charge as it appears on the monthly bill. Confusion often can arise when the merchant uses a different billing name or address than the expected trade name. About 50-60 percent of these disputes are resolved by giving the cardholder additional information about the charge.

The "I didn't get it" category of consumer complaint covers untimely receipt or non-receipt for goods. This dispute involves situations where a cardholder claims that he or she did not receive ordered merchandise at the agreed-upon location or by the agreed delivery date. An issuer can charge back a transaction on the cardholder's behalf if the cardholder sends a letter to the issuer supporting his or her claim. Proof of shipment by the merchant is irrelevant; the Visa member acquiring the transaction can only counter the chargeback on the merchant's behalf by providing proof of delivery, signed by the cardholder or another authorized person.

The "I don[t want it" category of Internet disputes includes "quality" disputes, such as when merchandise is received broken, not as ordered (e.g., wrong color or size) or not as described. It is the most difficult type of dispute to deal with because value judgments are involved.

Only a tiny percentage of all Visa transactions are charged back, about 0.07 percent or 7 for every 10,000 transactions. Chargebacks for Internet transactions also are a small portion of all Internet transactions. Even though chargebacks are rare occurrences, they are more common for Internet transactions than for other types of transactions. However, it is difficult for us to say how much more common. Mer-

chants are supposed to report their Internet transactions to the Visa system using an E-commerce code. Not every merchant that operates both in the Internet and the "real" world—the so-called "bricks and clicks" merchants—report and break down their sales by channel. So the statistics available are not as comprehensive as we would like. That being said, the Visa chargeback rate for Internet transactions is estimated to be about 0.5 percent. Put another way, only about 50 out of every 10,000 electronic commerce transactions are charged back.

There are a number of reasons for this. The Internet is a new channel, much the way mail order and telephone order transactions were new a decade ago. Not all merchants have developed the back office and customer service facilities that consumers have come to expect, and those consumers use the Visa chargeback system to help them resolve their problems with merchants.

In addition, the Internet is a channel of commerce, in which, like mail order and telephone order, the card is not presented to the merchant when the transaction takes place. This naturally creates greater opportunity for unauthorized use of card account information. In this regard it is useful to note that chargebacks for mail order and telephone order transactions are 0.39 percent, or 39 per 10,000 transactions. The fact that there is greater use of chargebacks for payment cards used on the Internet or through mail order or telephone order does not mean that these channels of commerce are inherently more risky for consumers.

Other factors contribute to the higher chargeback rate for Internet transactions. Cardholders are doing business with unfamiliar merchants, or with individuals at auction sites. In some cases, these merchants or individuals are unscrupulous. In other cases, cardholders deny valid charges. In addition, digital goods present some special difficulties. Some digital good subscriptions require the use of a payment card account number for access and this sometimes results in customer confusion on the nature of the subscription terms and payments. Buying and delivering digital goods like software and music can be difficult on the Internet. For example, the Internet connection may be lost during long downloads. Or a cardholder might repeatedly hit the buy button on a site when the link does not respond quickly.

The Visa chargeback system operates in compliance with federal laws that provide a number of important consumer protections. The Truth in Lending Act, implemented through Regulation Z, gives cardholders various rights regarding billing error resolutions. And it allows the cardholder to assert claims and defenses against the card issuer. The Electronic Funds Transfer Act, implemented under Regulation E, applies to debit cards and also contains error resolution procedures. These legal protections apply to online transactions as well as to face-to-face transactions.

These legal protections are just the start of the consumer's protection. There are more protections that are provided voluntarily by competing payment systems. And there can be even more protections provided within systems, bank-by-bank, to meet the needs of cardholders. The payment card business is intensely competitive, with all competitors seeking to gain the business and loyalty of cardholders. Banks are extremely interested in having satisfied customers, as are merchants. Each will do what they can to continue customer relationships. In fact, a joint venture system, like Visa, enhances competition generally because it provides for bank-to-bank competition as well as system competition.

Visa also works with cardholders, merchants, consumer groups and seal programs to avoid consumer disputes in the first place. One important relationship we have established is with the online subsidiary of the Better Business Bureau, BBB Online. BBB Online has developed a comprehensive Code of Online Business Practices and a first-rate Reliability Trustmark Program. The code outlines the responsibilities of online merchants in five key areas: truthful and accurate communications, disclosure of policies, information practices and security, customer satisfaction and protecting children. Their Reliability Trustmark Program is one of the most significant trustmark programs on the web, providing more than 8,800 websites with a seal to signify to potential customers the merchant's commitment to good customer practices. The seal provides consumers navigating the electronic marketplace with a reassuring sign from a well-regarded and well-known organization, the Better Business Bureau.

On November 14, 2000, Visa joined forces with BBB and agreed to promote its Code of Online Business Practices and its Reliability Trustmark Program. This includes a consumer advertising and a consumer education campaign. Many websites that provide excellent customer service and protections are not part of the BBB Online program. But online consumers can be confident that online sites displaying the BBB Online reliability seal have the highest level of consumer protection.

Visa also maintains a chargeback-monitoring program. This program monitors a merchant's chargeback rate. If this rate exceeds certain levels, Visa asks the merchant's bank to ensure that the merchant takes steps to correct the problem. Usu-

ally, the problem is technical and is fixed immediately. In cases where the chargeback rate does not decline, Visa has a process of assessing fines. A merchant that does not correct a persistent chargeback problem can ultimately be denied the right to accept Visa payment cards for goods and services.

PRIVACY PROTECTIONS

Visa has taken steps to ensure that privacy notices are provided by merchants who accept Visa payment cards to consumers who shop online. Violation of consumer privacy expectations on the Internet is simply bad business, and consumers are right to be upset about the unwanted dissemination of information about their online activities. To respond to privacy concerns, in October 2000, the Visa International Board adopted new consumer protection policies that set global disclosure standards for web merchants. The new policies require web merchants that accept Visa cards to display prominently on their websites the merchant's privacy policy and online security capabilities. These requirements become effective on June 1, 2001.

Merchant banks must update their merchant agreements to include these requirements no later than January 1, 2002. Banks may satisfy this requirement by mailing a disclosure addendum to each of their electronic commerce merchants. Many electronic commerce merchants already disclose this information. However, Visa and its member banks provide guidance to electronic commerce merchants that need assistance in meeting the privacy policy requirement. For instance, we encourage merchants to use the Privacy Policy Statement Generator developed by the Organization for Economic Co-operation and Development.

