AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE INTERNATIONAL CONSUMER PROTECTION ACT OF 2003

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 17, 2003

Serial No. 108–45

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
89–470PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (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
RICHARD BURR, North Carolina
Vice Chairman
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
ERNIE FLETCHER, Kentucky
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho

JOHN D. DINGELL, Michigan
Ranking Member
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
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California

DAN R. BROUILLETTE, *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*

FRED UPTON, Michigan
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
Vice Chairman
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
ERNIE FLETCHER, Kentucky
MIKE FERGUSON, New Jersey
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

JAN SCHAKOWSKY, Illinois
Ranking Member
HILDA L. SOLIS, California
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
JIM DAVIS, Florida
PETER DEUTSCH, Florida
BART STUPAK, Michigan
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

THE INTERNATIONAL CONSUMER PROTECTION ACT OF 2003

WEDNESDAY, SEPTEMBER 17, 2003

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

The subcommittee met, pursuant to notice, at 10:03 a.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Shimkus, Terry, Issa, Otter, Schakowsky, Stupak, Green, and Dingell, (ex officio).

Staff present: Ramsen Betfarhad, majority counsel; Kelly Zerzan, majority counsel; Jill Latham, legislative clerk; Vikki Ehrlich, deputy communications director; and Jonathan J. Cordone, minority counsel.

Mr. STEARNS. Good morning everybody, and welcome to the Subcommittee's legislative hearing on "The International Consumer Protection Act of 2003." My colleagues, increasingly we hear of scams and other fraudulent and deceptive acts perpetrated against the American consumer by persons and companies that are located overseas.

The Federal Trade Commission data shows a substantial rise in consumer complaints that they receive from U.S. consumers against foreign companies. The data shows that the number of cross-border fraud complaints collected by the FTC rose to over 14 percent of all complaints, excluding identity theft. That number was just 1 percent in 1995.

The same data shows that over 24,000 of those complaints by U.S. consumers were directed by foreign companies and represented 17 percent of all money lost to fraud in the year 2002. Of the total number of U.S. consumer border fraud complaints, nearly half had to do with foreign money offers and advance fee loans.

One quarter of the complaints involved scams around sweepstakes and free prices or gifts. Moreover, fraud and deception involving Internet auctions represented 10 percent of cross-border complaints that were filed in 2002.

As a member closely involved in our committee's effort to draft anti-spam legislation, I found it particularly interesting that in more than 70 percent of the cases an American consumer is first contacted by fraudsters based overseas through the e-mail.

This is true of fraudsters from all countries, except Canada, where the preferred method is still the telephone. Therefore, I

agree with the Commission's view that enhancing the FTC's ability to address cross-border consumer fraud and deception more effectively will also have a real and substantial impact on reducing spam.

I do think we also have a growing problem where the American consumer is victimized by way of fraud and/or deception that finds its genesis beyond our borders and beyond the present reach of our law enforcement and this trend will not subside.

We all know that as consumers we are increasingly becoming part of a highly integrated global marketplace. There is no escaping that fact. Therefore, I strongly support the efforts of the FTC directed at combating cross-border fraud.

In principle, I support the Commission's proposed legislation seeking enhanced authority that it deems necessary for it to effectively combat cross-border fraud. I am confident that at this time this legislation, when perfected, will become one of the most significant pieces of legislation authored by Congress in support of the American consumer.

In the past few weeks, I, along with the ranking member of the subcommittee, have been working closely with the Commission to address our concerns with the proposed legislation, with the aim of perfecting this very important legislation.

My objective is to ensure that the civil liberties of Americans are in no way undermined for the sake of combating cross-border fraud. Finally, I plan to continue working in a bipartisan fashion with the Commission and others toward the expeditious introduction and consideration by the committee members of a good bill, worthy of speedy approval.

I invite all of my members of the subcommittee to join in our efforts by becoming original co-sponsors of this bill. So I look forward to our witnesses testimony and the enactment of a good bill protecting consumers from cross-border fraud this session of Congress. And with that, the ranking member.

Ms. SCHAKOWSKY. Thank you, Chairman Stearns, for holding this hearing on the International Consumer Protection Act of 2003. The draft legislation that Chairman Stearns and I have circulated grants the Federal Trade Commission additional powers to combat international consumer fraud.

The draft bill is a work in progress, and I look forward to hearing the expert testimony from today's witnesses; their thoughts on the draft bill, and the problems that the bill aims to address.

The chairman itemized the ways in which the FTC's "Consumer Sentinel" found consumer fraud as this growing problem, and the documentation, and so I won't repeat that. But clearly cross-border fraud is a serious problem that Congress needs to address.

And he also raised that some of you may have and that we have had as well, that the legislation that grants the FTC greater powers to share since it is sensitive information with foreign governments about individuals and businesses, that it raises some difficult questions for the subcommittee and the Congress as a whole in striking that delicate balance between protecting civil liberties and fighting consumer fraud.

We need to ensure that we don't give the FTC a license to violate individual rights, but still provide the tools that it needs to protect

consumers. We fought hard throughout our history to maintain a free and open society, and clearly we don't want to sacrifice those freedoms in the name of combating consumer fraud.

And finally I want to sincerely thank Chairman Stearns and Chairman Tauzin for working with me in a bipartisan fashion on this important legislation. I really commend them for being inclusive and I hope that we will be able to introduce and pass a bipartisan bill in the very near future. Thank you.

Mr. STEARNS. I thank my colleague. The gentlemen from Illinois, Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman, and thank you, Mr. Muris, for joining us today on an issue that is very, very important. We just came out of a conference meeting that was somewhat contentious on many issues, and some of it that we hope you will be addressing through the FTC and the whole issue of how do we continue to open markets and go into international trade, and use all this new technology, and make sure that our consumers are protected.

And so we look forward to the hearing, and I appreciate your attendance, and Mr. Chairman, I yield back my time.

Mr. STEARNS. I thank the gentleman.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Thank you, Mr. Chairman, for holding this hearing. It is important that legislation be thoroughly discussed in a realm that includes those significantly impacted by a bill and you have given us the valuable opportunity to do just that.

I would also like to thank the distinguished panelists that have joined us today. Your testimony will shed valuable light on the legislation before us and bring American consumers one step closer to the protections they need and deserve.

The marketplace continues to evolve as technologies are forever improving and affording consumers and businesses alike with more opportunity than ever before. Unfortunately, as with anything, these opportunities are not always seized in the name of all that is right and just. Criminals are as likely, if not more so, to demonstrate the phenomenal capabilities available today at the expense of people's hard-earned money and assets.

We must ensure that an adequate counter-force is not just keeping up or being maintained, but staying ahead of the criminal game. The Federal Trade Commission must be given the power, authority and resources necessary to do just that. The Federal Trade Commission has proven to be enormously valuable in regulating how business is done and protecting the rights and interests of all parties involved. We must thoroughly, consistently and continuously examine what the FTC is able to do and how it might be more effective in its pursuits.

There are numerous scam artists out there looking to make a buck without having to work for it. The people of Wyoming—as with people in every state—will benefit greatly by the protections and powers extended within the proposal before us today. We must take swift action.

Again, I thank the panelists and am certain that today's testimony will further illuminate the path that this legislation must take in a timely manner.

I thank the Chairman again and yield back the remainder of my time.

PREPARED STATEMENT OF HON. C.L. "BUTCH" OTTER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF IDAHO

Mr. Chairman, I appreciate the opportunity you have provided for this subcommittee to review and examine this legislation. I do see the value in removing some barriers that currently prohibit the exchange of information between domestic and foreign agencies working to protect consumers from fraud. Yet, I have real concerns with some of the extensions of power this bill seems to give the Federal Trade

Commission. I think there are some legitimate civil rights issues the committee must resolve before we move legislation.

In addition to providing an unprecedented means of communications and business opportunities, E-commerce has generated a number of complex issues relating to responsibility, enforcement, and the jurisdiction of laws regulating the Internet and other technological means of doing business. There is no doubt American consumers deserve the best efforts of the FTC in their pursuit to inform and warn the public of possible scams and in the investigation of those operations that violate the law. However, in reading certain provisions of the International Consumer Protection Act draft bill, I became concerned that this proposal may be inadvertently circumventing the sovereignty of our nation and the rights of our law abiding citizens. I am uneasy when this discussion reaches the point of asking U.S. agencies or commissions to enforce the laws of other nations on our citizenry, or visa versa.

Before moving forward on this issue, we must clarify that U.S. citizens will only be accountable to U.S. law. I cannot in good conscious support something that could require my U.S. law-abiding constituents to comply with the laws of foreign lands as a condition of doing business on the Internet.

Furthermore, I find the current language concerning the definition of the adverse results test unacceptable. The Federal Trade Commission cannot be permitted the opportunity to circumvent our legal system by casting internal determinations when applying an adverse result test in order to gain access to delayed notification rights.

While these are no doubt serious issues, I look forward to working with the commission on finding appropriate and constitutional ways to provide Americans increased protection from international scams and frauds perpetrated via the Internet and other technological means.

PREPARED STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Thank you Chairman Stearns and Ranking Member Schakowsky for holding this hearing on the International Consumer Protection Act.

I understand that this legislation is a high priority for the Federal Trade Commission, and particularly for Chairman Muris and Commissioner Thompson.

So I appreciate the Chairman's willingness to appear before us today to lay out the FTC's proposals to fight deceptive practices that have an international scope and are increasingly affecting U.S. consumers.

It's no surprise that international consumer protection is becoming an issue of increasing relevance to this subcommittee.

Globalization, increased world trade and the proliferation of Internet-based services and commerce has dramatically changed the world in which we live.

Many of these changes have been for the better; however, they have also created fertile ground for fraudulent activities.

Consequently, the act of fraud itself has taken on a global nature, thus making it increasingly difficult for law enforcement and the FTC to find and prosecute perpetrators of fraud.

We've learned from various consumer complaints that international fraud can take many forms.

Identity theft and financial scams are two extreme examples, but telemarketing and spam are issues that I'd bet most of us in this room have had to contend with.

Congresswoman Heather Wilson and I have dropped a good, consumer-friendly bill that would address our spam problem by giving consumers and the FTC the tools they need to push back against the spammers.

And I hope that this bill we're considering today will give the FTC even more ammunition in the fight against spam.

International problems require international solutions, and the only way to effectively fight cross-border fraud is through international cooperation.

While the FTC's mission heretofore has been primarily domestic in nature, the protection of U.S. consumers against fraud and other deceptive practice now dictates that the FTC adopt an international scope.

To that end, we need to provide the FTC with expanded investigatory and enforcement capabilities, and I applaud our Chairman, Ranking Member and the FTC for tackling this issue head on.

In our efforts to fight cross-border fraud, however, I do want to make sure that the policies we enact protect the privacy and civil liberties of all involved parties.

Our witnesses have indicated that several provisions of this bill could raise 4th Amendment questions.

These are troubling concerns that must be addressed before we move forward with this legislation.

Given the bi-partisan nature of the negotiations thus far, however, I am confident that our subcommittee can produce a bill that will effectively protect U.S. consumers from international fraud while also preserving constitutional rights and privileges.

Thank you to all of our witnesses for appearing before us today.

I look forward to your testimony.

And with that, Mr. Chairman, I yield back the balance of my time.

Mr. STEARNS. We welcome the Chairman of the Federal Trade Commission, the Honorable Timothy Muris. We welcome your opening statement.

STATEMENT OF HON. TIMOTHY J. MURIS, CHAIRMAN, FEDERAL TRADE COMMISSION

Mr. MURIS. Thank you very much. I am pleased to appear to testify on the International Consumer Protection Act of 2003. Mr. Chairman, and Ranking Member Schakowsky, I personally want to thank you and your staffs for the many hours of hard work that you have devoted to developing this legislation.

I know that some of these issues are complex and we really appreciate you working with us. I do understand that it is a work in progress. We have listened to the concerns that many people have raised. We think that we can work with you and make changes that would satisfy those concerns, and still allow us to address this very important issue.

As you know, the FTC is the agency that is primarily responsible in the Federal Government for protecting American consumers. There are limitations on our ability to fight cross-border fraud that make it increasingly difficult to meet this responsibility.

Today, cross-border fraud operators victimize large numbers of Americans and the problem is growing. For example, fraudulent Canadian telemarketers victimize American consumers and hide their ill-gotten gains in foreign bank accounts.

Website operators victimize consumers worldwide and remove their sites when they learn they are being investigated. Deceptive spammers can easily hide their identity, disguise the electronic path of their e-mail messages, and send messages from anywhere in the world to anyone in the world.

Not surprisingly, this is reflected in our complaint data base that you mentioned. We have a chart here to your right which shows that there were more than 30,000 complaints collected in "Consumer Sentinel" that involved either domestic consumers complaining about foreign businesses, or foreign consumers complaining about domestic businesses.

About 80 percent of these cross-border complaints were U.S. consumers complaining about foreign businesses. With these complaints, we have had a corresponding increase in our cases involving cross-border fraud.

Last year, for example, we brought about 20 new Federal District Court lawsuits involving foreign defendants or foreign consumers. We have continued to litigate and settle dozens of cases involving fraud and deception that operate cross-border.

Indeed, today we are announcing settlements in two cross-border lottery cases that will return almost $2 million for consumer re-

dress. An increasing number of these cross-border cases involve allegedly deceptive spam, which is often cross-border in nature.

We have found that the path from a fraudulent spammer to a consumer's in-box typically crosses at least one international border, and usually several. In other words, this legislation is anti-spam legislation, and it is very important for us in the battle against spam.

We are in the process of implementing a plan that we announced last year, which is a five point plan to combat cross-border fraud. It includes working with multilateral organizations, enforcement task forces, public/private partnerships, and technical assistance groups to developing countries.

My colleague, Mozelle Thompson, is the head of the OECD Consumer Protection Committee. The OECD recently has promulgated very important guidelines to deal with the cross-border fraud problem.

Quite simply, we need new legislative authority. The attraction to deal cross-border if you are a fraudster is just overwhelming. One reason is that you can target a larger market.

Another reason is that by operating cross-border, you make it more difficult for the relevant law enforcement authorities to deal with you. Further, you can move your money outside the United States, so that we need a foreign action to collect on a judgment in the United States.

This is time consuming, expensive, and sometimes we can't do it at all. The legislation that we have proposed, and is reflected in the draft bill, has four main goals. The first is to strengthen our ability to share information with, and provide investigative assistance to our foreign counterparts, who often are investigating the same targets that we are.

Second, we seek to improve our ability to gather information by sharing confidential treatment of information we receive from certain sources. Without such assurances, this valuable information in many cases, we just are not going to get it.

Third, we seek to improve our ability to obtain consumer redress in cross-border cases by clarifying our authority to act in such cases, and expanding our ability to use foreign counsel to pursue assets off-shore.

Finally, we seek to strengthen our international cooperative relationships by obtaining authority to conduct staff exchanges, and to provide financial support for certain joint products.

The Congress already has provided tools to cooperate internationally to the SEC, to the CFTC, to the FTC and the Antitrust Division for Antitrust, and what we are seeking is similar authority for cross-border fraud.

We have consulted widely on this legislation, both within and outside the government, and with the Congress, and we are committed to working closely with you to make it an appropriate bill to achieve the balance that you all mentioned this morning.

We greatly appreciate the opportunity and your help in this important issue, and we look forward to continuing to work together.

[The prepared statement of Hon. Timothy J. Muris follows:]

PREPARED STATEMENT OF HON. TIMOTHY J. MURIS, FEDERAL TRADE COMMISSION

Mr. Chairman, I am pleased to appear before the Subcommittee today to provide information on the challenge of cross-border fraud and the efforts of the Federal Trade Commission ("Commission" or "FTC") to address this growing problem.[1]

The FTC is the federal government's principal consumer protection agency, with a mandate to prohibit unfair or deceptive acts or practices and to maintain vigorous competition in the marketplace.[2] The Federal Trade Commission Act authorizes the Commission to file federal district court actions, which typically seek preliminary and permanent injunctions to halt deceptive activity and seek to provide redress for injured consumers.[3]

An increasing number of these actions involve cross-border fraud and deception, which adversely affect American consumers and businesses. These actions often involve foreign businesses and individuals, consumers, assets, or evidence. Similarly, an increasing number of consumer complaints collected in our *Consumer Sentinel* database maintained by the Commission involve either domestic consumers complaining about foreign businesses or foreign consumers complaining about domestic businesses.[4] Thus, we are devoting additional resources to fighting cross-border fraud within the existing legislative framework and are proposing certain legislative changes that would give us additional tools to help address the problem of cross-border fraud. Most of our proposed changes are based on authority Congress has already given to securities, antitrust, and banking enforcers in the international context.

Today's testimony begins by describing the growth of cross-border fraud and the problems associated with this growth. It then discusses our efforts within the existing legislative framework to combat cross-border fraud. Finally, it examines the need for additional legislation to help us fight cross-border fraud and describes our legislative recommendations.

I. THE PROBLEM OF CROSS-BORDER FRAUD

Today, cross-border fraud operators are victimizing American consumers to an extent unknown just a few years ago, and the problem is growing worse. Globalization of trade, improvements in the international telephone system, and the advent of the Internet have given consumers direct access to foreign sellers. Today, there are satellite networks broadcasting advertisements around the world, with operators waiting to take orders in many languages. Telemarketers routinely call U.S. consumers from Canada. Most significantly, electronic commerce in many instances is blurring the effect of national borders.

Cross-border commerce creates new opportunities for consumers and businesses, but it also poses new challenges to consumer confidence and to law enforcement. Consumers cannot assess the credibility of many merchants located across the globe as easily as they could with local vendors, and law enforcement cannot protect consumers as easily from fraud operators who, effectively, may be out of reach.

