AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

H.R. ———, A BILL TO RENEW THE FEDERAL TRADE COMMISSION'S AUTHORITY TO COMBAT CROSS–BORDER SPAM, SPYWARE, AND FRAUD THROUGH REAUTHORIZATION OF THE U.S. SAFE WEB ACT OF 2006

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JULY 12, 2012

Serial No. 112–164

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

82–427 PDF WASHINGTON : 2013

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chairman
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MARY BONO MACK, California
Chairman

MARSHA BLACKBURN, Tennessee
Vice Chairman
CLIFF STEARNS, Florida
CHARLES F. BASS, New Hampshire
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

G.K. BUTTERFIELD, North Carolina
Ranking Member
CHARLES A. GONZALEZ, Texas
JIM MATHESON, Utah
JOHN D. DINGELL, Michigan
EDOLPHUS TOWNS, New York
BOBBY L. RUSH, Illinois
JANICE D. SCHAKOWSKY, Illinois
JOHN P. SARBANES, Maryland
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

	Page
Hon. Mary Bono Mack, a Representative in Congress from the State of California, opening statement	1
Prepared statement	4
Hon. G.K. Butterfield, a Representative in Congress from the State of North Carolina, opening statement	8
Hon. Henry A. Waxman, a Representative in Congress from the State of California, prepared statement	41
Hon. Edolphus Towns, a Representative in Congress from the State of New York, prepared statement	43

WITNESSES

Hugh G. Stevenson, Deputy Director for International Consumer Protection, Federal Trade Commission	9
Prepared statement	11

SUBMITTED MATERIAL

Discussion Draft of H.R. ———, A Bill To extend the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006, and for other purposes, dated July 3, 2012, submitted by Mrs. Bono Mack	6

H.R. ———, A BILL TO RENEW THE FEDERAL TRADE COMMISSION'S AUTHORITY TO COMBAT CROSS–BORDER SPAM, SPYWARE, AND FRAUD THROUGH REAUTHORIZATION OF THE U.S. SAFE WEB ACT OF 2006

THURSDAY, JULY 12, 2012

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

The subcommittee met, pursuant to call, at 10:00 a.m., in room 2322 of the Rayburn House Office Building, Hon. Mary Bono Mack (chairman of the subcommittee) presiding.

Members present: Representatives Bono Mack, Harper, Lance, Cassidy, Guthrie, Butterfield, and Gonzalez.

Staff present: Paige Anderson, Commerce, Manufacturing, and Trade Coordinator; Kirby Howard, Legislative Clerk; Brian McCullough, Senior Professional Staff Member, Commerce, Manufacturing, and Trade; Gib Mullan, Chief Counsel, Commerce, Manufacturing, and Trade; Andrew Powaleny, Deputy Press Secretary; Shannon Weinberg Taylor, Counsel, Commerce, Manufacturing, and Trade; Michelle Ash, Democratic Chief Counsel, Commerce, Manufacturing, and Trade; Felipe Mendoza, Democratic Senior Counsel; and Will Wallace, Democratic Policy Analyst.

OPENING STATEMENT OF HON. MARY BONO MACK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mrs. BONO MACK. We will now come to order.

Good morning, everybody. The purpose of today's hearing is to provide subcommittee members with an opportunity to review and discuss the U.S. SAFE WEB Act of 2006. And the chair now recognizes herself for an opening statement.

When it comes to the future of electronic commerce, consumer trust and online privacy are certainly "trending topics." Even though it serves billions of users worldwide—with e-commerce in the United States topping $200 billion last year for the first time and up 15 percent so far this year—the Internet very much remains a work in progress. Still, in just over 25 years, the Internet already has spurred transformative innovations. It has incalculable value. It has become part of our daily lives. And it has unlimited potential to affect positive social and political change. But do Amer-

icans really believe enough is being done today to protect them from online fraud?

Frankly, I am concerned that e-commerce will cease to grow and flourish if consumers lose faith in their ability to be protected from online predators, jeopardizing future innovation as well as our Nation's fragile economic recovery.

One important tool in combating cross-border fraud, spam, and spyware is the U.S. SAFE WEB Act of 2006, which is set to expire next year. Today we will be considering legislation which I plan to introduce this week to reauthorize this important crime-fighting and consumer protection law for another 7 years.

Clearly, there is a lot at stake. About a decade ago, the FTC began to highlight the growing problems it encountered in effectively combating Internet scams and fraud directed at American citizens by foreign operators, oftentimes involving organized crime rings. By 2005, an estimated 20 percent of consumer complaints the FTC received involved fraud originating outside of the U.S. According to an analysis of those complaints from the Consumer Sentinel Network, Americans suffered annual losses to foreign operators totaling nearly $220 million.