Visa also has taken other steps to help consumers protect their privacy online. Our website contains an extensive consumer guide to online privacy protection. In addition, we participate in pro-privacy industry organizations such as the Privacy Leadership Initiative, a group of major corporations and associations, dedicated to promoting privacy on the part of U.S. business and educating consumers about ways in which they can protect their privacy.

Finally, Visa has provided extensive legal and regulatory guidance to our member banks to ensure that the mandated online and offline privacy protections of the Financial Modernization Act of 1999 are fully implemented. Financial institutions must be in compliance with the privacy provisions of this law by July 1, 2001. These rules generally require financial institutions to disclose their privacy policies at least annually and to provide their customers with the opportunity to opt-out of certain information sharing practices with third parties. These Federal privacy rules apply to information collected on websites in connection with providing a financial product or service. Financial services websites now must comply with notice and opt-out requirements.

Visa appreciates the opportunity to appear before you today. We believe that our payment system represents a reliable and secure means of conducting online transactions in which the rights of consumers are well protected. Visa will continue to adapt to new technologies and practices. Combating fraud and maintaining information security are top priorities of Visa and its member financial institutions.

I will be happy to answer any questions that you may have.

Mr. STEARNS. Mr. Charney?

STATEMENT OF SCOTT CHARNEY

Mr. CHARNEY. Thank you, Mr. Chairman. It's a pleasure to be here. The subcommittee asks, "Are consumers safe," and I think the answer is not safe enough and not yet. And the reason for that are several factors. First is the origins of the Internet, built as a military communication system, it had a trusted group of users and crime wasn't a problem. Then in the early 1890's, IBM introduced the PC, the government decides the Internet should be a public resource and suddenly everyone is on the Internet and it has no embedded security. And as a result of that we've seen a rise in both cyber fraud and cyber crime and conceptually, these are really different, but overlapping terms. Cyber crime generally refers to attacks against the confidentiality, integrity and availability of computer networks and systems. Cyber fraud cases are usually cases where the Internet is used as a tool to facilitate some sort of fraud-

ulent activity. And in those cases, very often the Internet is being used as a communications device to reach out to consumers with fraudulent, deceptive information to encourage consumers to part with personal information, credit card information and the like.

So cyber fraud and cyber crime are problems and they're real challenges and here's why. First, of all there's a lack of authentication on the Internet. It's hard to know who you're dealing with. That is one of the reasons I think, Mr. Bass, there was a discussion about using Social Security Numbers because it is a unique identifier. The difficulty is, as they become broadly used, they're no longer secret, shared secret identifiers, but they're in the public domain and they're value for authentication drops.

Second, the Internet has a lack of traceability. There are no real tracing tools built into the Internet and there are values in that in that it protects privacy and confidentiality and anonymity. At the same point, it allows criminals to act in the belief sometimes real, sometimes false, but their activities cannot be traced back to their source. Therefore, because of the perceived lack of traceability very often criminals feel more emboldened to engage in criminal activity.

The third problem, of course, is globalization, because the Internet is global there is far more criminal activity that is committed across national borders, and while criminals do not worry about passing borders, law enforcements and governments certainly do have to worry about investigations that havve an impact upon the sovereignty of other countries. In my 9 years as chief of the Computer Crime and Intellectual Property Section, I also chaired the G-8 subgroup on high tech crime that was a discussion of the former panel and clearly, countries are worried about how to protect their sovereignty at the same time that they assist in international investigations.

The next problem with the Internet is that its mixed use. It's part commerce, part speech, part political speech and because the Internet is used in many different ways, it is very hard to build regimes that can protect people on the Internet without possibly infringing on constitutionally protected rights. You see that, for example, in the Supreme Court decisions on the Communication Decency Act and the Third Circuit Decision on COPA, Children's On-Line Protection Act.

The other real challenge is how to get security into the network. The truth of the matter is that if you look at the General Accounting Reports on government security and all the cyber crime reports from the private sector, security is not where it should be. Part of the problem is how to fund that security. Many of my clients which are large companies, they want to use technology to increase efficiency, increase the bottom line, but security is a cost and because it's a cost it's hard to allocate resources to employing security. In fact, a Joint Security Commission Report of the Defense Department and CIA in 1996 said 10 to 15 percent of every information technology dollar should be spent on security, more probably 5 percent today.

So what are the solutions? Well, the first is the market. As consumers have gotten more concerned about cyber crime and more concerned about their privacy, the markets are responding with

better security, in particular, things like firewalls, virtual private networks and the use of encryption and Visa's response is a classic example to responding to those markets.

Second, regulation, at times will affect security in dramatic ways. The HICFA regulations on privacy and security will force health care providers to deploy far more security than they are today. And then finally, of course, is education, that is the public has to appreciate that on the Internet, like in the real world, if you see a deal that's too good to be true, it probably is. We often tell consumers that they should do business with companies they know and trust and that's one way to ensure that the relationship will be reliable. The difficulty with that is the Internet web business model is a low barrier to entry, anyone can open up a business on the Internet. So we're giving a little bit of a mixed message if we say only deal with businesses you know, but the beauty of this technology is anyone can start a business, even if it doesn't have a track record.

So there are some real challenges, but there are some solutions. Thank you.

[The prepared statement of Scott Charney follows:]

PREPARED STATEMENT OF SCOTT CHARNEY, PARTNER, PRICEWATERHOUSECOOPERS LLP

I would like to thank the Committee for inviting me to speak on the topic: "On-line Fraud and Crime: Are Consumers Safe?"

That question is admittedly difficult to answer. To begin with, safety—whether on the Internet or in the physical world—is never absolute. Clearly the Internet does affect the types of threats consumers face, and with mixed results. For example, there is no question that on-line banking substantially reduces the risk that one will be robbed at gunpoint after cashing a check at a bank branch but, at the same time, it increases the risk of white-collar hackers emptying customer accounts from remote locations. Rationally one might assume that consumers would approve of the trade-off. Yet the fear of a hacking incident (or put another way, lack of customer trust in technology) remains somewhat of an impediment to the growth of on-line banking.[1] Similarly, I have met many individuals who refuse to use their credit card over the Internet, expressing the fear that their credit card number will be intercepted. In reality, however, it is extremely difficult to intercept such data in transmission. Moreover, those same individuals will often admit to handing their credit card to a waiter they do not know, and blissfully drink their coffee while the waiter takes the credit card out of view. To some extent, therefore, it is perceived safety, more than actual safety, that may govern consumer habits on the Internet.