Using Internet and long-distance telephone technology, fraud operators can strike quickly on a global scale, victimize thousands of consumers in a short time, and disappear nearly without a trace—along with their ill-gotten gains. For example, fraudulent Canadian telemarketers victimize American consumers and hide their ill-gotten gains in foreign bank accounts. Website operators victimize consumers worldwide and take down their sites when they learn they are being investigated by law enforcement. And deceptive spammers can easily hide their identity, forge the electronic path of their email messages, and send messages from anywhere in the world to anyone in the world.

A. Complaint Statistics

Not surprisingly, an increasing number of complaints collected in *Consumer Sentinel* involve international transactions. In 2002, 14 percent of the complaints collected in *Consumer Sentinel* involved either domestic consumers complaining about foreign businesses or foreign consumers complaining about domestic businesses, as

---

[1] The written statement represents the views of the Federal Trade Commission. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

[2] 15 U.S.C. § 45(a).

[3] *See* 15 U.S.C. § 53(b). The FTC also is authorized to initiate administrative proceedings to enforce the Federal Trade Commission Act. See 15 U.S.C. § 45(b).

[4] *Consumer Sentinel* is a database of consumer fraud complaints maintained by the FTC. Complaints are entered into the database from many sources and are accessible to more than 700 law enforcement agencies in the United States, Canada, and Australia. The database currently contains over one million complaints. *See* www.consumer.gov/sentinel.

compared with less than 1 percent in 1995.[5] Seventy-nine percent of these complaints in 2002 involved U.S. consumers complaining about foreign businesses.[6] The complaints include more than 24,000 complaints by U.S. consumers against foreign companies, complaining about transactions involving more than $72 million.[7] The cross-border fraud schemes U.S. consumers complained about most often in 2002 involved foreign money offers, advance fee loans, prizes, sweepstakes gifts, and internet auctions.[8] The obstacles we face in fighting cross-border fraud leave U.S. consumers particularly vulnerable to such scams.

B. FTC Cross-Border Cases

In the past several years, there has been a corresponding increase in FTC cases with a cross-border component. These cases often target foreign defendants. The FTC has brought cases against defendants in Australia,[9] Canada,[10] Hong Kong,[11] Spain,[12] Switzerland,[13] and the United Kingdom.[14] Many of the cases have involved the transfer of assets to such offshore locations as the Bahamas,[15] the Cayman Islands,[16] the Cook Islands,[17] and Vanuatu.[18] The cases also frequently involve evidence located in other countries, including Canada, the Netherlands, France, Germany, Mexico, and Spain.[19] Other cases involve individuals and businesses based in the U.S. that target both domestic and foreign consumers.[20]

An increasing number of these cases involve allegedly deceptive unsolicited commercial e-mail, or spam, which is often cross-border in nature.[21] Indeed, the Commission's law enforcement experience shows that "the path from a fraudulent spammer to a consumer's in-box typically crosses at least one international border and usually several."[22]

---

[5] *See* FTC REPORT, CROSS-BORDER FRAUD TRENDS, JANUARY-DECEMBER 2002 4 (Feb. 19, 2003), *available at* <http://www.ftc.gov/bcp/conline/edcams/crossborder/PDFs/CrossBorderCY2002.pdf>.

[6] *Id.* at 9.

[7] *Id.* at 13.

[8] *Id.* at 10.

[9] *FTC v. Pereira,* Civ. Action No. 1:99 CV 01367 (E.D. Va. filed Sept. 14, 1999), *available at* <http://www.ftc.gov/os/1999/9909>.

[10] *E.g., FTC v. 1492828 Ontario Inc., d/b/a First Capital Consumers Group,* Civ. Action No. 02C 7456 (N.D. Ill. filed Oct. 17, 2002), *available at* <http://www.ftc.gov/opa/2002/10/firstcap.htm>. A complete list of all cases that the FTC has brought against Canadian defendants between 1997-2002 is contained in MASS-MARKETING FRAUD: A REPORT TO THE ATTORNEY GENERAL OF THE UNITED STATES AND THE SOLICITOR GENERAL OF CANADA (May 2003), *available at* <http://www.usdoj.gov/opa/pr/2003/May/remmffinal.pdf>.

[11] *FTC v. Hudson Berkeley,* Civ. Action No. CV-S-02-0649-PMP-RJJ (D. Nev. filed May 7, 2002), *available at* <http://www.ftc.gov/opa/2002/05/projectabsurd.htm>.

[12] *FTC v. BTV Indus.,* Civ. Action No. CV-5-02-0437-LRH-PAL (D. Nev. filed Mar. 27, 2002), *available at* <http://www.ftc.gov/opa/2002/04/btv.htm>.

[13] *FTC v. Dr. Clark Research Ass'n,* Civ. Action No. 1:03CV0054 (N.D. Ohio filed Jan. 8, 2003), *available at* <http://www.ftc.gov/opa/2003/01/drclark.htm>.

[14] *FTC v. TLD Networks Ltd.,* Civ. Action No. 00-CV-906 (N.D. Ill. filed Feb. 28, 2002), *available at* <http://www.ftc.gov/opa/2002/03/tld.htm>.

[15] *FTC v. SlimAmerica,* Civ. Action No. 97-6072 (S.D. Fla. filed Jan. 27, 1997), *available at* <http://www.ftc.gov/opa/1997/02/slim.htm>; *FTC v. Online Communications,* Civ. Action No. CV-S-96-00055-LDG (RLH) (D. Nev. filed Jan. 23, 1996), *available at* <http://www.ftc.gov/opa/1996/08/road2.htm>.

[16] *FTC v. J.K. Publications, Inc.,* Civ. Action No. CV 99-0044 ABC (AJWx) (C.D. Cal. filed Jan. 5, 1999), *available at* <http://www.ftc.gov/opa/1999/01/netfill.htm>.

[17] *FTC v. Affordable Media,* LLC, Civ. Action No. CV-S-98-669-LDG (RLH) (D. Nev. filed Apr. 23, 1998).

[18] *E.g., FTC v. J.K. Publications, Inc.,* Civ. Action No. CV 99-0044 ABC (AJWx) (C.D. Cal. filed Jan. 5, 1999), *available at* <http://www.ftc.gov/opa/1999/01/netfill.htm>.

[19] *E.g., FTC v. Electronic Prods. Distrib., LLC,* Civ. Action No. 02-CV-888H (AJB) S.D. Calif. filed May 7, 2002), *available at* <http://www.ftc.gov/opa/2002/05/projectabsurd.htm>; *FTC v. Assail, Inc.,* Civ. A. No. W03CA007 (W.D. Tex. filed Jan. 9, 2003), *available at* <http://www.ftc.gov/opa/2003/02/assail.htm>; *FTC v. 1492828 Ontario Inc., d/b/a First Capital Consumers Group,* Civ. Action No. 02C 7456 (N.D. Ill. filed Oct. 17, 2002), *available at* <http://www.ftc.gov/opa/2002/10/firstcap.htm>; *FTC v. CSCT, Inc.,* Civ. Action No. 03 C 00880 (N.D. Ill. filed Feb. 6, 2003), *available at* <http://www.ftc.gov/opa/2003/02/csct.htm>; *FTC v. Zuccarini,* Civ. Action No. 02C 7456.C.A. No. 01-CV-4854 (E.D. Pa. filed Sept. 25, 2001), *available at* <http://www.ftc.gov/opa/2001/10/cupcake.htm>; *FTC v. BTV Indus.,* Civ. Action No. CV-5-02-0437-LRH-PAL (D. Nev. filed Mar. 27, 2002), *available at* <http://www.ftc.gov/opa/2002/04/btv.htm>.

[20] *E.g., FTC v. Skybiz.com Inc.,* Civ. Action No. 01-CV-096 (N.D. Okla. filed May 30, 2001), *available at* <http://www.ftc.gov/opa/2001/06/sky.htm>.

[21] To date, the FTC has brought over 56 enforcement actions involving deceptive or fraudulent spam.

[22] Prepared Statement of the Federal Trade Commission, *Spam (Unsolicited Commercial E-Mail), Before the Senate Committee on Commerce, Science and Transportation,* 108th Cong. (May 21, 2003). This conclusion is also supported by the FTC's recent initiative to educate businesses about "open relays." Open relays allow third parties to route their e-mail through servers of

C. Problems Faced by Law Enforcement

Despite the FTC's vigorous law enforcement activities, cross-border fraud operators continue to use national borders to facilitate their schemes. Those engaged in cross-border fraud enjoy more attractive revenue prospects and face a lower likelihood of prosecution than domestic scam artists because:

- They can target a larger market.
- Evidence of their scams is often spread out in different jurisdictions, and it is difficult for the relevant authorities to share that evidence. Indeed, many U.S.-based defendants purposefully use foreign third parties to perpetrate their scams in an attempt to evade U.S. law enforcement authorities.[23]
- It is sometimes unclear which countries have legal jurisdiction to act.[24]
- U.S. enforcers have extremely limited ability to impose conduct remedies on foreign defendants because most courts will not enforce injunctive orders issued in other countries.[25]
- The fraud operators can move money offshore, thus necessitating a foreign action to enforce a U.S. court judgment. This is time-consuming, expensive, and, in many cases, futile, as many countries do not enforce U.S. court judgments obtained by government agencies.[26]

---

other organizations, thereby disguising the real origin of the e-mail. The FTC initiative, conducted in partnership with 16 other agencies in four countries, found that a significant portion of the open relays identified were located outside the United States, in countries such as China, Korea, Japan, Italy, Poland, Brazil, Germany, Taiwan, Mexico, Great Britain, Chile, France, Argentina, India, Spain, and Canada.

[23] For example, in *FTC v. Zuccarini,* Civ. Action No. 01-CV-4854 (E.D. Pa. filed Sept. 25, 2001), *available at* <http://www.ftc.gov/opa/2001/10/cupcake.htm>, the defendant had initially perpetrated his Internet scheme using U.S.-based Internet Service Providers (ISPs) and domain registrars. When he found out that the FTC was investigating him, he fled the country and continued to perpetrate his scheme through ISPs in the Netherlands and domain registrars in France, Germany, and Spain.

[24] The FTC recently faced this situation with respect to a matter that a foreign consumer protection agency referred to us concerning a scheme run by a U.S. company in various parts of Europe. Because of its enabling legislation, the referring agency could not bring an action against a U.S. company. Upon investigation, FTC staff learned that no U.S. consumers were injured by the scheme and neither the misrepresentations nor other conduct material to the fraud occurred in the United States. Given that the jurisdictional nexus to the U.S. was unclear in this case, as well as the practical problems that litigation would have posed, FTC staff decided not to pursue the case. By structuring its operations in this manner, the entity evaded law enforcement authorities on both sides of the Atlantic.

[25] *FTC v. Verity International* illustrates the limits of imposing conduct remedies on foreign defendants. 140 F. Supp. 2d 313, 318 (S.D.N.Y. 2001). In that case, the individual foreign defendants failed to comply with the asset-reporting requirements of a preliminary injunction obtained by the FTC. The U.S. court held them in contempt. In arguing against the motion for contempt, defendants pointed out that the contempt order would be futile because they were unlikely to enter the United States while the contempt matter was outstanding. The court acknowledged that defendants could avoid arrest by staying outside of the United States, but granted the motion for contempt, suggesting that preventing the defendants from entering the United States was an appropriate measure in this case. This case illustrates the limits of a contempt order on foreign defendants—as a practical matter, a foreign defendant can generally avoid sanctions for contempt by staying outside the United States.

[26] This problem has arisen in many FTC-related cases. For example, a receiver appointed in an FTC matter recently faced difficulties in obtaining relief from an Australian court. In *Evans v. Citibank Limited* & others, Equity Division Proceedings No. 4999 of 1999 (Sup. Ct. New South Wales), the receiver was not seeking direct enforcement of an FTC judgment, but instead was attempting to use the FTC's judgment as a basis for ordering a third-party bank to transfer certain assets to the control of the receiver under a constructive trust theory. The court held that the receiver's claims were "penal" in nature and denied the receiver's claim. This matter is currently on appeal. Similarly, *United States v. Asiatrust Limited,* Plaint No. 57/1999, was a case challenging the defendants' transfer of funds to a Cook Islands trust to defeat the FTC's judgment in *FTC v. Affordable Media, LLC,* Civ. Action No. CV-S-98-669-LDG (RLH) (D. Nev. filed Apr. 23, 1998). The High Court of the Cook Islands construed the case (which was pled as a new action) as one involving the enforcement of a penal law. The Cook Islands court dismissed the United States' action holding that the FTC's action was one to enforce "regulatory rights and powers." "They are or have a flavour of punishment and I conclude that these are at least in part, penal provisions, and fall within the relevant principle. It is also a public law which is sought to be enforced by the state or the sovereign alone for regulatory purposes and is one which ought not be enforced here." (4 Dec. 2001 Judgment at 8). The matter ultimately was resolved by settlement and the defendants repatriated their assets to the FTC pursuant to a stipulated judgment. *See also Impediments to Digital Trade Before the House Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce,* 107th Cong. (2001) (statement of Jeff Kovar, Assistant Legal Advisor for Private International Law, Department of State) ("Most foreign judgments are already recognized and enforced in the

Continued

- Enforcers have less incentive to pursue fraud operators who victimize consumers outside their jurisdictions but leave local consumers alone.

1The legislative recommendations that we make today will help to minimize some of these burdens, as further described below. In other cases, the burdens result from other countries' practices. We believe that our proposed legislation, if passed, will encourage greater reciprocity, providing an incentive for these countries to lift existing barriers to combating cross-border fraud.

D. Importance of Pursuing Cross-Border Fraud Operators

Pursuing those who victimize U.S. consumers from abroad is important to protect consumers from the substantial harm foreign fraud operators can cause.[27] Moreover, consumers' concerns about fraud and deception in the global marketplace could undermine their confidence in cross-border transactions and could lead them to conclude that they should only do business with local merchants. Unaddressed, these consumer concerns could hurt legitimate businesses by shrinking the market for their products and services. If the promise of the global marketplace is to be fully realized, governments must assure consumers that they are working to keep markets free from fraud and deception.

Pursuing U.S. businesses who victimize foreign consumers is also critical. Stopping U.S.-based cross-border fraud and deception will help protect legitimate U.S. businesses from dishonest competitors, as well as the reputation of the U.S. marketplace. Cooperation is also necessary to engender reciprocity: FTC action to protect foreign consumers from fraud and deception emanating from U.S. businesses increases the willingness of foreign governments to cooperate in protecting U.S. consumers from fraud operators in their countries.

II. THE FTC'S EFFORTS TO FIGHT CROSS-BORDER FRAUD AND DECEPTION

Despite the enforcement difficulties outlined above, the FTC has continued to fight cross-border fraud and deception within the existing legislative framework, through its enforcement and policymaking initiatives. On the enforcement front, in 2002, the FTC brought approximately 20 new federal district court lawsuits involving one or more foreign defendants or foreign consumers, and continued to litigate and settle dozens of other cases involving fraud and deception that operate across national borders. In the first quarter of 2003 alone, the FTC filed new cases involving advance-fee credit cards peddled by Canadian telemarketers,[28] allegedly bogus international driving licenses advertised through spam email by defendants in Denmark[29] and other foreign countries including Israel, the Bahamas, and Romania,[30] and products and programs sold over the Internet by defendants based in Switzerland,[31] Canada, the U.K., and Mexico,[32] that allegedly falsely claim to cure cancer, AIDS, and other serious diseases. Although we were successful in these cases, we encountered difficulties, as outlined above.

In addition to its ongoing work on investigations and cases, in October 2002, FTC Chairman Timothy J. Muris unveiled a Five-Point Plan for Fighting Cross-Border Fraud.[33] The Plan recognizes the importance of initiatives on both the international and domestic fronts and the need for action by both the public and private sectors. Highlights of the Plan follow:

Developing an OECD Recommendation on Cross-Border Fraud: FTC Commissioner Mozelle Thompson has led the United States delegation to the Organisation for Economic Cooperation and Development's Committee on Consumer

---

U.S. under state law, but most of our trading partners do not usually grant the same treatment to U.S. judgments.").

[27] Prepared Statement of the Federal Trade Commission, *Cross-Border Fraud: Improving Transnational Law Enforcement Cooperation: Hearing Before the Permanent Subcommittee on Investigations of the Senate Committee on Government Affairs,* 107th Cong. (June 15, 2001).

[28] *FTC v. STF Group Inc.,* Civ. A. No. 02 C 0977 (N.D. Ill. filed Feb. 10, 2003), *available at* <http://www.ftc.gov/opa/2003/02/medplan.htm>; *FTC v. Assail, Inc.,* Civ. A. No. W03CA007 (W.D. Tex. filed Jan. 9, 2003), *available at* <http://www.ftc.gov/opa/2003/02/assail.htm>.

[29] *FTC v. Carlton Press, Inc.,* Civ. A. No. 03-CV-0226-RLC (S.D.N.Y. filed Jan. 10, 2003), *available at* <http://www.ftc.gov/opa/2003/01/idpfinal.htm>.

[30] *FTC v. Mountain View Sys., Ltd.,* Civ. A. No. 1:03-CV-OOO21-RMC (D.D.C. filed Jan. 7, 2003), *available at* <http://www.ftc.gov/opa/2003/02/fyi0314.htm>.

[31] *FTC v. Dr. Clark Research Ass'n,* Civ. A. No. 1:03CV0054 (N.D. Ohio filed Jan. 8, 2003), *available at* <http://www.ftc.gov/opa/2003/01/drclark.htm>.

[32] *FTC v. CSCT, Inc.,* Civ. Action No. 03 C 00880 (N.D. Ill. filed Feb. 6, 2003), *available at* <http://www.ftc.gov/opa/2003/02/csct.htm>.

[33] *See* Timothy J. Muris, "The Interface of Competition and Consumer Protection," Prepared Remarks at the Fordham Corporate Law Institute's Twenty-Ninth Annual Conference on International Antitrust Law and Policy (Oct. 31, 2002), *available at* http://www.ftc.gov/speeches/muris/021031fordham.pdf.