The FTC subsequently identified severe limitations in its authority to combat cross-border fraud, spam, and spyware relative to that of other U.S. regulators. The biggest roadblock to protecting consumers was the Commission's lack of authority to share information with foreign law enforcement agencies.

In order to expand its ability to effectively fight online fraud, the FTC sent Congress legislative recommendations in 2005 seeking additional authorities. Without objection, Congress passed the U.S. SAFE WEB Act on December 6 of 2006, and it was then signed into law by President Bush on December 22 of 2006. Pursuant to the Act, the FTC issued a report in 2009, "The U.S. SAFE WEB Act: The First Three Years," detailing its use and day-to-day experience with the authority granted by the law.

Over a 3-year period, covering 2006 through 2008, the FTC received more than a quarter of a million cross-border complaints by American consumers. The FTC also reported that it shared confidential information in response to 38 requests from 14 foreign agencies in six countries, resulting in numerous enforcement proceedings.

By any measure, the U.S. SAFE WEB Act has been a clear success to date and should be reauthorized before its expiration next year. Let me emphasize a very important point: Our goal is to pass a clean reauthorization of the law, and my draft legislation does exactly that.

The U.S. SAFE WEB Act amends the FTC Act, authorizing the Commission to share information involving cross-border fraud with foreign consumer protection agencies, subject to important safeguards; protect from public disclosure confidential information received from foreign consumer protection agencies that otherwise would not be shared; pursue a broader class of frauds, involving international activity that harms U.S. consumers; seek redress on behalf of foreign as well as U.S. consumers victimized by U.S.-based wrongdoers; and finally, make criminal referrals for cross-border criminal activity when violations of FTC law also violate

U.S. criminal law. This is necessary because some foreign agencies address consumer fraud as a criminal—rather than civil—law enforcement issue.

Today, with nearly 1.5 billion credit cards now in use in the United States, nearly everyone in America has a stake in making certain that the FTC has the powers it needs to combat cross-border fraud, spam, and spyware.

In closing, let me emphasize, this is a very important bill, and I am asking for your favorable consideration as we begin the process of reauthorizing the U.S. SAFE WEB Act. It is good for American consumers, it is good for the future of e-commerce, and it is the right thing to do.

And with that, I would like to now recognize the ranking member of our subcommittee and my friend, Mr. Butterfield of North Carolina, for his opening statement.

[The prepared statement of Mrs. Bono Mack and the proposed legislation follow:]

Opening Statement of the Honorable Mary Bono Mack
Subcommittee on Commerce, Manufacturing, and Trade
Legislative Hearing on "H.R. __, a bill to renew the Federal Trade Commission's authority to combat cross-border spam, spyware and fraud through reauthorization of the U.S. SAFE WEB Act of 2006"
July 12, 2012

(As Prepared for Delivery)

When it comes to the future of electronic commerce, consumer trust and online privacy are certainly "trending topics."

Even though it serves billions of users worldwide – with e-commerce in the United States topping $200 billion last year for the first time and up 15 percent so far this year – the Internet remains a work in progress. Still, in just over 25 years, the Internet already has spurred transformative innovations. It has incalculable value. It has become part of our daily lives. And it has unlimited potential to affect positive social and political changes.

But do Americans really believe enough is being done today to protect them from online fraud?

Frankly, I'm concerned that e-commerce will cease to grow and flourish if consumers lose faith in their ability to be protected from online predators, jeopardizing future innovation as well as our nation's fragile economic recovery.

One important tool in combating cross-border fraud, spam and spyware is the U.S. SAFE WEB Act of 2006, which is set to expire next year. Today, we will be considering legislation which I am introducing this week to reauthorize this important crime-fighting & consumer protection law for another seven years.

Clearly, there's a lot at stake. About a decade ago, the Federal Trade Commission began to highlight the growing problems it encountered in effectively combating Internet scams and fraud directed at American citizens by foreign operators, often times involving organized crime rings.

By 2005, an estimated 20 percent of consumer complaints the FTC received involved fraud originating outside of the United States. According to an analysis of those complaints from the Consumer Sentinel Network, Americans suffered annual losses to foreign operators, totaling nearly $220 million.

The FTC subsequently identified severe limitations in its authority to combat cross-border fraud, spam and spyware relative to that of other U.S. regulators.

The biggest roadblock to protecting consumers was the Commission's lack of authority to share information with foreign law enforcement agencies.

In order to expand its ability to effectively fight online fraud, the FTC sent Congress legislative recommendations in 2005 seeking additional authorities. Without objection, Congress passed the

U.S. SAFE WEB Act on December 6, 2006, and it was then signed into law by President Bush on December 22, 2006.

Pursuant to the Act, the FTC issued a report in 2009, *"The U.S. SAFE WEB Act: The First Three Years"*, detailing its use and day-to-day experience with the authority granted by the law.