Second, it must be remembered that Internet safety, like technology, is not a constant. At the same time regulatory and market forces are doing much to improve consumer safety, technological changes pose new risks. For example, while better computer security, including the increased use of encryption, plays an important role in protecting consumers, new technologies such as broadband are putting home computers at greater risk. This is significant for several reasons, not the least of which is that consumers store sensitive personal data on their home machines, and they may also use those computers to access corporate networks, thus creating a vulnerable "weak link" between a hacker and corporate America.

So if I were to answer the question "Are Consumers Safe?", my answer would be "yes, but we clearly can do more." We can start by better authenticating both businesses and consumers in commercial transactions, and better protecting the confidentiality of data.

There is a now-famous cartoon of a dog, sitting before a computer terminal, who turns to another dog and says, "On the Internet, nobody knows you're a dog." One of the key changes that the Internet has brought about is the creation of customer accounts and other business transactions without the personal interaction that was

[1] Research conducted by the Banking Industry Technology Secretariat (BITS) Research and Communications Steering Committee found that consumers' anxieties about security are more acute in the "new and intangible cyberworld" than in the physical world and that these anxieties have caused consumers to proceed with caution. See "Consumers' Attitudes about Security, Privacy and Trust," BITS Research and Communications Steering Committee, April 4, 1998.

traditionally an essential part of such relationships. Although telephone calls have long been the basis for the establishment of certain business relationships without any face-to-face contact, the Internet allows for transactions with even less personal interaction between businesses and consumers.

Merchants, whether in the real world or cyber world, have always faced the challenge of authenticating their customers. In many cases—at least outside of small towns where everyone knows each other through face recognition—a merchant's success depends on his ability to sell to—and collect money from—people he or she does not know. In cash and carry transactions, the anonymity of the buyer is no problem, as the merchant is paid before the product leaves the store. In other types of transactions, such as check payments and credit cards, there needs to be trust since receiving actual payment is deferred in time.[2] In these situations, allowing a buyer to remain anonymous increases the risk of fraud (anonymous buyers do not fear being held accountable for payment), and may leave the merchant holding the bag (unless, of course, contract rules shift the loss to another party, such as a card issuing bank or an insurance company).

For these reasons, merchants have always looked for ways to prove a buyer's identity.[3] In short, there are three formulas for authenticating an unknown buyer's identity: something the buyer is, something the buyer has, or something the buyer knows. These different metrics are often combined in some way.

"Something the buyer is" refers to biometrics. In face-to-face transactions, many biometrics are available. The most common biometric is the signature, and merchants will often have a buyer sign some document (e.g., a check or charge slip). The advantage of a signature is its uniqueness, permanence, and evidentiary value (compare this to eye witness testimony of face recognition which is neither unique nor permanent, and of weak evidentiary value due to claims of mistaken identification).

"Something the buyer has" refers to something in the possession of the buyer. For identification purposes, it is common to require a driver's license or other government identification (e.g., passport), documents that have a high degree of reliability because an independent authority (the government) has assumed responsibility for verifying the identity of the person to whom it has issued the document. In business transactions, the "something the buyer has" is today most often a credit card. Although it is of course possible to manufacture such cards without authority, most common fraudsters have neither the means nor inclination to mass produce plastic cards, although there are certainly organized groups that do so. In any event, in face-to-face transactions, it is possible to use both "something the buyer is" and "something the buyer has," and that is frequently done. For example, a merchant will ensure that the customer both has the credit card ("something the buyer has") and that his signature matches the signature on the back of the card ("something the buyer is"). Another example: some credit cards come with photos, thus combining something the buyer has (the credit card) with something the buyer is (the facial appearance).

The problem is that these techniques do not work well in telephonic and electronic environments where neither physical characteristics nor personal possessions can be checked. Although both biometrics ("something the buyer is") and possessions ("something the buyer has") can be implemented electronically, the cost is substantial. Whether using biometrics or credit card readers, these techniques generally require the distribution of specialized hardware/software (e.g., fingerprint readers, credit card readers) and are often unworkable due to the difficulty of and cost of distributing such equipment in the business-to-consumer model.

Recognizing the impracticability of authenticating electronic and telephonic transactions using biometrics and possessions, merchants have relied upon the third type of authentication: "something the buyer knows," often referred to as a "shared secret." In some cases, this secret can be created by the consumer and merchant together. For example, the first time a customer does business with a website, the

---

[2] Who accepts the risk of loss is a separate question. For example, in a face-to-face transaction, a merchant may collect on a credit card payment even though the charge is later deemed fraudulent, so long as the merchant took certain steps to validate the card. In such cases, the bank issuing the card suffers the loss. By contrast, in MOTO transactions (Mail Order/Telephone Order), the merchant will suffer the loss, as the card is not present at the time of sale. Internet transactions are, not surprisingly, considered card-not-present transactions.

[3] It is important to note that authenticating users is important for reasons other than commercial transactions. In today's electronic environment, there is a strong need to be able to authenticate the sender and/or recipient of a message, in large part to protect the confidentiality of that message from improper prying eyes. If communications, particularly e-mails containing sensitive personal or corporate information, can be opened by someone other than the intended recipient, the end result may be a significant invasion of privacy or loss of proprietary information.

merchant may ask the consumer to create a password for future access. This "shared secret" is thereafter known only to the merchant and that consumer, at least if neither party discloses it to, nor has it stolen by, a third party. Even the proper use of this shared secret in future transactions only proves, of course, that the person signing on the second time is the same one who signed on the first time, but it does not prove that the customer, who has now signed on twice, is who he claims to be. Put another way, a fraudster who signs on to a site and creates a password will have a shared secret for his second visit, but he is still a fraudster.

More commonly, both merchants and consumers rely upon a third party to verify the secret. For example, if a consumer is purchasing goods with a credit card, he may also be asked to provide his home address as a shared secret; this is information that the merchant can have verified by a third party (e.g., a credit reporting agency). The problem with such shared secrets, however, is that they are often too broadly shared to be called a "secret" at all. Even worse, the secret may in fact be stored with the very information that the secret is designed to protect. Since a credit report may contain a credit card number and the buyer's home address, anyone who accesses the credit report also gains possession of the shared secret (the home address), thus defeating the entire scheme. Suffice to say, from an e-commerce perspective, authentication will remain a critical issue, at least in business to consumer (B2C) transactions.

The Internet certainly exacerbates such authentication issues for a host of reasons. On the civil side, differences in legal rules across international jurisdictions also may pose a significant impediment to both authenticating and protecting consumers. How can a retailer physically located in Australia authenticate a buyer claiming to be a European citizen browsing its website in the middle of the night from a location somewhere in Asia? And which set of regulatory rules should be applied to such transactions? Finally, if the transaction at issue turns out to be unsatisfactory, to which legal systems should the business or consumer turn for assistance, and is there any practical cost-effective way to vindicate one's rights?[4] One current consumer-oriented proposal—the Hague Convention—would allow consumers to sue in their home nation, thus requiring even the smallest website owner to defend suit in every jurisdiction from which an Internet user makes a purchase.