Policy since 1998 and has chaired the Committee since 2002. Under his leadership, the OECD issued Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders in June 2003. The Guidelines recognize that combating fraud and deception is an important priority for government consumer protection agencies. They represent the consensus of 30 countries on the importance of international cooperation to combat fraudulent and deceptive commercial practices. The Guidelines also provide impetus for legislative and policy reform in OECD countries for combating such practices.

Public-Private Partnerships to Combat Cross-Border Fraud: The FTC has issued a call to legitimate industry to help fight cross-border fraud, which hurts consumers as well as legitimate businesses. In many cases, domestic and foreign third parties, such as credit card issuers and networks, banks, and Internet service providers, can assist law enforcement by providing information about foreign fraud operators. Domestic third parties may be able to suspend domain names, telephone services, mailing services, or financial services to foreign fraud operators, who we may not be able to reach through court orders. Earlier this year, the FTC held a public workshop to explore these issues.[34] We are continuing to work with the private sector to follow up on some of the ideas discussed at the workshop, including better sharing of information between the private sector and the FTC. Discussions at the workshop also highlighted obstacles to public-private sector cooperation to combat cross-border fraud, which some of our legislative proposals seek to overcome, as explained further below.

Technical Assistance: The FTC wants to ensure that developing countries do not become havens for fraud. Therefore, we have conducted training missions on consumer protection issues in various developing countries, in cooperation with and funded by the U.S. Agency for International Development. Last year, we conducted training sessions for consumer protection authorities from 13 Eastern European countries. This year, we are conducting training sessions in Peru, Romania, and the Ukraine.

Developing and strengthening bilateral and multilateral relationships: The FTC has undertaken several activities in this area:

- The FTC has signed consumer protection cooperation agreements with Canada, the United Kingdom, and Australia, that have enhanced our cooperation with these countries.[35] We are continuing to expand our law enforcement activities with these countries.
- In Canada, the Commission participates in two consumer protection enforcement task forces: *Project Emptor* with British Columbia authorities, and the *Toronto Strategic Partnership* with a wide variety of Canadian and U.S. authorities.[36] In the past year, the FTC has announced numerous joint law enforcement actions taken with the assistance of these task forces, including actions involving credit card loss protection,[37] lottery/prize scams,[38] advance-fee credit cards,[39] and bogus cancer clinics.[40] Just this week, the FTC's Bureau of Consumer Pro-

---

[34] *See* <http://www.ftc.gov/bcp/workshops/crossborder/index.html>.

[35] See Agreement Between the Government of the United States of America and the Government of Canada Regarding the Application of their Competition and Deceptive Marketing Practices Laws, Trade Reg. Rep. (CCH) ¶13,503 (1995), *available at* <http://www.usdoj.gov/atr/public/international/docs/uscan721.htm>; Agreement Between the Federal Trade Commission of the United States of America and the Australian Competition & Consumer Commission On the Mutual Enforcement Assistance in Consumer Protection Matters (July 20, 1999), *available at* <http://www.ftc.gov/opa/2000/07/usaccc.htm>; Memorandum Of Understanding On Mutual Enforcement Assistance In Consumer Protection Matters Between The Federal Trade Commission Of The United States of America And Her Majesty's Secretary of State for Trade And Industry And The Director General Of Fair Trading In The United Kingdom (Oct. 31, 2000), *available at* <http://www.ftc.gov/opa/2000/10/ukimsn.htm>.

[36] For a further discussion of these task forces, see Mass-Marketing Fraud: A Report to the Attorney General of the United States and the Solicitor General of Canada 31-32 (May 2003), available at <http://www.usdoj.gov/opa/pr/2003/May/remmffinal.pdf>; see also Prepared Statement of the Federal Trade Commission, Cross-Border Fraud: Improving Transnational Law Enforcement Cooperation: Hearing Before the Permanent Subcommittee on Investigations of the Senate Committee on Government Affairs, 107th Cong. (June 15, 2001).

[37] *FTC v. STF Group,* Civ. Action No. 03 C 0977 (N.D. Ill. filed Feb. 10, 2003), *available at* <http://www.ftc.gov/opa/2003/02/medplan.htm>.

[38] *FTC v. Duraisami,* CV 03-01284-BJR (W.D. Wa., filed June 13, 2003), *available at* <www.ftc.gov/opa/2003/07/duraisami.htm>.

[39] *FTC v. Pacific First Benefit, LLC,* Civ. Action No. 02 C 8678 (N.D. Ill. filed Dec. 2, 2002), *available at* <http://www.ftc.gov/os/caselist/ca02c8678.htm>.

[40] *FTC v. CSCT, Inc.,* Civ. Action No. 03 C 00880 (N.D. Ill. filed Feb. 6, 2003), *available at* <http://www.ftc.gov/opa/2003/02/csct.htm>.

tection announced its participation in a new task force with authorities from Alberta, called the Alberta Partnership Against Cross-Border Fraud.

- The FTC is a member of the International Consumer Protection Enforcement Network (ICPEN), a group of consumer protection enforcement agencies from 32 countries that meets twice a year to discuss cases, investigation techniques, and other information. Seventeen ICPEN countries plus the OECD participate in *econsumer.gov,* a public website where consumers can file cross-border e-commerce complaints online, making them accessible to law enforcement agencies in the member countries. The site is available in English, French, Spanish, and German.[41] Complaints from econsumer.gov can help the FTC identify trends and wrongdoers on an international level.

In addition, the Five-Point Plan recognizes that, although there are certain activities the FTC can undertake within our existing legislative framework, new legislation is necessary to help combat the problem of cross-border fraud effectively. The remainder of this testimony focuses on the Commission's legislative recommendations.

III. LEGISLATIVE RECOMMENDATIONS

Despite our successes, we face daunting challenges in the battle against cross-border fraud and deception. Many of these challenges reflect the shortcomings of a legal framework developed when consumer protection was almost purely a domestic concern. In the emerging global marketplace, that framework must be expanded to allow the FTC to act with effectiveness and dispatch to protect American consumers. In testimony to Congress during hearings on spam, the Commission also emphasized the need for improvements to the FTC's law enforcement powers to combat cross-border fraud and deception perpetrated through spam.[42]

Indeed, an international consensus has developed on the need for countries to improve their domestic framework for fighting cross-border fraud and deception. The OECD Guidelines discussed above specifically provide that "[m]ember countries should review their own domestic frameworks to identify obstacles to effective cross-border co-operation in the enforcement of laws designed to protect consumers against fraudulent and deceptive commercial practices, and should consider changing domestic frameworks, including, if appropriate, through adopting or amending national legislation to overcome these barriers."[43] The FTC's legislative proposals would implement this provision. Even though new legislation would not solve all of the problems in fighting cross-border fraud, it could go far to reduce some of the obstacles we face.

The FTC is proposing legislation in four areas:

- **First, the FTC is seeking to strengthen its ability to cooperate with its foreign counterparts, which are often investigating the same targets as the FTC.**

We are currently prohibited by statute from sharing certain information we obtain in our investigations with our foreign counterparts. This prohibition can hurt U.S. consumers. For example, even if both the FTC and a Canadian consumer protection agency are investigating the same Canadian telemarketer that is defrauding U.S. consumers, in many cases, the FTC cannot share information it obtains pursuant to its main investigatory tool, the Civil Investigative Demand (CID), with the Canadian agency. This is true even though a Canadian action against the cross-border telemarketer would benefit U.S. consumers.[44] Similarly, in one recent case, the FTC obtained an order against a spammer defrauding U.S. consumers and found that the spammer had an affiliate that was perpetrating the same scam from a foreign country, targeting both U.S. and foreign consumers. The FTC cannot share the information it obtained pursuant to a CID with its foreign counterpart. The changes we are seeking would allow us to share such information and provide investigative assistance to certain foreign agencies in appropriate cases.

---

[41] *See* www.econsumer.gov.

[42] Prepared Statement of the Federal Trade Commission, *Spam (Unsolicited Commercial E-Mail), Before the Senate Committee on Commerce, Science and Transportation,* 108th Cong. (May 21, 2003).

[43] OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders C(2003)116 (June 11, 2003).

[44] The Commission cannot disclose "documentary material, tangible things, reports or answers to questions and transcripts of oral testimony" that are "received by the Commission pursuant to compulsory process in an investigation" without the consent of the person who submitted the information, except as specifically provided. 15 U.S.C. § 57b-2(b)(3)(C); 16 C.F.R. § 4.10(d).

- **Second, the FTC is seeking to improve its information-gathering capabilities.**

The key to combating cross-border fraud successfully is the ability to sue without tipping off investigative targets. Once notified of FTC action, targets in these types of cases often disappear and move assets offshore, beyond the reach of U.S. courts. Thus, we are seeking to improve our ability to obtain more information from third parties without requiring advance notice to our investigative targets.

Currently, we have no mechanism to require most third parties to keep CIDs confidential. Many third parties have told us that they will provide notice to the target before they will share information with us, sometimes because they believe notice may be required and sometimes even if such notice clearly is not required by law. Because of this concern, we often do not send the CIDs, thus losing a potential source of information in FTC investigations. We would like to be able to seek court orders requiring third parties to keep CIDs confidential for a finite period of time, which would improve our ability to gather information. This recommendation carefully balances law enforcement interests with privacy interests. In all cases in which we want a mandate that third parties keep CIDs confidential, we would be required to seek a court order, and the confidential treatment would be temporary. To further improve our ability to gather information, we also are seeking improvements in our ability to gather more information from federal financial regulators and foreign law enforcement agencies.

- **Third, the FTC is seeking to improve its ability to obtain consumer redress in cross-border cases by clarifying its authority to take action in such cases, and expanding its ability to use foreign counsel to pursue assets offshore.**

depriving wrongdoers of their ill-gotten gains, reducing the incentives to engage in fraud. To the extent that money can be returned to consumers, it reduces their injury and increases their confidence in law enforcement. Among the changes the Commission is recommending is a provision clarifying that the Commission has the authority to take action in appropriate cross-border cases and provide restitution to both U.S. and foreign consumers injured by cross-border fraud and deception. By clarifying the availability of remedies, Congress can protect Americans from foreign fraud operators and prevent the United States from becoming a haven for fraud artists targeting victims abroad. It also can send a strong signal to foreign courts considering whether to enforce an FTC money judgment when there are foreign as well as U.S. victims.

Moreover, the Commission increasingly is facing significant obstacles in obtaining the proceeds of fraud and deception from defendants who have assets abroad, beyond the reach of U.S. courts. The Commission therefore also seeks to target more resources toward foreign litigation to facilitate recovery of offshore assets to benefit defrauded U.S. consumers.

- **Finally, the FTC is seeking to strengthen its international cooperative relationships by obtaining authority to conduct staff exchanges and to provide financial support for certain joint projects.**

The FTC participates in many international projects to combat cross-border fraud, including the International Consumer Protection Enforcement Network (ICPEN), the Mexico-U.S.-Canada Health Fraud Task Force (MUCH), Project Emptor with various British Columbia authorities, and the Strategic Partnership with various Ontario authorities. The FTC also consults with foreign counterparts at bilateral and multilateral meetings. Often, it would be helpful for the FTC to provide monetary assistance to support cooperative projects and meetings of such groups. Currently, various appropriations statutes prohibit the FTC from using appropriated funds to pay any expenses of a Commission, council, board or similar group that does not have a prior and specific statutory approval to receive financial support.[45] The FTC's legislative proposals seek to overcome this restriction.

Congress has already provided many of the tools that we seek to agencies such as the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC). For example, thirteen years ago, Congress expanded the SEC's powers to cooperate with foreign authorities.[46] At the time, the SEC faced issues analogous to those faced by the FTC today regarding the growth of international fraud and deception in electronic commerce:

---

[45] *See* Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, Division J—Treasury and General Appropriations, Title VI, § 610, 117 Stat. 11, 465 (codified at 31 U.S.C. § 1345).

[46] Securities Acts Amendments of 1990, Pub. L. 101-550 (1990).

> The internationalization of the world's securities markets is a trend that is likely to continue at a rapid pace. The major forces driving this trend appear to be: rapid technological advances in communications and computer technology [and] the growing economic interdependence between the U.S. and its major trading partners . . . Therefore, securities regulators in each nation must work with their foreign counterparts to seek coordinated international solutions to assure fairer as well as more efficient market operations across borders.[47]

Since 1990, the SEC has been granted statutory authority to gather and share relevant information with its foreign counterparts. As a result of these statutory provisions, the SEC can offer significant benefits to those foreign authorities seeking reciprocal cross-border cooperation. Indeed, the SEC has signed Memoranda of Understanding (MOUs) with over 30 foreign agencies. These MOUs significantly streamline cross-border cooperation and, in some cases, has led to helpful information-sharing legislation in other countries.[48] Congress has given the CFTC similar powers and mechanisms for cooperation with foreign authorities.[49] Through our legislative proposals, we are requesting similar authority.

We have consulted on our recommendations with other federal government agencies, including the Department of Justice, Department of State, the Federal Reserve Board, the Office of the Comptroller of the Currency, the SEC and CFTC, as well as several private companies and public interest groups, including the National Consumers League, the Electronic Privacy Information Center, and Center for Democracy and Technology. We are working closely with these entities in fashioning the legislative provisions, both to meet their concerns and to achieve our objectives.

The Commission greatly appreciates the opportunity to provide this information to the Subcommittee. We look forward to continuing to work with Congressional staff on our legislative proposals.

Mr. STEARNS. Thank you, Mr. Chairman. I think I will start with my questions. Obviously from your opening statement, it is a very high priority, this proposed legislation combating cross-border fraud.

And I guess that you and your staff, let's say, after listening to you talk about the spam that it is probably right up to one of your highest priorities. Would you not agree?

Mr. MURIS. Yes. The FTC has become the premier government agency for fighting fraud. One of the reasons that you needed a Federal agency is that fraud has always crossed State borders, and now fraud increasingly crosses international borders.

There is no higher priority that we have than fighting fraud. There is no higher legislative priority than this particular piece of legislation. And more and more of the fraud is done through spam.

This is anti-spam legislation. Spam is an international problem. It is a growing problem, and it is swamping our e-mail. It is threatening. As another one of my colleagues, Commissioner Swindle, likes to say, spam is threatening to kill the killer app of e-mail. We really need lots of help, including the other spam legislation on which you are working.

Mr. STEARNS. Let me go to some of the areas since we passed the Patriot Act, and a lot of people are concerned. What do you think of the argument that as there is no requirement for dual-criminality in the proposed legislation that will chill speech protected under the First Amendment, and nullify the probable cause requirement of the Fourth Amendment, would you care to comment on that?

---

[47] H.R. Rep. No. 101-240 at 2-3 (1990), *reprinted in* 1990 U.S.C.C.A.N. 3889-3890.

[48] *See generally* Michael D. Mann & William Barry, *Developments in the Internationalization of Securities Enforcement,* 136 PLI/Corp 1999 (May 2002).

[49] H.R. Conf. Rep. No. 978, 102d Cong., 2d Sess. 70-71 (1992).

Mr. MURIS. Sure. Let me leave the Patriot Act issue aside for just a second, and focus on the concern that we would be involved in investigating activity that is legal in the United States, particularly under the First Amendment.

We think that we have limited the bill since it was originally proposed and we think some further changes would be helpful to address this issue. First of all, the bill is limited to fraudulent and deceptive commercial practices, or other practices substantially similar to practices banned by the FTC laws.

I think that is a touchstone. Again, the touchstone is fraud. Now, one of the things that I think is important to understand is that across the world, people who are looking at fraud, they don't necessarily have agencies like ours.

Indeed, if you look at across the whole world, the only agency that maps us precisely is Australia.

Mr. STEARNS. So in all of the European Union, they don't have a——

Mr. MURIS. Well, many places in the European Union, they don't follow the FTC model. They don't have necessarily consumer protection agencies. A lot of this is left to criminal authorities.

Now, the European Union, I think positively through Brussels is moving to have more concern about cross-border fraud. They are moving to implement this OECD recommendation that I mentioned, but it is important that I think that the legislation be written so that the touchstone is fraud and deception, or "substantially similar" conduct.

Since we sent proposed legislation to the Hill, we have supported such changes. I think a second point that is important to make is that we have discretion.

We certainly do not have to provide assistance. We would not provide assistance if it wasn't involving with the touchstone of fraud and deception, or substantially similar conduct.

In terms of assistance, the way the legislation is drafted, is that we would need to consider consumer injury. Again, that is the touchstone of what we do. So the bottom line is that I think the concern is absolutely legitimate that we not be involved in helping people overseas prosecute conduct that would be legal in the United States.

And we think that the bill as was originally proposed has some potential problems in it, and we think we have worked to address those. We think a few other changes could be helpful as well.

Mr. STEARNS. How do you respond to the observation that the delayed notice provision is too broad, and therefore should be stricken to ensure due process rights for individuals?

Mr. MURIS. Well, I think originally there were again some legitimate concerns about delayed notice. I think some additional changes could be helpful there as well. For example, the provision was written as requiring the judge to issue the delayed notice.

I think it would be better to leave it in the judge's discretion. This is an issue that raises many points about the Patriot Act, and I will now address those. We don't do criminal law. We don't do search and seizure. We don't detain suspects.

We would need a court order for this delayed notice. The delayed notification——

Mr. STEARNS. I agree with you that there is no comparison, but people as a metaphor are going to say here we go, and I just think it is important in this hearing to explore those to make sure that there is no comparison here at all.

Mr. MURIS. Well, absolutely, plus we have a time limit, and I think it would be useful to add that the 90 day's extensions could not exceed 1 year under the statute. I think that would be a useful change.

Again, I think the concerns that people are raising are legitimate, and I think we can address them. I think the Patriot Act is a metaphor and does not apply here. I am not obviously an expert on the issues surrounding the application of the Patriot Act, but whatever those concerns are—and I know that people disagree—I don't think they apply here.