Over a three-year period, covering 2006 through 2008, the FTC received more than a quarter of a million cross-border complaints by American consumers. The FTC also reported that it shared confidential information in response to 38 requests from 14 foreign agencies in six countries, resulting in numerous enforcement proceedings.

By any measure, the U.S. SAFE WEB Act has been a clear success to date and should be reauthorized before its expiration next year.

Let me emphasize an important point: Our goal is to pass a clean reauthorization of the law, and my draft legislation does exactly that.

The U.S. SAFE WEB amends the FTC Act, authorizing the Commission to:

- Share information involving cross border fraud with foreign consumer protection agencies, subject to important safeguards;
- Protect from public disclosure confidential information received from foreign consumer protection agencies that otherwise would not be shared;
- Pursue a broader class of frauds, involving international activity that harms U.S. consumers;
- Seek redress on behalf of foreign as well as U.S. consumers victimized by U.S.-based wrong-doers; and finally
- Make criminal referrals for cross-border criminal activity when violations of FTC law also violate U.S. criminal law. This is necessary because some foreign agencies address consumer fraud as a criminal – rather than civil – law enforcement issue.

Today, with nearly 1.5 billion credit cards now in use in the United States, nearly everyone in America has a stake in making certain that the Federal Trade Commission has the powers it needs to combat cross-border fraud, spam and spyware.

In closing, let me emphasize, this is a very important bill, and I am asking for your favorable consideration as we begin the process of reauthorizing the U.S. SAFE WEB Act. It's good for American consumers. It's good for the future of e-commerce. And it's the right thing to do.

[DISCUSSION DRAFT]

JULY 3, 2012

112TH CONGRESS
2D SESSION

H. R. _____

To extend the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To extend the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. EXTENSION OF THE U.S. SAFE WEB ACT OF 2006.

Section 13 of the U.S. SAFE WEB Act of 2006 (Public Law 109–455; 15 U.S.C. 44 note) is amended to read as follows:

1 **"SEC. 13. SUNSET.**

2 "Effective September 30, 2020, this Act, and the
3 amendments made by this Act, are repealed, and any pro-
4 vision of law amended by this Act shall be amended to
5 read as if this Act had not been enacted into law.".

OPENING STATEMENT OF HON. G.K. BUTTERFIELD, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

Mr. BUTTERFIELD. Madam Chairman, I thank you for holding today's hearing on reauthorizing the U.S. SAFE WEB Act of 2006.

When the Act passed in the 109th Congress, it was overwhelmingly supported by both Republicans and Democrats, and it passed the House under suspension of the rules. The law provides the FTC with expanded and enhanced authorities with the aim to combat cross-border spyware and spam attacks against the United States, as well as to help protect consumers against phony Internet rip-offs and telemarketing scams. The enhanced authority has empowered the FTC to better protect American consumers through robust cross-border information sharing, investigative assistance and correlation-building with foreign consumer protection agencies.

In a 2009 report to Congress, the FTC noted that "the Act has helped overcome cross-border enforcement challenges it faced in the past, and it is critical to the FTC's ability to combat global scams that consumers will face in the future." Simply put, the expanded authorities are working to protect the American people.

The SAFE WEB Act included a sunset provision that will cause these enhanced authorities to expire in December of 2013 if Congress does not act. The proposed bill we are discussing today will, if passed, extend the law to September 2020. While I support these important consumer protection provisions being extended, I join the current commissioners of both political parties in calling for this reauthorization to be continued in perpetuity.

I hope that my colleagues will agree that this law is paying dividends to the American people. Instead of including another sunset provision in any reauthorization, we should strongly weigh the unanimous support of the commissioners to make it permanent.

I look forward to hearing from today's witness from the Commission, Mr. Stevenson, and appreciate him being here today.

Madam Chairman, I look forward to working with you and our colleagues on the subcommittee in fully authorizing this very important and successful law. Thank you.

Mrs. BONO MACK. Thank you, Mr. Butterfield.

And seeing no other members who wish to make opening statements, we will turn our attention to our one witness that is joining us today. We have Hugh G. Stevenson, Deputy Director for International Consumer Protection at the Office of International Affairs at the Federal Trade Commission. Thank you very much for being here. Mr. Stevenson has prepared an opening statement that will be placed into the record. He will now have 5 minutes to summarize his statement in his remarks.

Again, thank you for coming. If you can just look at the little clock in front of you—it is a timekeeper, kind of typical American values—green means goes, yellow means start wrapping it up or hit the gas, and red means try to come to a conclusion. Please just remember to turn your microphone on and bring it close to your mouth so that the TV audience at home can hear you.

And with that, Mr. Stevenson, you are recognized for your 5 minutes.