On the criminal side, fraudsters have continued to use the Internet's lack of authentication to facilitate illegal schemes. One bank, for example, reported a fraud scheme that illustrates the authentication issue from both the consumer and financial institution perspectives. After several of the bank's customers contacted the bank concerning the status of the credit card they had ordered online, the bank reported a false advertising Internet scam. The perpetrator utilized the bank's name to lure victims to a fraudulent web site and charged victims $99.00 for a guaranteed Visa or Master Card. To facilitate payment of the $99.00 fee, the fraudulent web site allowed the customers to provide their checking account information directly online, thus allowing the perpetrator to direct the withdrawal of funds from the victim customers' accounts. The customers also had the option to send checks to a mailbox address for deposit. An investigation by the United States Secret Service and the bank's corporate security department revealed nearly $300,000.00 was deposited into the perpetrator's account in a 30-day period.

That fraud may be facilitated by the Internet is of course no surprise, but in considering consumer safety we must remember to add two other Internet attributes: scalability and globalization. It is not just the risk of an event that matters, but the size of the event, and the Internet presents a platform for large-scale abuses that are generally not practical in the physical world. In short, large scale abuses can occur at anytime and anywhere, and can be committed by anyone in the world with Internet connectivity. For example, a hacker can breach network security and simultaneously breach the confidentiality and privacy of thousands of customer records in real time. This radical change occurs because of the way data is consolidated and thereby made accessible, distributable, and usable. By way of contrast, ten years ago a fraudster working at a busy restaurant or bar might have been able to steal at most dozens or even hundreds of credit card numbers on a good night and would have been hard pressed to make use of all those numbers quickly. Today, with Internet merchants allowing credit card purchases twenty-four hours a day for everything from major home appliances to groceries, thousands of credit card numbers may be quickly consolidated on a single computer. Those numbers can then be stolen en masse, and quickly used. Moreover, such credit data may be combined with other personal information, thus making identify theft a real risk.

---

[4] *See, e.g.,* the Hague's Preliminary Draft Convention On Jurisdiction And Foreign Judgments In Civil And Commercial Matters, Article VII (allowing consumers to bring causes of action against merchants in the forum in which the consumer is habitually resident).

Equally problematic is that global connectivity allows hackers to access those numbers and distribute them, again globally, within minutes. Hackers are not hampered by the existence of international boundaries because property need not be physically carried, but can be shipped covertly via telephone and data networks. A hacker needs no passport and passes no checkpoints, thus eliminating any hope of interdiction by customs authorities. And while hackers "roam" freely, law enforcement should and must respect national boundaries.

There are things being done, however, by both industry and the government, to help reduce these risks. VISA, for example, has promulgated requirements that merchants encrypt credit card data not just in transmission, but in storage. AMEX is relying upon smart card technology to better authenticate users, and has introduced another technology which permits a member to use his or her credit card without the actual card number being passed to the end merchant. This technique limits the distribution of the actual card number, thus reducing the risk of fraud. As for the government, in addition to fulfilling its traditional responsibility to react to crime when it occurs, it has been working proactively in several international fora to ensure that computer crime issues are addressed. For example, at the G8, nations have agreed that certain computer abuse must be criminalized, and that each country must designate a high-tech point of contact, available 24 hours-a-day and 7 days-a-week, to respond quickly to computer related crimes. A draft cybercrime treaty at the Council of Europe would expand the scope of these agreements to a larger group of nations. Although there is still a long way to go, such efforts—by both markets and governments—have served to make the Internet safer.

Mr. STEARNS. Ms. Grant.

STATEMENT OF SUSAN GRANT

Ms. GRANT. Thank you for asking the National Consumers League to participate today. Though we were founded in 1899, long before the Internet was born, we've kept up with cutting edge issues such as electronic commerce. Internet fraud is really the dark side of electronic commerce and anybody who goes on-line is a potential victim.

We have submitted written testimony which we would appreciate being entered into the record.

Mr. STEARNS. By unanimous consent, so ordered.

Ms. GRANT. And that describes in detail the consumer and law enforcement services that we provide really as a public service from a nonprofit organization. But I just want to highlight the importance of the two roles that we play. One is fraud prevention. Our trained counselors help consumers identify the red flags of fraud and prevent victimization and that's really crucial because as any law enforcement agency will tell you, although they may be able to take action against the bad guys, getting people's money back is often difficult or impossible.

And then the second really important thing that we do is notify law enforcement agencies quickly about crooks and their victims. We do that through an ingenious computer system which was actually the inspiration for the FBI's Internet Fraud Complaint Center.

It may sound as though we're competing with each other, private organizations and government agencies, but we're not. There's plenty of fraud to go around. We all play an important role. I think that in many instances consumers come to us because we're a trusted source of information and also because they're confused about what government agencies to go to. We can help them by getting our information to all the right agencies.

We've learned a lot about Internet fraud over the years and in our written testimony we've described to you the consumers who are victimized and how they're victimized. Younger people tend to

be more often on-line fraud victims than older, but nobody is immune. People are losing more and more money every year.

The victims tend to come from the States where most people live, California, Florida, Texas and New York top the list and that's also where many of the cyber crooks are, but we're seeing growing numbers of cyber crooks from other countries and this is a big challenge for law enforcement agencies as we've already heard.

We're also seeing more use of credit cards as a payment in what turned out to be fraudulent Internet transactions. From our standpoint, that's a good thing. We actually urge consumers to pay with credit cards because of the strong legal dispute rights if somebody uses their card number without authorization, if they don't get anything or if what they get was misrepresented.

We are concerned, however, about some new forms of payment from debit cards to demand drafts from people's bank accounts to things like cyber wallets and other means of payment that are not—that don't afford consumers the same protection as the laws that we have concerning credit cards.

I would like to really focus my remaining time on the solutions which I know you're most interested in. And as we said in our written testimony, we think the first thing we need to do is set some basic rules for e-commerce, similar to the way that we did in enacting the law and the telemarketing sales rule promulgated under it which sets a code of conduct for telemarketers. We need a code of conduct for e-tailers that requires certain disclosures and prohibits certain practices. We have a model to look at in the Consumer Protection, in the context of electronic commerce guidelines which were issued in December 1999 by the Organization for Economic Cooperation and Development. We should take steps to implement those guidelines.