This statute as written has a specific requirement to show that the acts are related to fraud and deception. There is a very similar process that already exists and has existed for many years for the SEC and the banking agencies. I don't think there have been a lot of problems with that.

So I really think that we can have a delayed notification provision that makes sense. Let me just back up and mention why it is so important to have this. We are dealing with fraudsters or people who commit or who are engaged in fraudulent spam.

When we seek information about them from third-parties, if the third-parties feel that they have to notify the targets of our investigation, well, the assets that they have, and maybe the parties themselves, are going to disappear.

That is why we need a delayed notification. With ISPs, for example, and spam—this is covered in some different aspects of the proposed legislation—there are ISPs who feel that when we contact them about fraudulent spam that they need to try to contact the target.

Obviously that deters us from trying to get information from them, and from them being the ISPs, about these targets. It does not make any sense that we can't have a provision subject to court supervision, and subject to the requirements that I mentioned, where we can have delayed notification.

Mr. STEARNS. Let me just ask one quick question. You are going to make the information that you collect available to other governments. So people are going to say is it necessary for the FTC to disclose this information to other governments, and are there safeguards that must be established if it is disclosed for the protection of privacy.

So that is just a broad comment, and so if we could answer that, then I think we have sort of taken care of some of the main concerns here.

Mr. MURIS. I think those concerns are legitimate. What we found in working with our law enforcement partners around the world is that they will give us information and engage in reciprocal arrangements if we can promise them confidentiality.

They will give us the information on condition often of confidentiality. The way that the law is right now is that even if we are investigating the same target, and say with the Canadians. We have a lot of telemarketers in Canada who are targeting U.S. consumers.

The Canadians have on their own done what I think is a very commendable thing. They don't want Canada to be a haven for cross-border fraud, even though the fraud is aimed more at the United States than at the Canadians.

But we are limited in our ability to share information and to receive information from the Canadian law enforcement partners. This bill would allow us to do that, and I think with appropriate safeguards.

Mr. STEARNS. I thank the chairman, and the gentle lady, Ms. Schakowsky.

Ms. SCHAKOWSKY. Yes, I would like to yield if he would like to the ranking member on the committee for a statement.

Mr. DINGELL. Thank you for your graceful kindness to me. I have already inserted a statement into the record through the kindness of the committee. I would like to welcome the chairman of the Federal Trade Commission here, Mr. Chairman. Thank you for being with us.

We look forward to working with you. You are addressing a very important matter, and I am pleased to see that the Federal Trade Commission is proceeding vigorously to address a matter of real concern and growing concern to Americans. I thank my colleague, and I thank you, Mr. Chairman.

Ms. SCHAKOWSKY. Thank you. It is really the same areas that I wanted to explore and just get some clarity on the dual criminality issue, for example. You are seeking language that specifically states that "a violation of Federal law is not required for the Commission to render assistance to a foreign law enforcement agency." Is that right? Is that still the language that we are working with?

Mr. MURIS. I actually think that we could strike that specific language, because the additions that we have proposed in terms of tying it to fraud and deception, or "substantially similar" conduct. I think with those additions it will adequately protect us.

I think the language that you are talking about is unnecessary and in some ways unnecessarily provocative. I would note just one more thing, that these limits which I think are good and appropriate, are limits that the SEC, and the antitrust laws, and other laws, don't have. But I think that we can work with them, and I don't think that they are a problem.

Ms. SCHAKOWSKY. Good. I would certainly feel more comfortable without those particular words, but nonetheless, are there examples of information where there has been no violation of U.S. law, and maybe in another country they would consider—well, why was it there in the first place? What are we thinking about in that instance?

Mr. MURIS. Sure. Here is the problem. The problem is that when you first start an investigation, you don't know precisely what the issues are and what he violations are, and because there are so many different laws that don't exactly match up with ours.

We want the touchstone to be fraud and deception and "substantially similar." For example, there is spam legislation, and there will probably be spam legislation here, and besides this, more specific spam legislation overseas.

They might not precisely match up, even though they are essentially aimed at the same thing. The spam legislation might talk about deceptive headers in one place, and it might talk about it slightly differently in another place.

So even at the end of the day, where you might be going after precisely the same conduct and it is illegal in both places, particularly at the beginning, it is not going to be exactly clear that they match up precisely.

So we think that rather than have the broader discretion that the SEC and other people have, if we say fraud and deception and "substantially similar" conduct, we think that addresses the concern and should avoid problems.

Ms. SCHAKOWSKY. Okay. You talked about the need for confidentiality. Give me an example of new authority in terms of confidentiality that this would offer.

Mr. MURIS. We have some interesting problems particularly when we deal with foreign criminal authorities. Since we are not a criminal authority, they would like certain assurances out of us.

For example, one thing that is related to your question is that they often won't cooperate with us and share information unless we have something explicit that says that we can make criminal referrals, because that triggers their ability to share information with us.

They also are concerned about giving us confidential information if it would be subject to release under our Freedom of Information Act. I can't overstate that if we are going to deal with spam and deal with cross-border fraud, we need cooperation from foreign authorities, and we need this legislation to get that.

We are the biggest economy in the world, and we are going to benefit many times over in a world of reciprocity, because everyone essentially wants to sell in the United States.

There are going to be many more people, and there are going to be many more times when we benefit from the reciprocity than other people benefit. The Canadian example is an excellent one. Canadian consumers are not the ones who are primarily harmed. It is American consumers.

But the Canadians do not want the reputation of being a haven for cross-border fraud, and we are limited in our ability to cooperate with them right now. Under this legislation, it would be easier for us to cooperate with them, and that is going to be mutually beneficial. But it is American consumers who are the primary targets.

Ms. SCHAKOWSKY. And clearly that is the goal of this legislation, but the FOIA exemption, for example, could it not give broad exemption to banks and other financial institutions to share confidential information about their customers at their discretion?

Mr. MURIS. Again, This is not open-ended fishing expeditions. We need and we have rewritten the proposals from what we originally proposed, and we have a few more suggestions to tie it directly to the touchstone of fraud and deception.

On the delayed notice, I mentioned giving courts discretion is important. On the FOIA, I think that a law enforcement exception is appropriate. It is well recognized. It has existed for years.

We just need to make sure that it applies in this particular context, because quite frankly when people were writing these laws in terms of the Federal Trade Commission, we didn't have a cross-border problem. We didn't have an Internet.

What happened with the telemarketers is that in the United States, with various States and various law enforcement officials, we really cracked down on fraudulent telemarketing in the United States.

Well, lo and behold a lot of them relocated to Canada, and when people drafted these various laws, including FOIA, and including the laws that deal with us, they didn't have this in mind. So we are really completely consistent with the original principles of law enforcement exceptions for FOIA.

Ms. SCHAKOWSKY. Thank you.

Mr. STEARNS. I thank my colleague. The gentleman from Illinois.

Mr. SHIMKUS. Thank you, Mr. Chairman. Tim, again, it is good to see you and have you here. We are wrestling here in the national arena with the Patriot Act, and this relationship between how do you enforce the laws, and how do you get agencies to talk to each other, and also international agencies, international law enforcement with our law enforcement.

And I think that is part of the challenge, and what is admissible, and what is not admissible. So this is very similar to that whole debate. A lot of the witnesses, or some of the witnesses in the next panel will talk about civil liberty concerns with the bill.

And I am hoping that you can address some of those for me, and explain what is the reasoning for the Freedom of Information Act exemptions.

Mr. MURIS. Let me just talk at a broader level, and then come down to specifics. We have a serious problem in dealing with fraud. As a law enforcement agency, we need to be able to cooperate in the same way that we cooperate with domestic agencies. We need to be able to cooperate with our foreign counterparts, and that is really all we are asking.

Whether it is a domestic setting, or a foreign setting, there are obviously concerns about the powers of the government. I understand those concerns. I think that our track record as an agency is excellent. We are a small agency with limited resources.

We have virtually no reputation for going on wild goose chases, and we are going after people who are fraudsters. Essentially all we are asking is to have the same kinds of abilities as many other agencies have to cooperate and share information subject to that information not becoming public.

The same cooperation that we have with domestic officials, we want to have that with foreign officials. I think in general that some of the concerns raised were legitimate, and in working with the staffs, and working with the Senate, we have proposed lots of changes to address those concerns, because indeed I think they are legitimate.

Mr. SHIMKUS. And you know that one of our primary roles is to have oversight of the Federal agencies that we have jurisdiction of. Do you think or don't you think—I mean, I do—that there probably should be some reporting requirements to us so we can perform our oversight role?

Mr. MURIS. Absolutely, and that was something that we didn't have in the original proposal. People have raised that, and I think that is a good idea. It is going to take 3, 4, or 5 years to get some experience. So I think it would be better to have an initial 3-year reporting requirement, over 3-year cycles.

I think that will give us a real opportunity to gather experience and to explain the experience. We are on a steep upward curve here in cooperation internationally and learning how to cooperate internationally.

We are trying emulate in some ways what has happened internationally on price fixing. Congress has given a lot of this authority, in terms of dealing with international cartels and price fixing.

In the last several years, there has been excellent enforcement, and some important cases pursued. We are trying to emulate that experience with cross-border fraud. We are several years behind, but this legislation would be extremely helpful.

Mr. SHIMKUS. Thank you, Mr. Chairman, and I yield back my time.

Mr. STEARNS. Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman. Mr. Chairman, I ask that my statement be made part of the record.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. STUPAK. Thank you.

Mr. Chairman, Federal Trade Commission records show that about 46 percent of the complaints of cross-border fraud originate from Canada, and so I am trying to ask some questions along those lines on this cross-border fraud.

Some of the members have brought it up earlier, but what protections would there be in place, and I know that we have some proposals from the FTC there to combat this cross-border fraud, but what protections would be in place to limit the disclosure of private consumer information to foreign governments, and what protections will exist to limit the foreign government's use of that information?

Mr. MURIS. First of all, let me just describe what we do domestically. I think we have an excellent track record. We cooperate with other Federal agencies, with State Attorney's General, with local law enforcement authorities, obviously with U.S. Attorneys.

What we are proposing is to be able to engage in the same sorts of cooperation. The most important safeguards are in terms of the touchstone; that we are dealing with fraud and deception. There are obviously a lot of legal requirements that are imposed upon

government officials, in terms of ethical and other requirements about what they can do.

There is a concern that we not be used to investigate conduct that is legal under U.S. law. I think that is a legitimate concern. I think various changes in the statute, in the draft since it has been proposed, would address that.

Including that we would have a lot of discretion. In terms of delayed notification, which is very important to us because we need to get information about people who we think are engaged in spam or other fraud, and we don't want them to be notified.

We think that additional safeguards like discretion on the part of the judge would be useful. So I can't over-emphasize enough that we already are engaged in enormous cooperation with law enforcement agencies and have been for a long time within the United States.

Because the problem is migrating, particularly to Canada as you mentioned, and because these people are targeting U.S. consumers, we are asking for the same kinds of ability to cooperate with the same kind of protection with people outside of the United States.

Mr. STUPAK. Well, let me ask this question, and is the FTC then really the agency that should be handling this? Do you work with the State Department since we have sort of like foreign countries involved?

You mentioned that domestically that you work with State Attorney Generals, like the State Attorney General of Michigan, and since we border Canada, should they be involved in this? Do we have the right agency here in doing this?

Mr. MURIS. Well, we are the primary agency in the Federal Government that deals with consumer fraud. Now, quite frankly, I am happy to get more agencies involved. We are hoping to get more criminal enforcement. We put an emphasis on criminal enforcement.

We have several U.S. Attorneys working with us on investigations of spam, for example. I think you need a Federal coordination agency with enforcement authority, and that's us. Obviously in terms of the State of Michigan, we work closely with that State, and with other States that border Canada.

They are obviously quite interested in this. Of course, the telemarketers are telemarketing all over the United States. Just in terms of telemarketing, for example, since the telemarketing sales rule went into effect about 8 years ago between the States and the Federal Trade Commission, we have brought something like over 1000 cases.

We work closely together and the coordination function is important, and that is what we do.

Mr. STUPAK. Should there be pressure from the State Department to put more—well, I hate to use the word pressure, but to at least discuss it with Canada? It sounds like if we can drive them out of this country, and they just go north to Canada, whatever pressures we use to get them out of our borders and send them elsewhere, couldn't those same pressures be used in Canada, and use a cooperative approach to try to drive them out?

Mr. MURIS. Well, in fact that is what we are doing, and that is why we need this law, because we are hindered—the kind of cooperation that we engage in with the State of Michigan and with the U.S. Attorneys, we can't do all of that with the Canadian officials.

The Canadians—and again to their credit, these are companies targeting, or mostly targeting, U.S. consumers, and the Canadians do not want to become a haven or known as a country where they have these people attacking the United States.

Mr. STUPAK. Right.

Mr. MURIS. They are working with us and this legislation will allow us better to be able to work with them. If we are investigating the same target, we can engage in the kind of information sharing that we can with the Attorney General of Michigan.

Mr. STUPAK. Well, a lot of telecommunications companies, especially telemarketers, are in India. If we pass this legislation, would it help you, whether it is Canada, India, or wherever it may be?

Mr. MURIS. Absolutely. Unfortunately the problem is growing and it is only going to get worse. The problem of the Internet is a problem. The Internet has had tremendous benefits, but it has also opened up the potential to do fraud over the Internet.

If we are going to seriously attack fraud, we need legislation to allow us to deal with a cross-border problem, because quite frankly more and more of it is becoming cross-border.

Mr. STUPAK. Well, maybe I should be talking to you about my drug law, and I am trying to get the FDA to crack down on these Internet sales, and it has been 5 years, and they won't even give us a yes or a no on my legislation. Maybe I ought to come to the FTC. Thanks.

Mr. MURIS. Thank you.

Mr. STEARNS. I thank the gentleman. Mr. Issa, the gentleman from California.

Mr. ISSA. Thank you, Mr. Chairman. Commissioner, I've only got a couple of questions, and perhaps as time goes on some of the others will be answered, and so I won't ask too many. But if I understand correctly, your proposal would result in a year of delayed notification.

Mr. MURIS. Yes, but again, I think we should change the language from where the judge has to do it, to where it is in the judge's discretion. That is a legitimate point that people have made, and let me just give you the context again.

For example, I mentioned the ISPs and spam. We go to some ISPs right now. We know it is spam, and they know it is spam, and they feel that they have to try to contact the target of our investigation. That doesn't make any sense to me, but they read certain laws that way, and we are asking that the law be changed so that we can get information from them without scaring our target away.

We try to get money back for consumers. Well, once the target gets a hint of what we are doing, the money, not surprisingly, disappears.

Mr. ISSA. And I appreciate that. I guess being a Californian and being aware of the dot.com year which started off as one quarter, and then become 1 month, and some would say became a week, I am a little incredulous that we would allow spamming to go on for a year.

It seems like an inordinately long period of time in what is an almost instantaneous business, and one in which movement and reorganization, et cetera, would go on. Would you conceivably allow for a much shorter period of time, before you would have to go back and renew on, let's say, a monthly basis with a Federal Judge? I am very concerned that saying, look, we just sort of have this 1 year guideline, is about 12 times longer than I would think would be necessary.

Mr. MURIS. Here is the problem. First of all, the renewal that we are talking about would be in essence in 90 day increments. The problem is we can't find these people right now, even domestically, and finding them—the spammers may move on, but it is often the same spammers and the same sellers.

We have to issue—we call them CIDs, but they are subpoenas essentially. We have to issue 10 or 15 subpoenas sometimes just to track somebody at all. You can't track them directly over the Internet because of the anonymity. You have to follow the money.

So even though they have moved on in real time, if we are going to deal with these people, our investigations have to take a long time. Internationally, unfortunately, a year is not very long. Obviously if our experience is that—one of the reasons that the report function would be so useful would be that we would be able to track some of this.

But I think that 90 day increments is not long at all. I am a Californian myself. I grew up in San Diego, and we originally——

Mr. ISSA. Hi, neighbor.

Mr. MURIS. We recently brought a case involving so-called "phishing." It involved a juvenile in California who was spaming and claiming that he was—I think it was AOL, and he stole hundreds of identities of people, and he would charge to their credit cards. It took us a long time to track that down.

Mr. ISSA. Was he still a juvenile when you were done?

Mr. MURIS. Yes.

Mr. ISSA. Too bad. And following a slightly different path, what are the foreign government entities with which you would share and what would be the control on personal information?

Would you be willing to be specifically limited in sharing to that same judge that issued the subpoena? In other words, not all countries, all entities, are equally trustworthy. We could specify off the top of our heads on those Canadian entities that are our counterparts, and the protections are somewhat similar.

But I have no idea who you share with in India and what the impact would be. Is that something that you envision specific oversight by the subpoena power on or some other agency?

Mr. MURIS. There are a couple of things there. The original proposal that we made was probably too broad, and we in working with people have cut it back. It is clear that we need to have discretion in how we are sharing, and we need to have guidelines.

Again those are changes that we have made as people have raised these legitimate concerns.

The guidelines that now are drafted, and which give us discretion, tell us the things that we need to be worried about. We need to be worried about consumer injury. We need to be worried about that we are dealing with fraud and deception, or "substantially similar" conduct.

I think that those guidelines are tighter than they were originally and I think they are appropriate. I think obviously that we need to have a little experience, and then Congress could evaluate to see if they want to broaden them, or tighten them.

Mr. ISSA. Thank you. Thank you, Mr. Chairman, for holding this hearing, and obviously this is an important piece of legislation, and I appreciate you making this available to us.

Mr. STEARNS. I thank the gentleman. The gentleman from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman, and like my colleagues, I am glad that our subcommittee is holding this hearing. When I was first approached on the International Consumer Protection Act, I looked at it from the spam perspective, but I know that it is much bigger than that, simply because my colleague on the committee, Congressman Wilson and I, have been working for three sessions to pass anti-spam legislation. And we are working in our committee now to see if we can do it, and to empower the FTC to be able to be the enforcement agency.