We should also enact uniform protection for different forms of electronic payment so that consumers have the same dispute rights and also to hold the e-tailers feet to the fire. After all, if there are complaints against vendors for what appears to be fraud and misrepresentation, they can lose their ability to continue to participate in the electronic payment system and that's a very important tool.

We need, as we heard earlier today, to provide more resources to law enforcement agencies to fight Internet fraud. We'd also like more resources from the government. We, for instance, a couple of years ago received a grant from the Department of Justice which helped us improve the law enforcement services that we provide and we would appreciate more funding to continue those services and we also need funding for consumer education. This is an ongoing need. We all share the responsibility in it. We've done a lot of work with private sector partners and we would welcome government grants to do that work as well.

[The prepared statement of Susan Grant follows:]

PREPARED STATEMENT OF SUSAN GRANT, DIRECTOR, INTERNET FRAUD WATCH, NATIONAL CONSUMERS LEAGUE

Thank you very much for inviting me to speak to you today. Though the National Consumers League was founded more than one hundred years ago to advance the economic and social interests of consumers, long before the Internet was born, we have kept on the cutting edge of issues such as electronic commerce. Internet fraud

is the dark side of electronic commerce, and anyone who goes online is a potential victim.

Our involvement in fighting Internet fraud has its roots in the National Fraud Information Center, a program that NCL set up in 1992 as the first nationwide toll-free hotline to assist consumers with questions or problems concerning telemarketing fraud. In 1996, as many of the same scams that we saw in telemarketing began to appear in cyberspace, we created a companion program, the Internet Fraud Watch, and a Web site, www.fraud.org. These programs perform two very important functions.

Fraud Prevention

The first is fraud prevention. More than half of the 1,000-1,200 consumers who contact us by phone or via the Web site each week have not yet been victimized. They are doing exactly what we want all consumers to do—checking out offers that sound enticing but may not be legitimate. Our trained counselors help consumers identify the "red flags of fraud," such as sweepstakes winnings that require payment to claim, unrealistic promises of big returns on investments with little or no risk, easy ways to earn money with little or no work, and guaranteed credit even for those with bad credit histories. It is crucial to prevent victimization whenever possible because, as those in law enforcement will tell you, chances of actually recovering money from crooks are usually fairly low. We reinforce the advice that our counselors provide by sending everyone who contacts us educational materials, by mail or email, on the specific types of scams about which they inquired.

Alerting Law Enforcement Agencies Quickly

The second vital function of our fraud programs is to alert law enforcement agencies quickly about con artists and their victims. We transmit the information that consumers have provided to us by phone or via the online form on the Web site to the appropriate federal, state and local law enforcement agencies, alerting them to scams about which they may not already know and to people who need their help.

Agencies tell us in advance what they wish to receive by certain criteria, such as geographic location, type of scam, or other factors. For example, the Florida Attorney General's Office wants complaints where either the consumer or the perpetrator is in that state. The Securities and Exchange Commission receives information about investment-related scams. The Postal Inspection Service is interested in cases where the payment was sent by mail. Our FAST Alert System matches the information that our counselors take from consumers with the agencies' criteria and automatically relays those complaints by fax or email. We also send agencies a daily log showing them what other agencies have received the same fraud reports and the contact information so that investigators and prosecutors can coordinate their activities. To date there are more than 230 agencies on our system.

Since it is not uncommon for one complaint to be of interest to several agencies, we save consumers the trouble of having to contact each directly. We also upload new complaints on a weekly basis to the Consumer Sentinel database, which is maintained by the Federal Trade Commission and the National Association of Attorneys General. Law enforcement agencies can query Consumer Sentinel to find information that aids in their investigations and prosecutions.

The Worst Internet Scams

What is the worst scam on the Internet? That depends on how you look at it. In terms of volume, it's online auction fraud. As a survey that we recently conducted shows, most sellers are honest, and most buyers are happy with their experiences. But there are some individuals and companies who offer items on online auctions that they don't really have or that don't remotely resemble the descriptions they provide. Last year, 78% of the Internet fraud complaints we received were about online auction transactions. The good news is that this is down from 87% the year before, but it is still a significant concern. Whenever consumers pay in advance for items they haven't seen, there is an element of risk. We launched a public education campaign earlier this year to tell consumers how they can protect themselves in online auctions.

We have attached to our testimony the list of the top ten Internet frauds of 2000, and that information is on the Web site at www.fraud.org/internet.It00totstats.htm. The Web site also provides basic Internet tips and specific tips on common Internet scams. More than 300,000 people visit our Web site every week. Some Internet scams are the same as we see in telemarketing fraud; for example, work-at-home schemes, advance fee loans, bogus offers of credit cards, and empty promises of free or cheap trips. Others are specifically Internet-related. Online auctions are a phenomenon made possible by this new interactive medium. Other frequent complaints are about offers for Internet services and sales of computer equipment and software.

Based on the amount of money that victims lose, Nigerian money offers are the worst Internet scam. These offers, which used to come by airmail but now are increasingly arriving by email, promise millions of dollars in exchange for allowing your bank account to be used to safeguard someone else's riches. But the real intent is to take money out of your account, not put money in it. These scams rose to the top ten Internet frauds last year, and victims are losing an average of $3,000 in money they've paid or that was taken from their bank accounts. Another category with high dollar losses is travel scams, an average of $1,464 per victim last year. Overall, the average loss to Internet fraud was $427 in 2000, up from $310 in 1999.

Victims of Internet Fraud

The biggest losers to Internet fraud are people in their 20s, 30s and 40s, who represented 77% of the victims we heard from last year. Among the top ten frauds, the most young victims are found in the advance fee loan category, the most older victims in bogus credit card offers. But no one is exempt; there is a scam for everyone. The states with the most people are where the most victims are located: California, Florida, New York, and Texas.

Those states are also the top locations for cybercrooks. But since the Internet has no geographic boundaries, neither do the con artists. Nearly 4% of the Internet scams reported to us last year originated from Canada, a little more than 2 % from other countries, and offshore fraud is growing.

Because we hear from so many online auction victims, the most common method of solicitation is through Web sites. But 12% of the victims were solicited through emails last year, up from 9% in 1999, and 4% were solicited through newsgroups, a sharp increase from 1% last year. Consumers have to be wary no matter where they go on the Internet. A friendly tip from someone in a newsgroup can actually be a trap set by a fraudster.

Since many online auction transactions are completed with the high bidder sending payment offline to the seller, the most frequent methods of payment are money order and check. But more consumers are paying for fraudulent online transactions by credit card, 11% last year compared to 5% in 1999. We advise consumers to pay by credit card because of the strong legal dispute rights they have for unauthorized charges, nondelivery or misrepresentation. However, we are beginning to see payments made with debit cards or by demand drafts from consumers' bank accounts, and the legal dispute rights in those cases are not as strong. This is a concern, especially as new forms of electronic payment such as cyberwallets are developed.

Making the Internet Safer for Consumers

There are several things that should be done to make the Internet a safer place for consumers and enable e-commerce to achieve its full potential:

- Set some basic rules for e-commerce. Five years ago, the federal Telemarketing Sales Rule was promulgated by the FTC to require certain disclosures and prohibit specific practices. States are empowered to help enforce the rules in federal court. In December of 1999, the Organization for Economic Cooperation and Development issued Guidelines for Consumer Protection in the Context of Electronic Commerce, which provide suggestions to the member countries for how e-commerce should be conducted. The United States played a major role in drafting the guidelines. Now we should implement them by setting some basic rules for e-tailors, such as requiring that they provide their physical addresses, and prohibiting practices that should be illegal on their face, such as advance fee loan offers from entities that are not regulated financial institutions.
- Enact online privacy protection. Consumers should have legal protections against commercial email that they never agreed to get and having their personal information shared by companies to whom they provide it without their permission.
- Enact uniform protection for different forms of electronic payment. To encourage e-commerce, debit card issuers currently provide more generous dispute rights to consumers than those required by law, but those policies are not written in stone, and other forms of electronic payment aren't treated the same. Dispute rights for fraud and misrepresentation don't just help consumers—they make the sellers more responsive to problems and more likely to conduct themselves properly in the first place, because if they don't they may not be paid and could even lose their ability to participate in the electronic payment system.
- Provide more resources for fighting Internet fraud. Law enforcement agencies need more resources to train investigators and prosecutors and to bring actions that may entail appearing in court in another country. We need more resources to sustain the League's fraud programs, too. In the past few years, we have received grants from the Bureau of Justice Assistance in the Department of Justice that have enabled us to upgrade our data system and improve services to

law enforcement agencies and consumers. We need more federal funding to supplement the support that we receive for the programs from our members and businesses that care about fighting fraud.

- Provide more resource for consumer education. Education is needed on an ongoing basis to make consumers aware of the danger signs of fraud and give them confidence in the new electronic marketplace. We have done many educational projects about e-commerce in the last few years with support from the private sector. For example, our *Be e-Wise: How to Shop Safely Online* brochure, which is on the League's main Web site, www.nclnet.org, was produced with a grant from MasterCard. More recently, we developed a Consumer Guide for Internet Safety and Security, also on the League's Web site, with support from Dell Corporation. The government should join the private sector in providing resources for nonprofit groups such as ours to reach out to consumers with the information they need to protect themselves in cyberspace.

Thank you very much for asking the National Consumers League to share its knowledge and suggestions on this important issue.

Mr. STEARNS. Thank you, Ms. Grant.

Let me start out my questions by asking you in your testimony you explained the highest volume of Internet related fraud is for on-line auction fraud. What are the specific types of auction fraud that you have reported?

Ms. GRANT. Two very simple types. I'm the high bidder. I sent my money to the seller. I either never got anything or what I got didn't remotely resemble what I was promised. And my favorite story in that regard is somebody who thought she was getting a portable wheelchair and instead received an aluminum lawn chair on casters. People are not seeing what they get before they get it and before they pay. So there's always an element of risk there. And we've been doing a lot of consumer education to tell people how they can reduce the possibility of loss by doing things such as using escrow services which act as go betweens, taking their payment and only forwarding it to the seller when they confirm that they got what they were promised.

Mr. STEARNS. What Internet frauds were most reported last year?

Ms. GRANT. Well, on-line auction scams topped the list. I'm happy to report that that's going down. It was 78 percent of the Internet fraud that we heard about last year as opposed to 87 percent the year before. It's gone down because of efforts by some of the large on-line auction houses to better police themselves and consumer education as well.

Mr. STEARNS. What steps can consumers take to protect themselves from on-line fraud?

Ms. GRANT. Well, we've heard that people are well advised to shop with companies that they know and trust, but we've also heard that there are a lot new players on the Internet. One of the things that we can do is help consumers recognize the hallmarks of fraud. It doesn't matter what the company name is. There are certain kinds of things that are offered and certain ways that they're offered that we know are fraudulent and we need to convey that information to consumers. For instance, somebody on-line, not a banker, another financial institution, who promises to give you a credit card or a loan as long as you pay a fee up front. We know that those offers are fraudulent. Actually, if we had a good on-line commerce rule we could prohibit those kinds of offers as we do in the telemarketing sales rule.

Mr. STEARNS. Do you think there's legislation that's needed in this area?

Ms. GRANT. We think legislation that would charge the FTC with developing an e-commerce rule would be very helpful. It's not necessarily going to prevent fraud, but it would do a couple of real useful things. One is it would create some bright lines which would help people understand what's fraudulent and what's not, what's appropriate behavior and what's not and the other is that when you have laws like this and I should point out that the telemarketing sales rule is helpful not only to the Federal agencies, but to the State Attorneys General who are able to go into Federal court to enforce it.

You can take easy action against a company if they're doing something which on its face because there's a rule that prohibits it is illegal.

Mr. STEARNS. Mr. MacCarthy, if I ask you to compare on-line commerce with off-line commerce, which would you say is safer?

Mr. MACCARTHY. I think with respect to the important for Visa cardholders, they're both equally safe.

Our zero liability policy which prevents cardholders from being held responsible for unauthorized use of their cards applies both on-line and off-line. So in the relevant respective applies to the Visa payment system, zero liability protects cardholders from unauthorized use 100 percent, on-line or off-line.

Mr. STEARNS. Aren't chargebacks more frequent on Internet transaction than other type of transactions?

Mr. MACCARTHY. They are and the fraud rates differ. The general fraud rate for all transactions is 7/100ths of 1 percent for all the areas in which cards are not present. It's 15/100ths of 1 percent. So there is a difference between the two and I think there's some things that explain that historically. When you go into a card not present environment, if you've stolen some cardholder information, you don't have to look the merchant in the eye. And also if you've gotten cardholder information, but you don't really have the card, you don't really have an alternative but to go to the card not present environment.

So those things explain the difference, but the thing I want to point out is that what those numbers measure is not the danger to consumers. It's the likelihood that someone will use that channel to commit fraud. And again, the consumers are protected 100 percent in either channel by the zero liability policy.