And I know the concern that I have is that a lot of our States have passed very tough laws, but again spam comes across State boundaries as well as international boundaries, and my argument is that we need to do something here on spam, and empower the FTC. And again this International Consumer Protection Act will give you that ability to deal with our trading partners, whether it be Canada, or India as Mr. Issa said, or other countries that we work with on lots of other ventures, and of course we can do it on spam also.

You indicated that the legislation was needed to improve the international cooperation necessary to combat the cross-border fraud. Do your counterparts in other countries have this ability? I know that you answered that a little bit about the criminality of it.

But do other countries have the ability—and particularly in consumer issues, like spam, and unsolicited faxes, and things like that—to cooperate on an international level in the same or similar ways that you are seeking here?

Mr. MURIS. Well, that is an excellent question, and we are on a—what I would hope is a very steep increase in international cooperation, which will really be facilitated by the passage of this legislation.

We also have the various agreements with other countries, and the OECD recommendation which I mentioned, which was passed. It could not have been done without the unanimous agreement of the countries, but guidelines on cross-border fraud will I think encourage much greater cooperation.

I mentioned in a comment or a question from the Chairman that the European Union is moving more in this direction. I think the concern over spam is undoubtedly driving a lot of this, and I am hoping that we can emulate the cooperation that has just occurred in the last really 5 years on going after price fixing, and the antitrust problem of price fixing.

We can do the same thing with excellent international cooperation on fraud. Quite frankly passing this legislation will be a tremendous signal to our trading partners and to the other countries around the world that we are serious about this problem.

We have organized to a significant extent law enforcement agencies in the United States over the last couple of decades to attack the fraud problem. It is a problem that will always be with us, like theft or other problems, but we need to deal with it. We hope to be able to engage in the same kind of organization internationally.

Mr. GREEN. Mr. Chairman, I don't have any other questions, but I thank you, and hopefully we will be able to do a one-two punch not only in this legislation, but also the strongest anti-spam legislation that Congress can pass. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman. Mr. Terry.

Mr. TERRY. Mr. Chairman, I only have one short question. You had mentioned that you felt that it was a legitimate concern that the conduct needs to be illegal in the United States for you to become involved.

I agree with that, but if the conduct would be illegal in the United States, what are the barriers to cooperation with a foreign government like Canada? I guess what I am saying is what is the need for this type of a bill if the conduct is illegal here?

Mr. MURIS. Well, first of all, what I have said is in terms of the touchstone that we would like are fraud or deception, or "substantially similar" conduct, because the agencies overseas and countries overseas don't line up, even if they are going after the same practices, they don't necessarily line up with laws that read exactly like ours.

The problem is, and Canada is a perfect illustration, the telemarketers have set themselves up—such as many of the fraudulent telemarketers in Canada—to target U.S. consumers. We cannot cooperate with the Canadian authorities the same way that we can cooperate with domestic authorities. That is what we are asking, to be able to work with——

Mr. TERRY. What specifically though is preventing you from being able to cooperate? What in our laws, rules, regulations, or whatever, prevent you from cooperating, especially if it is illegal conduct here?

Mr. MURIS. There is a whole series of things that we cannot do. We cannot guarantee confidentiality of information. We can't share information outside the United States.

So both ways we have a problem. We have a problem getting foreign judgments enforced, which part of this legislation would address. There are courts that read our laws in ways that we think this legislation would fix, so that they would enforce a foreign judgment.

I mean, the simplest problems that I alluded to a second ago is that we can't share the information. There is a Canadian telemarketer, for example, targeting the United States. We can't share information we found through one of our subpoenas with the Canadian authorities.

If the Canadian authority makes a request to us, we can't investigate and help that Canadian authority, and give him the information back, even though the Canadian authority is trying to track down someone who is targeting U.S. consumers. The law prohibits us from taking all those steps that I have just mentioned.

Mr. TERRY. And that's where my confusion comes in, because we are all aware of at least on the criminal side that there is cooperation in investigations with other countries, and it does not seem to me that they are coming before us.

Maybe in Congress' past, they have given that type of specific authorization. Whereas, the difference that you are—your actions are only civil and not criminal.

Mr. MURIS. That is the point precisely. As Congress has given this kind of authority to all sorts of agencies, as to both civil and criminal, and there are these multilateral assistance treaties, MLATS, which Congress has passed authority for on the criminal side.

There are the SEC, and the CFTC, and the banking agencies, have a lot of the authority that we are asking for, and some of it going back many years. We don't have it, and that is exactly what we are asking for.

Mr. TERRY. Well, to further my purpose here, when you want to use this proposed new law, and let's say it is in effect, will this be raised by the way of Canada coming to us, or Mexico, or a foreign government, or is it usually initiated because of a complaint filed by an American citizen that they have been defrauded, and then you follow up and investigate?

Mr. MURIS. Certainly if we have a world of mutual cooperation, we will benefit many more times than other countries, because we have the biggest economy. People want to sell. The legitimate companies want to sell to us and the fraudsters want to sell to us, because our economy is so big, and our people are so rich.

So in a world of increased reciprocal obligations and reciprocal cooperation, we will be the winner. What the Canadians are doing is quite commendable. You know, Canadian consumers are not primarily the victims. It is Americans. But they don't want to be a haven for cross-border fraud.

That is commendable, and what we are asking for is the ability to be able to cooperate with them in a more effective way that will protect American consumers.

Ms. SCHAKOWSKY. If the gentleman will yield.

Mr. TERRY. Yes.

Ms. SCHAKOWSKY. My understanding though is that this is because consumer complaints from the United States have ended up sometimes at a stone wall because we don't have the authority. But is that not true that this is really generated because we want to be able to protect our consumers from whom we are hearing about these problems?

Mr. TERRY. Absolutely. And taking back my time. That is exactly the point that I want to make, is that I think the philosophy behind this bill should be the protection of American consumers, as opposed to simply an agreement of cooperation when another country contacts us.

Both are commendable, but certainly my priority would be the protection of U.S. consumers.

Mr. MURIS. I agree with that and I understand that, but what I am saying is that because we are the biggest economy, and because we are such an attractive target, in a world where countries agree to cooperate with each other, it is our consumers who are going to be benefited many more times than others.

Mr. STEARNS. I thank the gentleman. The gentleman from Idaho, Mr. Otter.

Mr. OTTER. Thank you, Mr. Chairman. I have a written statement that I would ask for unanimous consent to have entered in the record.

Mr. STEARNS. By unanimous consent, it is so ordered.

Mr. OTTER. Mr. Chairman, and ranking member, I thank you very much for this important hearing. I have some concerns about it, and most of those concerns I think have already been voiced by other folks.

But in the draft legislation, and I want to refer you to Section 8, confidentiality, delayed notice of process, and specifically Section 21A, confidentiality and delayed notice of compulsory process for certain third-parties, pages 15 and 16.

My question is that I am concerned about the current language in relationship to the adverse testing result, or the results of testing. Could you explain why the FTC thinks it is necessary to have the power to determine the possibility of adverse results without first consulting with the appropriate judge, and presenting and seeking such latitude as you are asking for?

Mr. MURIS. My understanding is that generally we would have to go to a judge, with the exceptions that are already in the statute, and so I don't think we are asking for unilateral——

Mr. OTTER. Excuse me, but the exceptions that are in the statute relative to fraud, foreign fraud?

Mr. MURIS. Well, it is the exceptions that are in the Electronic Consumer Protection Act statute. I don't think they relate specifically to foreign fraud. They relate generally to law enforcement. I don't think that we are asking for any new or unique unilateral powers, or ex parte powers.

Mr. OTTER. Prior to the passage in October of 2001, and what we refer to affectionately, and sometimes not so affectionately, as the Patriot Act, law enforcement had some of these abilities, and referring primarily to organized crime, and drug trafficking, and pornography.

But even they had only a 48-hour waive time, and then they had to go back to a judge, and with compelling evidence, get the judge to agree to the continuation of surveillance, or wire tapping, or whatever it was.

And so I did not know that this also—I remember it being pornography, RICO, and drugs. I don't remember it referring to fraud.

Mr. MURIS. Well, I think that there is confusion here. We don't do criminal cases, and we don't do search and seizures, and we don't detain suspects. We are talking about delayed notification, like when we go to a third-party to get information about a spammer or someone engaged in fraud. We are talking about confidentiality, preventing the target from being notified.

I mean, some of the concerns, and I think there are obviously legitimate concerns in the criminal context. We don't have those powers. We are obviously not talking about some of the abilities, the extraordinary abilities that exist in the criminal context.

Mr. OTTER. Who would then prosecute these cases?

Mr. MURIS. We prosecute cases civilly, and we are trying to get criminal authorities more involved. Overseas, sometimes these cases are prosecuted criminally. I personally think more fraud cases should be tried criminally.

It is very hard quite frankly to get criminal prosecutors to do that. We have powers, and we are very effective, because we can get money back for consumers when we can find the money. Obviously if the parties were notified, the money would disappear. So that is one of the reasons that delayed notification is important to us.

Mr. OTTER. Well, I am not totally satisfied with that answer, but I want to go on, because my time is going on, and this question that I have refers to Section 5, Powers of the Commission.

And I believe that the way that this draft—if I had the latest draft—as it is currently written, it allows the FTC to investigate U.S. citizens because they may have broken a foreign law. Can you help me out with the sovereignty of a U.S. citizen over a foreign law?

Mr. MURIS. We will get to you a whole series of changes that we think would address some of the concerns that you have. Do you have the July 15 draft? We think that there are a lot of changes that could be made to address some of these concerns, and we would be glad to sit down——

Mr. OTTER. I do have the July 15 draft.

Mr. MURIS. We would be happy to sit down and walk you through those. A concern has been raised, and we understand the concern. We think we need to make changes to address it that we would be investigating people for conduct that is not illegal under U.S. law.

We want the touchstone of this statute to be narrower and to be fraud deception, or "substantially similar" conduct. So I think the concern that underlies your question is a legitimate one, and we think there are appropriate limitations that should be put in the statute.

Indeed, we can live with these limitations, because we think they are appropriate. These are limitations that are narrower than the limitations right now that the FTC, and the CFTC, the banking agencies, and others have in dealing with these issues.

Mr. OTTER. Thank you, Mr. Chairman.

Mr. STEARNS. I thank the gentleman, and we thank the chairman for his being a witness and his attendance, and his staff for coming, and we will move to the second panel.

The second panel is Mr. Mark MacCarthy, senior vice president, public policy, VISA, USA; Mr. Mark Rotenberg, executive director, Electronic Privacy Information Center, (EPIC); and the third is Mr. Ari Schwartz, associate director, Center for Democracy and Technology. Let me welcome the three of you, and we welcome the opening statements of the individuals. Mr. MacCarthy, we will let you start here.

STATEMENTS OF MARK MACCARTHY, SENIOR VICE PRESIDENT, PUBLIC POLICY, VISA, USA; MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER; AND ARI SCHWARTZ, ASSOCIATE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. MACCARTHY. Thank you, Mr. Chairman, and Ranking Member Schakowsky. My name is Mark MacCarthy, and I am the senior vice president for public policy at VISA USA. Thank you for the invitation to appear here today.

We appreciate the opportunity to talk about the important issues raised by the International Consumer Protection Act of 2003. I would like to thank the committee for focusing on this important issue.

Fraudulent activities should not be beyond the scope of law enforcement efforts simply because the fraudulent actor and the victim are located in different jurisdictions. Enforcement agencies in different countries should be able to cooperate and to share information in order to address cross-border fraud.

I would also like to thank Chairman Muris and the other members of the Federal Trade Commission, especially Commissioner Mozelle Thompson, for their efforts in this area. Commissioner Thompson especially worked with the Organization for Economic Cooperation and Development to draft the recommendations that Chairman Muris referred to, for governments to cooperate in this area.

In February the FTC held a workshop, a public workshop, where businesses and consumer groups, and law enforcement officials all shared the view that there needs to be better cooperation between the FTC and its counterpart agencies in order to combat cross-border fraud.

The legislation before you generally accomplishes that objective. Mr. Chairman, the VISA payment system is the largest consumer payment system in the world. There are more than 1 billion VISA branded cards in the world, and they are accepted at millions of locations in more than 150 countries.

The VISA card transactions volume now exceeds $1 trillion annually. The development of the electronic marketplace has been a wonderful thing, and VISA has been proud to participate in the development of that new market, but it has created new opportunities for fraud.

An Internet merchant can establish a website in one country, and provide products and services to customers in another country, and perhaps engage in fraudulent and deceptive conduct, where they know that they will not be accountable in the country where they are selling the products.

VISA has programs in place to protect consumers from fraud. This kind of fraud and other kinds of fraud. We provide a zero liability policy for the unauthorized use of VISA cards. This zero liability policy goes beyond the protections in the current law.

If a customer has not made a particular transaction, VISA will ensure that the customer is not responsible for that fraudulent charge. We have other anti-fraud programs. Verified by VISA allows cardholders to authenticate their identities on-line. Our cardholder information security program has a set of data security requirements for Internet merchants and others who share, and hold VISA cardholder data.

In addition, VISA's sophisticated global networks detect fraud at its earliest stages by analyzing cardholder accounts for unusual spending patterns. A brochure describing these various programs is attached to my written testimony and available on the table for those of you who want to pursue that.

But as a testament to VISA's ongoing fraud prevention efforts, VISA's general fraud level has declined since the early 1980's. Fraud within the VISA system is now at an all-time low of just 7 cents for every $100 of transactions.

We have some information on the extent of the cross-border fraud which tends to confirm the information that Chairman Muris shared with you. For U.S. cardholders who are victims of fraud, approximately 80 percent of the problem occurs within the borders of the United States. That means that 20 percent comes from abroad.

But our risk management staff feels that increasingly fraudulent merchants are operating off-shore by working with financial institutions that are located outside of the United States. This makes the FTC's cross-border fraud initiative even more urgent.

VISA tracks the level of fraud, and the number of high-risk merchants through a especially designed high-risk merchant program. This program also allows us to discipline merchants who have excessively high charge backs.

When fraudulent activity does occur, VISA works with law enforcement, including with local investigators, with the FTC, with the FBI, with the Secret Service, with Treasury officials and with other law enforcement personnel.

I appreciate the opportunity to appear before you today. We think that our systems provide a comfortable and secure way for customers to shop on-line. Combating fraud will continue to be a major priority for VISA and its member institutions, and I would be happy to answer any questions that you might have on what VISA does or the legislation before you.

[The prepared statement of Mark MacCarthy follows:]

PREPARED STATEMENT OF MARK MACCARTHY ON BEHALF OF VISA U.S.A. INC.

Chairman Stearns, Ranking Member Schakowsky and the Members of the Subcommittee, my name is Mark MacCarthy. I am Senior Vice President for Public Policy for Visa U.S.A. Inc. Thank you for the invitation to participate in this hearing. Visa appreciates the opportunity to address the important issues raised by the proposed H.R. , the "International Consumer Protection Act of 2003," which would increase the authority of the Federal Trade Commission ("FTC") to address cross-border fraud and deception. I also would like to thank the Subcommittee for focusing on this important issue of cross-border fraud. Fraudulent activity should not be beyond the scope of enforcement efforts simply because the fraudulent actor and the victim are located in different jurisdictions. Enforcement agencies in different countries should be able to cooperate and share information in order to address cross-border fraud.

Finally, I would like to thank Chairman Muris and the other members of the FTC, especially Commissioner Thompson, for their efforts in this area. Chairman Muris focused on this issue in November of last year. Commissioner Thompson worked with the Organisation for Economic Co-operation and Development to draft recommendations for governments to cooperate in this area and to pass appropriate legislation. In February the FTC held a public workshop where businesses, consumer groups, and law enforcement officials shared the view that there needs to be better cooperation between the FTC and its counterpart agencies to combat cross-border fraud. The legislation before you today generally accomplishes that objective.

The Visa payment system, of which Visa U.S.A. is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. There are more than one billion Visa-branded cards, and they are accepted at millions of locations in more than 150 countries. Visa card transaction volume now exceeds one trillion dollars annually. Visa plays a pivotal role in advancing new payment products and technologies to benefit its 21,000 member financial institutions and their hundreds of millions of cardholders worldwide.

Electronic payments are an important part of electronic commerce and cross-border transactions. Visa believes that it has responded and continues to respond effectively to the ever-changing challenges posed by the increasingly global nature of consumer transactions. In this regard, Visa has a keen interest in fraud prevention and combating emerging fraud techniques.

Although electronic commerce is a large and growing channel for the sale of goods and services to consumers, as recognized in the proposed International Consumer Protection Act of 2003, the development of the electronic marketplace also has created new opportunities for those engaged in fraud and deception. One such opportunity lies in cross-border operations. An Internet merchant can establish a Web site that can be accessed from anywhere in the world and thereby offer and provide products or services to customers without fear that it will be held accountable under the laws of the country where the customer is located.

Visa recognized early on that the Internet and other advancements in communication technologies would result in heightened concern over the potential for fraud. Visa's operating rules provide zero liability for the unauthorized use of Visa credit cards and debit cards, including where the unauthorized use results from fraud. In this respect, Visa rules go beyond existing consumer protections under federal law. Part of zero liability is a global merchant chargeback mechanism. If there is a problem with a merchant and a customer has not made a particular transaction that a merchant has attempted to put through the Visa payment system, the Visa chargeback system will ensure that the customer is not responsible for the fraudulent charge.

As the leading consumer electronic commerce payment system in the world, Visa considers it a top priority to remain a leader in the development of technology, products, and services to protect consumers from fraud. Visa currently has in place many security measures to prevent fraud. For example, one of Visa's fraud control programs, Visa's Secure Commerce Program, includes Verified by Visa. Verified by Visa is a service that allows cardholders to authenticate their identities while shopping online. Cardholders using Verified by Visa add a personal password of their choosing to their existing Visa cards. When cardholders get to the "checkout line" of a participating online store, they enter their personal password in a special Verified by Visa window. The password links legitimate cardholders to their account information. This verification process protects consumers' cards from unauthorized use and provides greater control over when and where cards are used. Visa's Secure Commerce Program also includes the Cardholder Information Security Program,

which is a set of data security requirements for merchants, gateways, and Internet Service Providers, and any other entity that holds cardholder data.

In addition, Visa's sophisticated global networks are designed to detect fraud at its earliest stages by analyzing cardholder accounts for unusual spending patterns and other confirmed risk characteristics to identify likely fraudulent activity. Once potential fraudulent activity is identified, Visa's network immediately contacts the cardholder's issuing financial institution, which will then notify the cardholder of the abnormal activity to ascertain whether the transactions were authorized. Visa also maintains the Exception File, 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 through the Visa payment system have their account numbers checked against the Exception File.

Additionally, Visa now offers Personal Identity Theft Coverage as a new optional benefit for Visa cardholders, which provides eligible cardholders with coverage ranging from $1,000 to $15,000 in reimbursement for lost wages, legal fees, and other costs associated with recovering from identity theft.

Visa's fraud programs extend beyond the transaction level to educate consumers to better understand and prevent fraudulent activity. Visa provides consumer-oriented information about its fraud prevention programs on its Web site and provides security guidance for consumers focused on e-commerce risks. Visa also helps consumers better understand and prevent fraud through preparation and dissemination of materials on fraud prevention topics, such as identity theft prevention.[1] Visa also has partnered with the consumer network Call for Action, to provide free, confidential counseling for victims of identity theft.

In short, Visa maintains ever-evolving practices to respond to the latest techniques of those who attempt to commit fraud. Visa strongly believes that its practices should enable consumers to feel comfortable using their Visa payment cards both domestically and abroad. Indeed, as a testament to Visa's ongoing fraud prevention efforts, Visa's general fraud level has declined since the early 1980's, with cross-border fraud levels also remaining low despite the emergence of e-commerce. Fraud within the Visa system is at an all-time low of just seven cents per $100 transacted. For U.S. banks and U.S. cardholders who are victims of fraud, approximately 80% of the problem activity occurs within the U.S. borders. Visa maintains fraud offices throughout the world to handle issues and administer fraud prevention programs. In addition to protecting the consumer through zero liability, Visa tracks the level of fraud and the number of high-risk merchants through a specially designed high-risk merchant program.

Finally, when fraudulent activity does occur, Visa works with law enforcement by notifying issuers of compromised account numbers and requesting that the issuers contact the investigating agency. Visa also works closely with local investigators, the FBI, Secret Service, Treasury Officials, and other law enforcement personnel on a wide range of fraud issues.

Visa appreciates the opportunity to appear before you today. We believe our payment system creates a comfortable and secure environment for consumers engaged in both domestic and international transactions. Combating fraud will continue as a top priority of Visa and its member financial institutions.

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

Mr. STEARNS. I thank the gentleman. Mr. Rotenberg, welcome.

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Thank you, Mr. Chairman, and members of the committee. I appreciate the opportunity to be with you this morning. The Electronic Privacy Information Center is a public interest research group here in Washington. We work with a wide range of consumer and civil liberties organizations both in the United States and around the world, and I would like to begin by commending you, Mr. Chairman, and the other members of the committee, and the FTC, for the work on this act.

We think that this is a good proposal and an important proposal, and one that responds to growing concerns obviously that American consumers have about fraud and theft on the Internet.

[1] *See, e.g.,* Visa's brochure "Protecting Consumers From Identity Theft."

At the same time in expressing our support for this proposal, I need to emphasize ongoing civil liberties concerns that we have about his legislation. Now, I testified in the Senate this summer on the companion measure, and I see some changes have been made, and I think that this is a step in the right direction.

I was also pleased to hear the Chairman say this morning that he thought that provision regarding creating authority to prosecute people in the United States, where it would not be illegal under U.S. law, and it could be removed, that is a very important change, and we were pleased to hear him say that.

We were also pleased to hear him say that he would favor reporting requirements for the use of this new authority, and we think that is important as well to evaluate how the FTC uses its powers.

But nonetheless, we have serious concerns regarding the impact of this bill on the Freedom of Information Act, and also on privacy safeguards that Americans currently have, and I would like to devote my time if I could to those two issues at this point.

I need to take just a moment to try to explain the structure of the Freedom of Information Act, because I think there may be some confusion in this area. The law as passed by Congress and enforced by the courts recognizes a presumption and the openness of records held by government agencies, and this is very important for our open form of government.

It allows the public to understand the activities of its government and to actively participate in decisionmaking. That that presumption is limited by a series of exemptions, and there are nine exemptions covering a wide range of activities, from national security matters, and enforcement matters, to matters involving the protection of personal privacy.

And invariably what happens when people seek information from a Federal agency, if the agency believes that it needs to protect the information because it falls within one of these exemptions, it will apply the exemption, and withhold the information, and then the two parties may go to court and argue about the scope of the exemption.

In fact, my organization, because it has been involved in many FOIA suits with many Federal agencies, and sometimes we get the information, and sometimes we don't. But I think we all respect the process, even the agencies do in applying their exemptions.

We have even had the experience with the Federal Trade Commission where we pursued a FOIA request to try to get access to the complaints that the Commission was receiving from consumers about privacy matters, because we wanted to see how well the Commission was responding to the concerns of Americans.

Some of the information was disclosed and some of it wasn't. That is not unusual. The key point is that this bill proposes to create a new statutory exemption, in addition to the exemptions that already exist, and I think that this is a mistake.

I think the FTC can say to foreign governments that it wants to work with that we currently have the ability in law to protect the confidentiality of information in ongoing criminal investigations. We currently have the ability in law to protect confidential sources, to protect business information, and privacy information.

We do not think it is necessary under our law to create a new exemption to be able to cooperate with you in these international investigations. So we feel quite strongly that it would not be necessary to create a new FOIA exemption as this Act proposes to do.

Now, I would also like to say a few words about the impact of the bill on privacy safeguards, and this is important as well. We give the Federal Government an enormous amount of authority to pursue criminal investigations, but we do so in a way to enable oversight and accountability, and frankly to make sure that the government does its job as it should.

One of the core principles in our Fourth Amendment that enables the search by government of a person's private possessions is notice to the target of an investigation, and you will see it on the t.v. shows and you will read it in the cases, but in our country the police simply cannot go into a home without providing notice to the homeowner that a police officer is about to enter.

And we carry that principle across many, many different areas of criminal investigations. Now, there are a few significant exceptions. As one of the members pointed out earlier, in the wiretap area, for example, we create a 48 hour period of time that allows for delayed notification, so that someone who is the target of an investigation and thinks that they may be subject to an intercept is not able to allude capture and detection.

And that is recognized in law, but a proposal for a 90 day delayed notification, or a 1-year notification, is really quite extraordinary, and I don't see what the basis would be for such an extensive notification.

I have other suggestions, which I would be glad to provide to the committee. I would just like to say finally, Mr. Chairman, I think that it is very important with legislation like this to understand not only does it impact the rights of Americans, but we also send a very powerful message to other governments that we work with about how criminal investigations are to be undertaken.

And I think that the United States has shown that open government and privacy protection are not incompatible with effective law enforcement.

[The prepared statement of Marc Rotenberg follows:]

Marc Rotenberg
Electronic Privacy Information Center, Executive Director
Georgetown University Law Center, Adjunct Professor

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today regarding consumer fraud and the reauthorization for the Federal Trade Commission. My name is Marc Rotenberg and I am the executive director of the Electronic Privacy Information Center (EPIC). EPIC works with a wide range of consumer and civil liberties organizations both in the United States and around the world.

I would like to begin by thanking the Committee for focusing on the issue of

cross-border fraud. One of the consequences of the rapid growth of the Internet has been the dramatic expansion of both commercial opportunity online and of commercial fraud. It is clearly in the interests of businesses and consumers to ensure a stable, growing, and fair online marketplace. Fraudulent and deceptive business practices that would otherwise be prosecuted in the United States should not be beyond the reach of United States law enforcement simply because an operator sets up shop outside the country. In similar fashion, government agencies seeking to protect the interests of consumers in their jurisdictions should expect the cooperation of the Federal Trade Commission when cross-border problems emerge.

I would also like to thank the FTC Chairman and the other members of the Commission for their efforts to address this new challenge and for the workshop in February that provided a wide range of important perspectives on this topic. Chairman Muris outlined the plan to pursue cross-border fraud in November of last year. He said that the FTC would advocate the adoption of a recommendation of the Organization for Economic Cooperation and Development (OECD) on cross-border fraud and would seek appropriate legislation. Commissioner Thompson, working through the International Marketing Supervision Network and in cooperation with the FTC's international counterparts, has helped develop a common understanding of what constitutes core consumer protection in the international realm.

The February workshop, organized by the FTC, set out the views of consumer and privacy organizations, businesses and foreign agency officials. Chairman Muris noted that cross-border complaints by US consumers rose from 13,905 in 2001 to 24,313 in 2002. Canadian consumers also report a near doubling of complaints with online commerce between 2001 and 2002. The *Consumer Sentinel*, the FTC's central complaint database, records over 72 million dollars lost by U.S. consumers to cross-border fraud in 2002, nearly seventeen percent of all money lost to fraud. According to the FTC, 68% of all fraudulent foreign money offers come from companies located in Africa; 41% of fraudulent advance-fee loans come from Canadian companies, and 61% of fraudulent prize and sweepstakes offers are from companies located in Canada.

There was consensus at the February FTC workshop on the need to tackle the problem of cross-border fraud and to enable better cooperation between the FTC and its counterparts. The FTC proposal grows out of the work of the February meeting, the OECD, and the continued efforts to promote international cooperation. A story in the Washington Post just yesterday about the "J.D. Marvel" company makes clear that cross-border consumer fraud is a very real problem for many American consumers.

EPIC has a particular interest in the protection of consumers in the global economy. We have successfully pursued privacy complaints on behalf of consumers under Section 5 of the FTC Act that have international implications. For example, our earlier work on the privacy implications of Microsoft Passport, the online authentication scheme, was considered favorably by both the Federal Trade Commission and the European Commission. EPIC also work closely with consumer and civil liberties organizations on the development of international policy. In particular, the Trans Atlantic Consumer Dialogue (TACD), a coalition of sixty consumer organizations in the United States and Europe, has urged officials on both sides of the Atlantic to address this challenge. Similar views have been expressed by consumer organizations in other parts of the world. We have also worked with the OECD for more than a decade, in areas such as privacy protection, consumer protection, cryptography, and electronic commerce, to promote the development of policies that promote economic growth and safeguard democratic values. We are pleased that these efforts have come together in the current proposal before the Committee to combat cross-border fraud.

In the statement today, I will recommend passage of legislation that will enable the Federal Trade Commission to work more closely with consumer protection agencies in other countries to safeguard the interests of consumers and users of new online services. Nevertheless, in creating these new enforcement authorities, there is a clear need to safeguard important legal safeguards that are central to the US form of

government. In particular, certain provisions of the draft International Consumer Protection Enforcement Act, put forward by the FTC, should be revised to safeguard privacy, promote government accountability, and enable the development of reporting standards that will allow this Committee and the public to assess how well the FTC is doing its job and whether further steps may eventually be necessary. Without these changes, the legislation opens the door to abuse in that it creates new enforcement authority without corresponding safeguards. Civil liberties groups in both the United States and Europe have already expressed strong opposition to a proposal of this type that was put forward by the Council of Europe to combat cyber crime.

It is particularly important to understand that when the United States provides information about consumers and business in the United States to foreign law enforcement agencies it opens the door to prosecution that may not satisfy the substantive requirements or safeguard the procedural rights that would be available in this country.

SPECIFIC PROVISIONS IN THE FTC PROPOSAL

Information Disclosure to Foreign Governments (Draft bill - Sections 5b and 7)

We recognize that the cross border enforcement of consumer fraud will require cooperation between the FTC and sister agencies in other jurisdictions. To some extent, the sharing of information between agencies will be necessary to pursue violators and enforce judgments. At the same time, it is critical to ensure that only the necessary information is disclosed and that appropriate safeguards are established when such information is disclosed.

In our view, the FTC proposal creates too few restrictions on the disclosure of information concerning individuals and entities within the United States. One particular provision is simply offensive. A proposed amendment to Section 6 of the FTC Act that enables the FTC to assist foreign law enforcement agencies states that "such assistance may be provided without regard to whether the conduct identified in the request would also constitute a violation of the laws of the United States." This provision should be removed since it effectively nullifies the probable cause requirement of the Fourth Amendment to the Constitution. It would allow an investigation of a United States individual or agency though the basis for the investigation involved no suspicion of any acts constituting a crime in the United States.

We further recommend that the disclosure be only to "appropriate" foreign agencies, not "any" foreign agency as is currently specified in the bill, and we urge the FTC to post the names and contact information for any foreign agency that it considers appropriate to receive information. Not only should the FTC share information with appropriate agencies, it should share information only at appropriate times and in connection with a specific investigation. The Custom Service, for example, limits the exchange of information and documents with foreign customs and law enforcement to those instances where the Commissioner "reasonably believes the exchange of information is necessary . . ." 19 C.F.R. sect. 103.33. The FTC should not permit disclosures to any foreign government agency where the public and concerned parties cannot readily identify the agency.

We further recommend the recognition of a dual criminality provision to ensure that the United States assists in the prosecution of individuals and entities within the United States only in those circumstances where the crime charged would also be a crime under United States law. Absent such a provision, it is conceivable that a bookseller or music publisher in the United States could be subject to prosecution under foreign law where such government does not provide for strong protections for freedom of expression. This problem could arise in particular with publications that criticize state governments.

Amendments to US Privacy Statues (Sections 8 and 9)

The FTC legislative proposal would amend two critical US privacy statutes to reduce the likelihood that the target of an investigation would be notified of the investigation. In particular, the International Consumer Protection Act would amend the Electronic Communications Privacy Act, and the Right to Financial Privacy Act. But the arguments for denying notice to the target of an investigation could too easily be made with respect to targets in the United States. The proposed changes here not only set a bad precedent but would also send a bad message to consumer protection agencies in other countries about the conduct of investigative actions by democratic governments.

We recommend that the provisions that reduce procedural safeguards be removed.

Disclosure of Financial Information (Section 11)

This provision would give the FTC authority to access financial bank reports and other financial data under the guise of fighting against cross-border consumer fraud and deception. However, there are no reporting or notification requirements that record the exchange of information; there are no audit provisions that oversee the exchange of the information; there is no limit on who within the authorized agencies can exchange information, and there is no limit on what the content of the reports, records or other information shall consist off.

These provisions make it too easy for the listed agencies to share financial information. The provision would give the FTC discretion to share financial information without any oversight to make sure it is shared appropriately. This discretion leaves the exchange of information open to abuse. Moreover, there is no limit on what sort of information can be exchanged. There is no provision that states that records or information cannot consist of information identifiable to a particular customer. In this way, the authorized agencies could examine records about customers of financial institutions, without notification requirements, under the guise of examining records regarding the financial condition of the institution.

Although the objective of the proposed amendment, to ease the sharing of information amongst agencies involved in protecting consumers against fraud, is laudable, the amendment should include provisions that ensure that personal financial information is shared in an accountable and transparent manner. Acknowledging the FTC's desire to be able to share information appropriate to real-time law enforcement needs, the following additions to the amendment may be appropriate:

- a provision that information exchanged under 1112(e) cannot contain information identifiable to any one individual without triggering a reporting requirement.
- a provision that a designated official at the authorized agencies have a log of all personal information that is exchanged under 1112(e).
- a provision that such a log is available to the public under FOIA, unless there is a compelling law enforcement reason to exempt it.

Adding such provisions would allow an appropriate amount of accountability into the information exchange process, while still allowing the FTC and the other listed agencies to have the flexible use of information for their law enforcement needs.

Freedom of Information Act Exemptions (Sections 7b and 9)

The FTC proposes to exempt itself from certain open record obligations under the Freedom of Information Act. We believe this change is unnecessary and, if enacted, will reduce government accountability.

The current FOIA exemptions for ongoing criminal investigation, § 552(b)(7)(A), and for the protection of confidential sources, (b)(7)(D), would likely prevent the disclosure of information that the FTC seeks to protect without any further amendment.

Moreover, three other exemptions may also apply to information collected by the Commission; the exemption for business information under § 552(b)(4); for personal privacy under § 552(b)(6); and for records of financial institutions under § 552(b)(8).

EPIC has already pursued an extensive FOIA request with the FTC involving the investigation of privacy complaints under Section 5 of the FTC Act. In that case, the FTC has demonstrated its willingness to apply the current statutory exemptions. Some of the information we sought concerning current matters was withheld. The FTC cited the (b)(7)(A) exemption.

Since the existing exemptions already provide adequate protection for the Commission, a new exemption is not necessary and only adds confusion to a long-standing statutory scheme that has been subject to judicial interpretation for almost thirty years. Therefore, we recommend that provisions to limit the application of the Freedom of Information Act be stricken from the FTC proposal, or at the least that a thorough analysis be done to determine whether the current exemptions combined with current case law are sufficient before any new exemption is created.

GENERAL RECOMMENDATIONS

Reporting

We recommend the creation of new reporting requirements that would focus specifically on the FTC's activities undertaken pursuant to this new legislative authority. There should be an annual report provided to the Congress and made available to the public at the web site of the FTC. This report should include such information as the number of complaints received during the past year, the number of investigations pursued, and the outcome of these investigations including whether any damages were assessed and whether any relief was provided to consumers as a result of the investigation. The report should also indicate which foreign agencies the FTC cooperated with and the nature of the information provided and the information received.