Mr. STEARNS. Mr. Charney, is the authentication technology progressing at appropriate pace to keep up with fraudulent actors? I think you've mentioned that American Express is using a smart card technology to protect its consumers?

Mr. CHARNEY. Right.

Mr. STEARNS. You might want to just explain some of that.

Mr. CHARNEY. Yes, I mean one of the things that some of the credit card companies are trying to do is turn these Internet transactions into card present transactions. So if your computer has a card reader and you have to insert your credit card into a slot, then the vendor at the other side doesn't just get your number from you typing it in, but knows you actually have the card. So that becomes almost closer to a card present transaction. You still can't look at

the signature on the back of the card, but you know the person has a credit card in hand.

The difficulty is those credit card readers are hardware, not software, therefore, they tend to be more expensive to deploy.

Mr. STEARNS. I've seen in the European Union I think they've started that. I think I saw that maybe up in Canada or somewhere that the smartcard, you put it in your computer now and it's using it rather than giving your number over the Internet.

Mr. CHARNEY. Smartcards have gotten far more acceptance in Europe than in the United States.

Mr. STEARNS. Do you think that's the way to the future that instead of giving your credit card over the Internet, you'll have it swiped in with maybe a little bit more identification?

Mr. CHARNEY. Absolutely. I think you'll see that and you'll see more biometric authentication over time. You can now buy laptops, for example, that will look at fingerprints to ensure that you're the person you claim to be. It raises interesting privacy issues, but many of them can be addressed in other ways.

Mr. MACCARTHY. Mr. Chairman, I think the possibility of using smart cards in a swiping context is a real possibility that will help to control fraud in the on-line environment, but let me direct your attention to another program that Visa is embarking on. It's our pay authentication program. It's currently a pilot program, but it will enable to issuers to confirm a cardholder identity during the on-line transaction itself and it involves the cardholder inserting a PIN number in the process of the transaction and that along with these other technologies that are coming on-line, the smart cards and so on, we think will help to control the fraud rate in the on-line environment.

Mr. STEARNS. My time has expired. Mr. Towns?

Mr. TOWNS. Thank you, Mr. Chairman. Let me begin with you, Ms. Grant. You mentioned the basic rules of e-commerce need to be set and I agree with that. These advanced fee loans from entities that are not regulated financial institutions, what are these unregulated financial institutions you refer to and how much of the on-line fraud problems do they account for, do you know?

Ms. GRANT. The kind of folks who offer loans and credit cards for a fee up front are not financial institutions at all. They're con artists working out the Internet version of boiler rooms, just making those offers and targeting people who are having financial difficulties. In fact, part of their pitch is that you're guaranteed a loan or a credit card, even if you have poor credit and sometimes they combine those offers with by the way, we'll clean up your credit history which we all know cannot happen.

They rank in the top 10 Internet frauds consistently, so it is a serious concern.

Mr. TOWNS. You talk about the need to enact consumer protections against the unauthorized sharing of personal information. What specific protections do you believe are needed?

Ms. GRANT. One concern is unsolicited commercial e-mail. We see a growing number of fraudulent solicitations being made to consumers by what's commonly referred to as spam and we'd like to see a law that would prohibit people from receiving unsolicited e-mails unless they've specifically agreed to do so with the sender.

But we also need, just in general, on-line privacy protection to keep consumers information from being shared when they give it to one entity with others without their knowledge and consent. We feel that that is the root of a lot of situations where people find themselves being charged for products and services that they've never agreed to and I should note that in the OECD's guidelines for consumer protection and e-commerce, one of the things that they call for is for countries to implement privacy protections along the line of the OECD guidelines for personal privacy protection. We think that that is important, not only on-line, but off-line.

Mr. TOWNS. My final question, Mr. Chairman. Ms. Grant, you mentioned the important role, the FTC's Telemarket and Fraud Rule has played in addressing crime. Is it your view that the FTC should issue on-line fraud rules in the same way that it addressed telemarketing fraud by regulation in the past?

Ms. GRANT. Yes, I think it would be very helpful for a e-commerce, but prohibiting acts that should on their be illegal and requiring disclosures that would help consumers know who they're dealing with, where the entity that they're dealing with is located and other key information that they need to make a wise on-line buying decision.

Mr. TOWNS. Let me thank you very much. Let me thank all of you for your testimony. You've been extremely helpful.

Mr. Chairman, I yield back.

Mr. STEARNS. Thank you to my colleague. Mr. Bass?

Mr. BASS. Thank you, Mr. Chairman. This has been very interesting testimony.

Mr. MacCarthy, this is probably going to be the nurdiest question I've ever asked in a subcommittee hearing. You say in your testimony that total fraud, total fraud is 7 per 10,000. Card not present fraud is 15 per 10,000, but that includes, that 15 per 10,000 includes the 7 per 10,000. Is that correct or not?

Mr. MACCARTHY. That's correct.

Mr. BASS. 7 per 10,000 is total for everything.

Mr. MACCARTHY. That's right. If you just look at total off-line as opposed to total in its entirety, you'd have a smaller number than 7. And if it's important for you, I could provide that information.

Mr. BASS. I'd be interested to know because this is going to be almost waste of time. I'd like to know what the fraud rate is for within the card not present category for Internet transactions versus telephone, anything else. You don't have to answer now. But that would be an interesting number.

Mr. MACCARTHY. I can give you that one. The first one you were asking for, I'd have to get back to you on. In the Internet context if you just look at Internet transactions, the fraud rate is 24/100ths of 1 percent.

Mr. BASS. 24 per 10,000.

Mr. MACCARTHY. Which is higher than the 15 and higher than the 7. We think, obviously, there are reasons why in the card not present environment, generally, you'd have a different——

Mr. BASS. Do you think that's a big problem or not? I'm just trying to get a feel for——

Mr. MACCARTHY. We think it's a problem that relates mostly to two factors. One is we've got a new channel of new commerce here.

Many of the merchants are not as well established as merchants that have been involved in mail order and telephone order. Their back offices may not be as well developed as some of the more established companies. And they may not take as full advantage of the fraud protection services that we provide as some of the more established merchants do.

The second is that we think that fraudsters like the anonymity of the Internet. In face to face fraud you've got to look the merchant in the eye. In the telephone context you've at least got to talk to him . In the Internet, you don't to do either.

Mr. BASS. Are there Internet payment companies that have developed user fees? First of all, why is Visa 95 percent of all? Why isn't it Diners and Master—I know you guys are obviously the best in the world, but did you say that 95 percent of all credit card transactions are Visa?