The FTC has already begun the process of making some of this information available with the Consumer Sentinel web site. Canada, Australia and the United States, have also established eConsumer project that helps provide similar information on the international front. While both projects are important, we believe that formalizing reporting requirements for investigations as well as complains will make it easier to assess how well the FTC and other agencies are responding to the challenges of cross-border fraud.

We would also urge the FTC to consider the creation of an advisory council for the major multilateral law enforcement groups, such as the International Consumer Protection and Enforcement Network, that would allow the participation for a US consumer representative and a US business representative. Participation by representatives of the consumer and business community will help ensure oversight and reduce the risk of unaccountable activities.

International Privacy Framework

The OECD proposal for protecting consumers in the global economy is consistent with other efforts of the OECD to promote economic growth while safeguarding democratic values. In this spirit, we would like to underscore the need to ensure that new efforts undertaken by the United States in cooperation with other governments should be consistent also with the OECD recommendation on privacy protection. The FTC has already worked to ensure that principles similar to those contained in the OECD Privacy Guidelines were established for transborder data flows between the United States and Europe in the context of the Safe Harbor proposal. That arrangement allows US firms to enter European markets and process data on European consumers on the condition that they follow and enforce strong privacy standards.

We urge the adoption of a similar framework to regulate the transfer and use of personal information that will occur between national governments as they pursue joint investigations and prosecutions. Governments, no less than the private sector, should be held to high standards in their use of personal information, particularly because the misuse of such information may subject individuals to unfair and unfounded prosecutions.

Emerging Privacy Problems with the WHOIS Database

As the FTC pursues international consumer protection, it is important to consider the implications of providing access to various databases. The Senate FTC reauthorization bill, S.1234, initially proposed to grant the FTC access to the National Crime Information Center database. As EPIC explained in testimony for the Senate Commerce Committee on June 11th, access to the NCIC database would create risks to consumers in the United States, particularly where the information was used for purposes unrelated to lawful investigation. We were pleased to find that this provision was removed from the Senate measure and does not appear in the House proposal.

Now, we would like to call your attention to another database that may also raise serious problems for consumers in the United States. The WHOIS database provides an important resource for the administration of the Internet. It helps track security problems and identifies domain registrants who wish to be identified. The problem today is that the WHOIS database is being used for many other purposes, including fraud. The WHOIS database facilitates opportunities for fraudulent activity by compelling the disclosure of detailed personal information that is then made widely available. To prevent such misuse of the WHOIS database, strong privacy protection is critical for protecting consumers against Internet-based fraud.

The WHOIS database exposes detailed personal data of domain name owners to the public without limitation. The information in the database is available to more than just system administrators, but also to criminals intending to commit fraud, identity theft or stalking. The database may also be used for distributing spam, which could involve a fraudulent activity. Further, the information in the WHOIS database is globally available, thus enabling criminals worldwide to prey upon American consumers. The FTC has cited such cross border identity fraud as a growing problem. Access to WHOIS data compounds the problem of identity theft.

Against the backdrop of rampant problems in the WHOIS database, some have advocated increased accuracy in WHOIS data without corresponding privacy safeguards. Because of the insufficient privacy safeguards in the existing WHOIS system, consumers seeking to protect their personal information from fraud may provide inaccurate or incomplete data to prevent dissemination of their personal information. Efforts to promote WHOIS accuracy will require strong privacy safeguards to minimize the risk of fraud.

The Public Interest Registry (PIR), the organization responsible for the management of the .ORG domain and one of the Internet's largest registries, has recently submitted important recommendations on privacy protection for the WHOIS database to the House Subcommittee on Courts, Internet, and Intellectual Property. The PIR recommendations, combined with the OECD Privacy Guidelines, provide a good basis for privacy safeguards for WHOIS data that would reduce the risk of Internet-based fraud and help safeguard American consumers.

We urge the Subcommittee to work with the FTC to ensure that strong privacy safeguards, based on internationally accepted standards, are established for the WHOIS database

FTC's Work on Do Not Call and Spam

Finally, Mr. Chairmen, I would like to say a few words about the FTC's work to

protect the privacy of American consumers. On the one hand, we are very pleased with the success of the FTC Do Not Call program. More than 41 million Americans have signed up for this list to reduce unwanted telemarketing. The Commission should be commended for implementing this system and for responding to many more requests than were originally anticipated.

At the same time, we were disappointed that the FTC Chairman recently suggested that he did not favor legislation to address the growing problem of spam. Particularly in the context of this hearing, which considers new powers given to the FTC to collaborate with consumer protection agencies in other countries, it is vital that the FTC understand the strong worldwide support for effective legislative responses to spam. While it is clear that legislation will be only part of the solution – technology, consumer education, and better industry practices all have a role to play -- the FTC will look badly out of step in the international arena if it pursues new consumer protection authority but opposes legislation on spam. For many Internet users, reducing the amount of spam is simply the number one concern in the area of "international consumer protection," which is the title of the bill now before the Subcommittee.

CONCLUSION

There is a clear need to enable the Federal Trade Commission to work in cooperation with consumer protection agencies in other countries to investigate and prosecute cross-border fraud and deceptive marketing practices. New legislation will be necessary to accomplish the goal. Nevertheless, the bill should be drafted in such a way so as to safeguard important American values, including procedural fairness, privacy protection, and open government. These principles of good government will assist consumer protection agencies around the world combat cyber fraud, and will help strengthen democratic institutions. Moreover, steps should be taken to protect the privacy of WHOIS data and to make clear US support for effective spam legislation.

Thank you for your attention. I will be pleased to answer your questions.

ABOUT EPIC

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and to promote the Public Voice in decisions concerning the future of the Internet. More information is available online at www.epic.org.

REFERENCES

Statement of Cedric Laurant, EPIC Policy Counsel, on "Potential Partnerships among Consumer Protection Enforcement Agencies and ISPs and Web Hosting Companies" for the Public Workshop on Public/Private Partnerships to Combat Cross-Border Fraud, before the Federal Trade Commission (February 19, 2003) [http://www3.ftc.gov/bcp/workshops/crossborder/comments/epic_Laurant.pdf]

EPIC, "Joint Letter and Online Petition: Require Accuracy for Nation's Largest Criminal Justice Database" [http://www.epic.org/privacy/ncic/]

Federal Trade Commission, Consumer Sentinel, Cross-Border Fraud Trends, January – December 2002, (February 19, 2003) [http://www.consumer.gov/sentinel/trends.htm]

Federal Trade Commission, Budget Summary, Fiscal Year 2004, Congressional Justification [http://www.ftc.gov/ftc/oed/fmo/budgetsummary04.pdf]

Federal Trade Commission, Budget Summary, Fiscal Year 2003, Congressional Justification [http://www.ftc.gov/ftc/oed/fmo/budgetsummary03.pdf]

Federal Trade Commission, Consumer Sentinel web site [http://www.consumer.gov/sentinel/]

Federal Trade Commission, Cross Border Fraud web site [http://www.ftc.gov/bcp/workshops/crossborder/]

Federal Trade Commission, "FTC Chairman Muris Presents the FTC's New Five-Point Plan for Attacking Cross-Border Fraud and Highlights Links Between Competition and Consumer Protection" (October 31, 2002) [http://www.ftc.gov/opa/2002/10/fordham.htm]

Marilym Geewax, "FTC Chief Favors New Tack vs. Spam," The Atlanta Journal and Constitution, August 20, 2003, at 3D.

In the Matter of Microsoft Corporation, No. 012-3240, before the Federal Trade Commission [http://www.ftc.gov/opa/2002/08/microsoft.htm]

International Consumer Protection Act of 2003, H.R. ___, draft, July 15, 2003

Don Oldenburg, "Complaints Lose Bite Across Borderlines," The Washington Post, September 16, 2003 at C09.

Organization for Economic Cooperation and Development (OECD), Directorate for Science, Technology and Industry, Committee on Consumer Policy, "Cross-Border Co-operation in Combating Cross-Border Fraud: The US/Canadian Experience." (February 6, 2001)

Organization for Economic Cooperation and Development (OECD), Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines"), reprinted in Marc Rotenberg, ed., *Privacy Law Sourcebook: United States Law, International and Recent Developments* 324-352 (EPIC 2002)

Privacy Coalition, "Framework for Effective Spam Legislation," (July 18, 2003), at http://www.privacycoalition.org/spam_letter.html.

Transatlantic Consumer Dialogue, "Resolution on Protecting Consumers from Fraud and Serious Deception Across Borders," Doc No. Internet-28-02 (November 2002) [http://www.tacd.org/docs/?id=179]

Mr. STEARNS. I thank the gentlemen.

Mr. Schwartz.

STATEMENT OF ARI SCHWARTZ

Mr. SCHWARTZ. Thank you, Mr. Chairman, and members of the subcommittee. Thank you for inviting the Center for Democracy and Technology to testify here today. As you suggested earlier, Mr. Chairman, the International Consumer Protection Act will mark a substantial expansion of the scope of the powers of the Federal Trade Commission.

CDT has been supportive of the work of the Federal Trade Commission over the past nine years, as it has helped consumers combat fraudulent and deceptive practices in a network economy, and especially on the internet.

As the number of people on-line continues to grow, e-commerce has become global in nature. Not surprisingly, global consumer

fraud has followed. As the FTC works to combat identity theft, internet fraud, to curb deceptive spam as we have been talking about earlier, and to protect privacy on-line, there is no question that the FTC needs authority to work with its international counterparts.

While the CDT is supportive of the goals of the Act and Chairman Muris' desire to work internationally, we believe that it is necessary to ensure proper safeguards are also in place to protect privacy and due process rights of individuals, while protecting consumers at the same time.

For the most part a proper balance has been struck in the act. However, we still remain concerned with two provisions in particular. First, we agree with the concerns that Mr. Rotenberg raised about delayed notice, and we do not think that the delayed notice provision as it stands adequately protects individuals.

Historically under the Fourth Amendment of the Constitution, individuals are given direct notice if the government wants their information in an investigation. If the government wants a record from my home, they have to knock on my door and serve me with a warrant.

As more information is held by third-parties—insurance information, credit cards, purchases, et cetera—government agencies have pushed to get this information without warning the subject of the investigation.

As more and more information moves to the network world, and thus, more information is held by third-parties, privacy and due process concerns are raised by this activity. In the past, subjects could move to stop mere fishing expeditions when they receive notice, and under this bill there would be little pushback on an FTC that exceeded jurisdictions in these cases.

CDT suggests that the delayed notice provision be removed entirely, but that at the very least it should be amended to remove the most vague of the acceptable reasons or the adverse results for such an action in order to limit potential for abuse. I have provided suggestions for doing so in my testimony.

Secondly, in here, and I was working off of the July 15th version of the bill, as that is the only version that we have seen, CDT remains concerned about the lack of dual criminality. Simply put the provision as it stands in that July 15th version could allow foreign governments to investigate American citizens in cases where no U.S. law has been broken, a clear violation of due process rights.

It has been suggested that the Act's provision in requiring the FTC only to take part in cases where the foreign law is substantially similar to U.S. law would mitigate this concern. However, it is not the foreign law that should be compared to the U.S. law.

It is the investigation that the foreign government is undertaking. The FTC should be required to show that the case under consideration be worthy of investigation under their own jurisdiction, and we have also suggested language that can mitigate these concerns as well.

While I address several other issues in my written testimony, I would like to conclude by emphasizing that these are broad and important new powers that the FTC needs to get its job done internationally.

Therefore, we hope that this committee will continue to oversea the Act implementation, especially with regard to accountability, privacy, and due process rights as it is put into effect. Thank you again for having me here and I look forward to your questions.

[The prepared statement of Ari Schwartz follows:]

PREPARED STATEMENT OF ARI SCHWARTZ, ASSOCIATE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

I. SUMMARY

Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee, the Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify today on the cross-border fraud proposals of the Federal Trade Commission (FTC).

The draft bill before the Subcommittee, the International Consumer Protection Act, is landmark legislation, reflecting a major expansion in the scope of the enforcement activity of the FTC. The problems to which this bill responds are certainly deserving of attention. As the number of consumers online continues to grow, and as we see significant increases in Internet usage by businesses and individuals in countries around the world, e-commerce has become global in nature. Not surprisingly, global consumer fraud has been an undesirable side effect, threatening the trust that is an element of e-commerce. As the FTC steps up its efforts to prevent Internet fraud, to curb deceptive spam, and to address other obstacles to Internet commerce, there is no question that it needs authority to work with its counterparts overseas to more effectively protect consumers. The International Consumer Protection Act transforms the FTC into a regulatory agency of truly international reach.

Yet, while CDT supports the overall intent of the Act, and while we highly respect the work of the Commission and its staff, and commend especially Commissioner Thompson and Chairman Muris for their leadership in this area, we would be concerned with any authorities that would infringe on the privacy and due process rights of individuals or diminish accountability of government agencies.

For the most part, the International Consumer Protection Act achieves the right balance. CDT has worked with the Commission to address several of our areas of concern either through text changes or through a better understanding of how the FTC operates.

However, CDT still has concerns with the bill that have not been addressed. In particular:

- The delayed notice provisions of the bill are very broad and would give the FTC the ability to obtain access to sensitive financial and other information without notice. We recommend narrowing the scope of the delayed notice provision to specific and justified circumstances.
- The authorization for FTC cross-border cooperation in cases involving conduct that would not be illegal if committed in the US (the lack of "dual criminality") opens the potential for diversion of scarce resources. At this phase in the development of the FTC's cross-border activity, it should focus on conduct that that is serious enough so that it would be illegal under US law.

We urge the Committee to amend the bill accordingly.

II. ABOUT CDT

CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies.

III. CDT'S CONCERNS WITH THE INTERNATIONAL CONSUMER PROTECTION ACT OF 2003

Delayed Notice of Access to Sensitive Records (Section 8)

Section 8 of the International Consumer Protection Act concerns the question of notice to the subjects of investigations that their records are being disclosed to the FTC. Notice of disclosure is a central element of fair information practices. Notice has become increasingly controversial as more and more records about individuals and companies are held by third parties. Obviously, if the government wants records from you that are relevant to an authorized investigation, it can force you to disclose them with a subpoena or other process, and it gives you notice when it serves the subpoena on you. This is the normal Fourth Amendment model and is the way that investigations were traditionally conducted. The recipient of the subpoena has the

opportunity to contest the subpoena, to protect against fishing expeditions. But more and more records about individuals and companies are held by third parties—including banks, merchants, insurance companies, credit card companies, and online service providers—who may have no interest in seeking to ensure that a subpoena is narrowly focused, since the records do not pertain to them. Increasingly, the government is seeking to prohibit holders of data from disclosing to their customers the fact that the government has sought their records. This means that the person whose privacy is being breached has essentially no opportunity to challenge the subpoena.

It is in this context that we are concerned about the delayed notice provision of the International Consumer Protection Act. Section 8 would grant the Commission power to access data about someone without providing notice to the individual and allowing the individual to challenge the subpoena. The delayed notice provision is not limited to cross-border investigations, but applies as well to purely domestic activity of the FTC. The fact that delayed notice might be used in the international consumer protection context heightens our concern, for it means that records will be disclosed to foreign governments, against whom redress may be extremely difficult if the records are misused.

We would prefer to see the entire delayed notice section removed to clearly ensure due process rights for individuals and set a strong example for consumer protection agencies around the world that notice is an important element of fair investigations. At the very least, the definition of "adverse result" should be more narrowly drawn so that the powers cannot be abused. We recognize that there are various definitions of "adverse result" on the books. The definition used by the FTC should be keyed to the specific and documented needs of the Commission. In particular, CDT recommends that subparagraph (2) ("impeding the ability of the Commission to identify or trace funds") and subparagraph (8) ("otherwise seriously jeopardizing an investigation or unduly delaying a trial") be removed from the definition of "adverse result." These two criteria seem so broad that they could apply to every investigation. (Every case involving fraud is likely to involve difficulty in identifying or tracing funds.) The serious problems faced by the Commission would be covered by the other components of the definition.

FOIA Exemptions (Sections 7 & 9)

The bill contains two different Freedom of Information Act (FOIA) exemptions. CDT believes that all FOIA exemptions should be approached with caution, since transparency is an essential value for a functioning democracy. Specifically, FOIA is often the only means to ensure government accountability. Moreover, "so-called (b)(3)" exemptions not only prevent individuals from obtaining information, but also are sometimes mis-interpreted by agencies as broad prohibitions against proactively disclosing information they would otherwise deem necessary to distribute to the public.

Section 7 of the International Consumer Protection Act would grant an exemption for foreign investigative materials given to the FTC. It is CDT's understanding that this provision is intended to parallel the existing exemption from FOIA in the Federal Trade Commission Act for materials acquired by the Commission by subpoena or voluntarily disclosure in lieu of subpoena in the course of an investigation. We understand the basis for this exemption, but recommend that it be narrowly drafted. For example, we recommend that the withholding be limited to circumstances where the foreign government agency has "requested confidential treatment as a condition of providing the material." In addition, CDT notes that Congress is still given the authority to gain access to these materials. Therefore, we encourage this Subcommittee to diligently pursue oversight of international consumer investigations to ensure effectiveness, since the public will not be able to scrutinize these activities through FOIA.

The second FOIA exemption, Section 9 of the Act, would exempt material voluntarily submitted to the FTC, "to the extent such disclosure could reasonably be expected to reveal either the identity of a person, partnership, or corporation that is the subject of such a disclosure, or the identification of a particular financial account, its ownership, or a confidential record of account activity." The original version of the bill had a particularly broad exemption that could have permitted the FTC to withhold, in a wide range of circumstances, information about fraud schemes targeting large numbers of individuals.

CDT worked with the FTC staff to develop the current language, to ensure that the name of the corporation or entity disclosing the information is exempt without removing from public view the fact or nature of the complaint itself. This language is an attempt to achieve a balance that will encourage companies to share information with the FTC and still require disclosure under the FOIA of adequate informa-

tion to inform and protect the public. As this provision is intended to encourage the sharing of information, CDT urges the Subcommittee to monitor its implementation. If companies are still not sharing information with the FTC as intended, this exemption should be revisited.

Dual Criminality (Sections 5 and 7)

As a general rule, US law enforcement agencies should cooperate with foreign governments only in the investigation of conduct that would be illegal under US law if it were occurring here. This is the concept of "dual criminality." It does not require that the laws of other countries use the same or similar words as ours as a pre-condition of cooperation. Rather, it is a principle that protects US citizens and ensures a prioritization of US law enforcement resources by focusing cooperation on those circumstances where is illegal under US law or would be illegal if occurring in the US. We are concerned that the draft bill rejects the principle of dual criminality, and would thereby authorize the FTC to spend taxpayer resources aiding foreign governments in investigating conduct that the US Congress has not deemed worthy of attention in the US. Dual criminality is especially important in the context of competitive practices and advertising, for some countries have very different definitions than we do of what is legal in terms of price comparison advertising and other competitive practices.

The International Consumer Protection Act represents the first major legislative expansion of the FTC's authority in cross-border fraud enforcement. We recommend a more incremental approach—extend cooperation to things that would be illegal under US law, before stretching resources and procedures to cover conduct that would not be illegal in the US. We recommend, therefore, in Section 5 of the bill, that the new subsection 6(j)(1) be revised to refer to "possible violations of laws prohibiting fraudulent, unfair, or deceptive commercial practices that are prohibited or, if committed in the United States, would be prohibited by any provision of the laws administered by the Commission," and that the proposed subsection 6(j)(2) be dropped. A similar change would be necessary in Section 7.

Other Concerns

We have a few other suggestions:

- The definition of "foreign law enforcement agency" is over-broad, and includes agencies that are really not law enforcement. It seems, for example, that the bill's definition of "foreign law enforcement agency" would be broader than the term "law enforcement agency" when used in reference to a State or local agency in the US.
- Under the new subsection 6(j) (15 U.S.C. 46(j), we recommend deleting (B) of the definition. Requests from foreign governments should be in writing, just as requests for disclosure from domestic agencies must include a written certification under subsection 6(f) (15USC46(f)).

IV. CONCLUSION

CDT commends the FTC for its initiative in the area of cross-border-fraud—a problem particularly important in the age of the Internet. We believe that a balance can be achieved to both protect consumers and protect the privacy and due process rights of individuals. The FTC should be given reasonable authority to cooperate cross-border, so long as any new powers are narrowly defined, are subject to checks and balances, and their impact on privacy and due process is limited.

We stress the important role that this Subcommittee has in overseeing the implementation of this Act. We urge the Subcommittee to hold hearings in the coming years on the effectiveness of this legislation and to especially monitor the accountability, privacy and due process concerns that we have raised today.

Mr. STEARNS. I thank the gentleman. I will start with my first series of questions. Mr. Rotenberg, when I was hearing you talk about procedural requirements and safeguards, since these are civil matters, how would you overcome the problem associated with a notification to people if you did not have delayed notification?

They would simply risk a flight. They would take their money and their evidence, and they would be gone. So don't you need to in a civil matter just to have a delayed notification?

Mr. ROTENBERG. Well, I think that is an argument that might favor delayed notification. I don't think it answers the question of

what the duration would be. I think that 90 days or a year is simply too long.

One area which I am fairly familiar with is the wire tap area, and obviously if you have—

Mr. STEARNS. Is the wiretap more in criminal or is that more—

Mr. ROTENBERG. Well, it is criminal, but let me explain how—

Mr. STEARNS. I mean, is there a difference between the civil and the criminal?

Mr. ROTENBERG. Right.

Mr. STEARNS. So that you are talking about a civil delay, which would be much more acceptable than maybe criminal?

Mr. ROTENBERG. Right, but in either scenario, you still need means of oversight and accountability, because frankly you want to be sure that an investigation is moving forward, and if you say to an agency that you have a year before anything needs to be said to the public about an investigative matter, I would have concerns about how seriously the agency is pursuing the matter.

So the example that I was going to in the wiretap area, where you don't want to tip off the target, typically law enforcement will get 30 days to pursue the investigation, which is the period of a typical wiretap application.

And if after 30 days, they have not obtained enough information to bring the indictment, they will go back before the court and ask for an extension, and say please give us another 30 days. We are still gathering evidence.

I think that a similar mechanism would work here. I mean, maybe you draw the line at 30 days, and create some mechanisms for renewal.

Mr. STEARNS. Mr. MacCarthy, VISA being as large as it is, you are probably an expert on identifying and combating cross-border fraud, and I guess you might give us some of the ideas of the emerging fraud techniques that you are using in VISA, and I guess some of the challenges that you have in combating fraud.

Mr. MACCARTHY. I think that the best way to answer that question probably is to tell you a little bit about our charge back system, and how it works, and how we keep track of merchants who are experiencing excessively high charge back rates.

Consumers have an ability if they have problems with merchants to talk to their financial institution that issued their card, and make a complaint, and these complaints can be in various kinds.

They can be that I didn't get the item that I paid for, and it can be that I got an item, but it wasn't what I wanted. It was of inferior quality; or it can be that I did not engage in that transaction at all.

And that kind of complaint is the one that is most worrisome to us, because it indicates that there might be some fraud or identity theft involved in the circumstances. And it is at that point that tour zero liability policy kicks in.

If there is fraud and the consumer was not engaged in that transaction at all, and did not authorize it, then there is no liability on the part of the consumer. But we keep track of all those complaints, and we note which merchants are involved in those complaints, and merchants that have a high percentage of their sales involved in these kinds of charge backs, or an excessively high

number, an absolute number of these charge backs, we put them on a list of high risk merchants.

And we monitor them to make sure that they reduce their problem transactions within a timely basis. Now, often those merchants are just—they are having back office problems, and some of the difficulties that are creating problems for them in their relationship with consumers.

But sometimes they are fraudulent merchants, and sometimes they are engaged in patterns of deception and fraud with consumers. And when that happens, we are typically in touch with law enforcement.

We provide them with information that relates to these kinds of circumstances. In other circumstances the law enforcement people, the FTC come to us with a request for information about a particular merchant, and in those circumstances what we tend to do is we pass the investigating agency, the FTC or whoever, on to the financial institution that has the relationship with the merchant.

Those financial institutions are the ones who sign up the merchant for using a VISA card. They have all the records and the data about that particular merchant. And from then on the financial institution and the law enforcement agency, and the FTC, engage in a discussion and a dialogue about sharing information.

What we are seeing is that more and more internet merchants and fraudsters are moving to a situation where they are dealing with an off-shore bank, and they are not dealing with a U.S. bank.

And so when we tell the FTC or other law enforcement agencies in the United States that the bank involved is a bank outside of the United States, and the merchant is located outside of the United States as well, they then have to turn around and try to deal with that foreign institution.

And typically they have to be able to deal with foreign law enforcement institutions to get the information that they need, and that is why the FTC's initiative in this area to have greater cooperation is something that is so important. We are seeing more, and more, and more the circumstance of where when we provide the information to the FTC, it is information about foreign merchants using foreign off-shore banks.

And they then have to turn around and go to foreign institutions to get the information that will allow them to pursue the investigation.

Mr. STEARNS. My time has expired. The ranking member, Ms. Schakowsky.

Ms. SCHAKOWSKY. Really, my only question is to establish your willingness, Mr. Rotenberg and Mr. Schwartz, to continue to—if you would be willing to continue to provide us language and suggestions, because Mr. Muris confirmed that what we are dealing with is a work in progress.

And you can see that questions about the fine balance have been raised on both sides of the aisle, and it seems to me that in this collaborative process that we have been having that we have a real good chance at developing a bill that addresses both the consumer protection concerns and the civil liberties concerns.

So I want to thank you for your input until now, but the latest draft that came from the FTC yesterday was an improvement. It

still does raise those other questions, and my hope is that with your help and with the cooperation from both sides of the aisle that we can move forward. So I just wanted to reaffirm your—

Mr. SCHWARTZ. Yes, we are definitely interested in working with you, and we have been working with the commission for the past few weeks on this as well, and I would like to echo Mr. MacCarthy's praise of Commissioner Thompson, who has been particularly open and has had an open-door policy, and letting us come in and talk over some of the issues with him.

Ms. SCHAKOWSKY. And I would like to say that as well. I had a long conversation with him yesterday, too, and so it seems that all the important stakeholders have been at the table, and continue to be, and I think that is the way that we ought to operate around here. Thank you.

Mr. SHIMKUS [presiding]. Mr. Otter.

Mr. OTTER. Thank you, Mr. Chairman. Let me also associate myself with the remarks of the ranking member. I appreciate the problem that you have, but I am also concerned about what we do to the basis of our republic, and especially the right to privacy, and especially all of those rights and liberties that we enjoy as a result of the basis of our constitutional government.

Mr. Rotenberg, you said during your testimony that these agencies were subject to oversight and accountability. Where?

Mr. ROTENBERG. That is a very good question, Congressman. I think the point that I was trying to make was that they should be subject to oversight and accountability. And there is a number of ways that this happens.

And obviously the oversight committees play a role, and the courts play a bit of a role, but I also think the public plays a very important role, and part of my concern about the limitations on the use of the open government laws in this bill is that it would make it more difficult for the public to find out how the FTC operates, and what information is being turned over to other agencies and other governments.

And as I looked more closely at the July 15th draft, I noticed something also that was interesting. While those new exemptions for FOIA are being created, there still is a provision in there that says that nothing in this bill limits the ability of the Congress or the courts to get access to the information, which means that it has occurred to someone that it would not be a good idea to make this enforcement authority completely secret.

That information will be available to the Congress, but I think that it needs to be available to the public. So my answer to your question, Congressman, is that oversight happens partly because the public has the ability to understand how its government is operating.

Mr. OTTER. While I don't disagree with your response, I would only engage in a further discussion here for enlightenment; that that may well be the oversight. But that I still find absent the accountability.

Accountability to me would mean that we could take some action against the agent or the agency, and actions that was appropriate in a violation of the Fourth, Fifth, and Sixth, or whatever amendment that it was.

And I find that absent across the board in our government, and by the way, the public is not extending these authorities to the government. The Congress is. It is our responsibility to provide if you will the framework of the rules and regulations by which our government operates.

The public's responsibility is to decide whether or not we ought to be the ones making that decision, and the Administration's responsibility is to push that just as far as they can, and it has been my experience that they always have. And so we must be very, very selfish I think about the authorities that we extend, and I still find absent in all of this stuff the accountability. Who gets punished if they violate the liberties, if they violate the rights or privacy? Who gets punished? Do you define punishment in here?

Mr. ROTENBERG. Congressman, the answer to that point is no. I don't think there is sufficient accountability.

Mr. OTTER. Am I right in reading—excuse me, but am I right in reading, is that the results of the accountability? Is that how we manifest accountability, is by some sort of punishment, or firing them, or whatever?

Mr. ROTENBERG. Well, I think there are a variety of techniques. I mean, one thing which we recommended earlier this summer, which the chairman supported this morning, was new reporting requirements.

And our view was that if you are going to give an agency new authority, you have to know how that authority is being used, and those reporting requirements can be very detailed. It can be required on an annual basis.

It should be made available to the public, and anyone who wants to know how much information was turned over to which governments, and what were the outcomes. They should have a right to know that. That is part of the accountability.

I am concerned as you are also, Congressman, about a provision in this bill which basically creates immunity for private parties to turn over personal information to the FTC as it pursues these investigations with foreign governments.

There is a new immunity provision in this bill, and it basically says to a bank, or a telephone company, or an internet service provider, that if the Federal Trade Commission comes to you and asks for information for one of these investigations, and you turn it over wrongfully it is later determined, you are still immune from any prosecution because of this act.

Now, I can understand on the law enforcement side why they do that. That's how they get cooperation. But the effect for the customer of those companies is that the rights that they would have otherwise have been removed. So I am completely in agreement.

Mr. OTTER. I just want to ask the panel one more question, and that is we keep talking about fraud and deception, and fraud and deception, and that it is a civil result. Can you ever conceive where fraud and deception would eventually turn into a criminal action, and where would we get the evidence then to pursue the criminal action once we have established fraud and deception?

Mr. ROTENBERG. That is another important point. I think the term civil is being misused a little bit this morning. I mean, these

are authorities of the government that fall in the broad category of criminal investigations.

And when we talk about civil litigation and civil discovery and delayed notification between private parties, it is completely different. In fact, in that context, people usually know when their records are being sought in a civil matter, because the way that they are obtained is through subpoena and civil discovery.

It is an unusual process to be able to obtain information secretly, and we do that in criminal investigations because of specific concerns that we have about targets of those investigations.

Mr. OTTER. If I might ask both Mr. Schwartz and Mr. MacCarthy to respond to that question.

Mr. SHIMKUS. Without objection, go ahead.

Mr. MACCARTHY. I don't have much to add on the civil versus criminal part of your question, but if I could take the opportunity to quickly respond to Marc's point about immunity. It puts companies like ours in a very awkward situation if we receive a request for information from the government, and it is all perfectly legitimate and above-board, and we cooperate with that.

And in a later process it sounds that somebody somewhere and not us, but somebody somewhere else didn't follow all the rules and regulations. If then we are liable for violating other rules, it makes it very, very difficult for us to be cooperative in that kind of circumstance. So for us the immunity provision does create an enormously important part of the legislation.

Mr. SCHWARTZ. I don't have that much to add either. I would just say that the comment that Chairman Muris made earlier that he saw some points where he would like to see more criminal actions taken in some of these civil cases.

And I was kind of interested to hear what he meant by that, and what kind of cases that he was talking about there in particular. He did not really go into too much detail there, and I would be interested to follow up on that point.

Mr. SHIMKUS. Thank you, Mr. Otter. Mr. MacCarthy, in regard to complying to a request for information as you were just mentioning, from the FTC, is that simply a letter, or are you replying to a subpoena? The Chairman had mentioned that they still use subpoenas.

Mr. MACCARTHY. It depends on the individual agency and the individual case. Often it is a CID or a subpoena that we are responding to. Whenever it is necessary, we require that in order to respond appropriately to the agencies.

Mr. SHIMKUS. All right. And in those subpoenas the information is usually fairly specific isn't it?

Mr. MACCARTHY. That's correct.

Mr. SHIMKUS. And then, Mr. Rotenberg, wouldn't one of the abilities of accountability be the subpoena? Can you describe what the process that is proposed in here? This is not an agency-issued subpoena is it? They have to go outside the agency where there would be some review?

Mr. ROTENBERG. Right. But still—and this was in response to the question from Mr. Otter. Still in other circumstances, there may be some remedy available to the target of an investigation where a

subpoena is wrongfully issued, or information is improperly disclosed.

The effect of the immunity provision here is to remove those options, and I would just suggest, Mr. Chairman, that in understanding the use of this new authority that when it is directed against people who aren't engaged in criminal conduct, there can be very serious repercussions, and I think we need to be aware of that.

Mr. SHIMKUS. Well, I think that is one of the reasons why at least for myself that it is important that when they seek this type of information that they have an independent review of the request and the information for which they are acting upon is real.

And that's why I think that a subpoena is absolutely necessary, and that does cover VISA and other entities in its specifics. So I would probably vote against this bill if it wasn't for that fact. Mr. Schwartz, do you have anything to add on the subpoena aspect and whether that provides sufficient accountability?

Mr. SCHWARTZ. No, I don't.

Mr. SHIMKUS. All right. The other area of discussion seems to be the 90 day notice, and Chairman Muris had mentioned that they need the 90 days because it is difficult to track internet fraud in particular, and that 48 hours may not be enough.

Mr. Rotenberg, you mentioned that maybe 48 hours would be more appropriate at 90 days, and then maybe another 90 days, and then another 90 days. And, Mr. Schwartz, you didn't mention anything about even 48 hours. So could you rebut the Chairman's, or agree, whatever you want to comment.

Mr. ROTENBERG. I should clarify, Mr. Chairman, because maybe I was a little confusing in my remarks. There are actually a couple of different ways delayed notification works, in the wiretap realm.

The 48 hours actually refers to the ability to conduct a search without going to a judge, and without obtaining a warrant. And if you have emergency circumstances, you can conduct that search and come back 48 hours later, or within 48 hours, and get the warrant.

The number that I was focusing on, and which I think is actually a good number for this bill, is 30 days. I think 30 days is a good period of time. And if it is the case in this on-line environment that things are happening quickly, and people are moving funds quickly, I would say that you would want to act sooner rather than later.

I think that 90 days or a year just opens the door to make it more difficult to move these investigations quickly. So that would be my proposal.

Mr. SHIMKUS. And I think that is a valid proposal. Mr. Schwartz.

Mr. SCHWARTZ. Well, as I said, I think that we would be open to discussing how to make this clear. I think under the July 15th draft that there was no—that the judge basically had to approve it, and Chairman Muris went into some details, saying that they want to open up the idea of making sure that there is a court order and under a judge's discretion.

If that is the case, the idea of looking for some kind of flight risk as part of this I think would be appropriate, and the issue of—I do agree that it is more difficult on the internet to track, and the time periods may be a little bit different there.

If you look at some of the spam cases that they have gone into, a lot of them are bouncing mail off servers in Shanghai specifically to hide the tracking of where the mail comes from, and I think that does prove that there is some international aspect to it that they don't have in the telemarketing cases.

So the time period I think is up for discussion. Thirty days with renewal sounds reasonable, I think; and 60 and 90 days sounds reasonable, depending on the circumstance, and I think we should discuss that in a little more detail. It is not something that we have really vetted with the FTC at this point.

Mr. SHIMKUS. Thank you. I think those comments are helpful, and certainly we will consider those. On behalf of Chairman Stearns and the ranking member, and the entire subcommittee. I thank you for your time coming in here today and helping to shape this important legislation, and the subcommittee now stands adjourned.

[Whereupon, at 11:43 a.m., the subcommittee was adjourned.]

○