Mr. MACCARTHY. That would be nice, but it would be misleading to say it that way. Ninety-five percent of all the Internet transactions are paid for using a payment card, a debit card or a credit card. We have 53 percent of that part of the market.

Mr. BASS. Okay, that clarifies that. Internet payment companies, they exist, don't they? Do you know what I mean by that, like PayPal and Honesty?

Mr. MACCARTHY. Right.

Mr. BASS. Are they subject to the same—what is your relationship with them? They don't actually sell anything.

Mr. MACCARTHY. It depends on how they're set out. I don't want to speak in particular about any one of those, the operations. But I think Susan Grant mentioned the concern that consumers should be aware of that when they do use these alternative payment mechanisms they may not have the same legal protections that they have when they use their traditional credit card and debit cards and they certainly don't have the zero liability and other protections that we've done to provide beyond the current legal protections that they have using their credit cards.

Mr. BASS. In other words, on an on-line auction, the seller has to have his or her own direct contract with Visa in order for the buyer to get the same protections versus an intermediary?

Mr. MACCARTHY. Many of the on-line participants, the sellers, are not individuals, they're businesses. They're small businesses, but they're businesses and many of them do have access to the payment mechanism. They can use Visa cards or master cards or any of the other traditional cards.

Mr. BASS. One other question mainly for you, Mr. MacCarthy, following up on a question that Mr. Deal asked of the earlier panel, do any of you hold the opinion that existing laws and regulations actually act as a barrier to investigating reported or suspected misuse and do any of these barriers preclude you from notifying consumers that they may have been victimized?

Mr. MACCARTHY. Not at the present. As you probably know, financial institutions live under the Gramm-Leach-Bliley Act and there are privacy protections and security protections built into that act for financial institutions. But there's a clear exception for the choice requirement for consumers to take into account the fraud situation. WE think that's essential. We have to be able to

pass on information to law enforcement people with whom we work very closely without having the possibility that a consumer would interpose privacy rights.

Privacy rights are crucial. We don't think there's a problem with having a generalized privacy rights, but in that kind of context it's very, very important. It's essential for us to be able to pass information on to law enforcement agencies for fraud prevention.

Mr. BASS. Thank you, Mr. Chairman.

Mr. STEARNS. time has expired. We are finishing up. The gentleman from Illinois, does he wish to ask any questions?

All right, I want to thank the second panel for their patience in waiting through the first panel and the subcommittee is adjourned.

[Whereupon, at 12:25 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

PAYPAL
June 29, 2001

The Hon. CHARLIE BASS
United States House of Representatives
Washington, D.C. 20515

DEAR REPRESENTATIVE BASS: We were pleased that you inquired about online payment services like PayPal at the May 23rd hearing in the Subcommittee on Commerce, Trade, and Consumer Protection entitled "On-line Fraud and Crime: Are Consumers Safe?" PayPal is the world's first and largest online payment service. With PayPal, individuals and businesses can transfer money instantly and securely using the Internet. This revolutionary service provides a faster, easier, less expensive, and safer way to move money in today's digital economy.

In response to your questions, Mark MacCarthy from Visa USA identified two important factors in Internet fraud. First, the Internet is a new channel of commerce. Many merchants are inexperienced with remote commerce and their back offices may not be as well developed as more established companies. Such merchants may not take as full advantage of the fraud protection measures that are available. Second, Internet commerce is more anonymous than traditional commerce. It is easier for criminals to commit fraud in an environment that does not require face-to-face contact or even a telephone conversation.

We concur with these intelligent observations and, like Visa, are working to lower fraud rates so that e-commerce can continue its dramatic growth—especially for small business-people and entrepreneurs who have not traditionally had access to a national market and cost-effective payment systems.

Though Mr. MacCarthy was thoughtfully cautious not to speak of any particular online payment service, a portion of your colloquy with him (excerpted below) may have left a mistaken impression about the protections enjoyed by consumers using PayPal. You summarized your understanding by noting that, "in an online auction, the seller has to have his or her own direct contract with Visa in order for the buyer to get the same protections versus an intermediary."

This is not the case with PayPal. A consumer using his or her credit card with PayPal retains all the rights and privileges accorded by the card-issuing bank, including the right to dispute payments. In the uncommon event of a dispute, PayPal works with the consumer and seller to resolve the issue. As the merchant of record for the card transaction, PayPal takes a chargeback if the issue cannot be resolved and if the seller will not honor his or her commitment. Consumers who use a credit card on PayPal retain all the protections offered by credit cards.

When consumers do not use a credit card with PayPal, sending money from their bank accounts or PayPal accounts, these transactions are the equivalent of sending money through Western Union, by check, or in cash. Once the recipient has retrieved the money from PayPal, there is no effective way to reverse the transaction, just as there is no way to stop payment on a check that has cleared.

Too often, consumers find bargains in online auctions that seem "too good to be true"—only to discover later that they are, indeed, not true. That is why PayPal takes the steps it does to protect its users against fraud. Our 75-person Fraud and Investigations team, which was recently recognized in the Wall Street Journal's online edition, has seen substantial success in preventing online auction and e-commerce fraud against consumers, and in providing assistance in the apprehension and successful prosecution of those who temporarily succeed. PayPal's proprietary

anti-fraud software, which analyzes the patterns of transactions searching for suspicious activity, helps the team identify potentially fraudulent sales and recover consumer funds before they leave the system, and has enabled PayPal to return payments to thousands of consumers. These efforts have also allowed PayPal to alert law enforcement of numerous fraud attempts against consumers before their conclusion, and to reduce the fraudulent transaction rate, in our network to well below the e-commerce industry average, as calculated by the Gartner Group.

For example, the day of the hearing, the FBI acknowledged our work to fight fraud by inviting us to participate in the press conference announcing that it had brought charges against approximately 90 criminals in "Operation Cyber Loss." The Bureau's press release cited PayPal's "great assistance in identifying individuals engaged in wrong doing . . ."

PayPal takes seriously its commitments to consumer protection and fraud prevention. We hope that this letter clarifies your impressions of our particular online payment service. By copy of this letter, we are requesting that Chairman Steams also include it in the hearing record. We are very pleased by your awareness of PayPal, our services, and the positive effect e-commerce is having on small and remote business-people who have historically not had access to a national marketplace. If we can answer any further questions, please contact me at the letterhead address or our Washington representative, Jim Harper of PolicyCounsel.Com at (202) 546-3701.

Sincerely,

VINCENT SOLLITTO
Vice President, Corporate Communications