STATEMENT OF HUGH G. STEVENSON, DEPUTY DIRECTOR FOR INTERNATIONAL CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Mr. STEVENSON. Thank you very much. Chairman Bono Mack, Ranking Member Butterfield, honorable members of this committee, my name is Hugh Stevenson. I am the deputy director for International Consumer Protection at the Federal Trade Commission, and I am here on behalf of the FTC to speak in support of renewing the U.S. SAFE WEB Act.

As you know, part of our bread and butter is bringing enforcement actions to protect U.S. consumers from fraud, from deception, from other commercial misconduct. And more and more, these enforcement actions cross borders. The defendants can be in other countries, the money can go to other countries, the evidence can sometimes only be found in other countries. The SAFE WEB Act of 2006 has provided us with key enforcement tools we need more and more to do this bread-and-butter work. And as you have recognized, unless you take action, we lose the Act's powers next year.

Now, what does this problem—cross-border fraud—look like? If we look at our joint database and consumer sentinel, we see hundreds of thousands of cross-border complaints from your constituents. We see millions of robocalls sent from outside the United States. We have seen millions of bogus debt-collection calls. In our cross-border cases, we have seen hundreds of millions of dollars in injury to U.S. consumers. And in our spam work, in one case alone, we have seen billions of spam messages sent.

Technology with a global reach has become even more prevalent, even more the new normal since 2006. The new technologies—and not just the web and email but increasingly also mobile devices—Smartphones, new methods of payment, voiceover IP, robocalls—all this means the frauds are faster, the frauds can reach farther, and the frauds are harder to discover.

What does the SAFE WEB Act do to help us here? It helps us to work together with agencies in other countries to investigate and bring cases using our subpoena power to get information, share it, get more information back. Easy example: We subpoenaed information from a U.S. company and shared it with the Toronto Police Service, which was investigating a scam that was targeting both U.S. and Canadian consumers, helped link the suspects to the scam, led to 14 arrests. Another simple example, payday lender case: We shared information with a U.K. agency, they shared information with us, we filed an action in court and obtained a million-dollar settlement with U.S. and U.K. defendants. The SAFE WEB Act also confirms that we have jurisdiction to pursue these cases and helps us build networks so necessary with our fellow enforcers.

Let me emphasize also what the SAFE WEB Act does not do. The Act does not set new substantive rules for business. It hasn't given us any new substantive rulemaking powers. What it does is provide us with enforcement tools.

The Act also does not cover every conceivable case. It limits cooperation to cases of fraud, deception, and other misconduct that is substantially similar to practices that already violate the FTC's consumer laws.

The FTC has referred many times in many contexts over many years to the need for just this kind of legislation, and we need the SAFE WEB Act now more than ever to meet the challenge of effective protection for U.S. consumers.

Thank you for your attention and I would be glad to answer any questions.

[The prepared statement of Mr. Stevenson follows:]

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Reauthorizing the U.S. SAFE WEB Act of 2006

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

July 12, 2012

I. INTRODUCTION

Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee, I am Hugh Stevenson, Deputy Director for International Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the FTC's testimony in support of renewing the authority that Congress granted to the FTC in the U.S. SAFE WEB Act of 2006. Without Congressional action, the Act will sunset in December 2013.

Congress passed the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 ("U.S. SAFE WEB Act," "SAFE WEB Act," or "Act")[2] to enhance FTC enforcement against cross-border fraud threatening American consumers in the global marketplace. The Act arms the FTC with key enforcement tools to combat Internet scams, fraudulent telemarketing, spam, spyware, and other cross-border misconduct that harms our consumers. In this Act, Congress gave the FTC enforcement tools similar to those long available to the Securities and Exchange Commission and the Commodity Futures Trading Commission.[3]

---

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner.

[2] Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 ("U.S. SAFE WEB Act"), Pub. L. No. 109-455, 120 Stat. 3372 (2006) (codified in scattered sections of 15 U.S.C. and 12 U.S.C. § 3412(e)). A copy of the public law is available at http://www.gpo.gov/fdsys/pkg/PLAW-109publ455/pdf/PLAW-109publ455.pdf.

[3] *See* Securities Acts Amendments of 1990, Pub. L. 101-550, 104 Stat. 2713 (1990); *see also* Futures Trading Practices Act of 1992, Pub. L. No. 102-546, § 302, 106 Stat. 3590, 3622 (1992). Neither the SEC legislation nor the CFTC legislation contained a sunset provision. Accordingly, over the past 22 years, the SEC has used its cross-border enforcement powers to develop strong enforcement cooperation arrangements — including a multilateral memorandum of understanding under the auspices of the International Organization of Securities Commissions (IOSCO) — based on its statutory authority to collect and share investigatory information when there are suspicions of securities laws violations in foreign jurisdictions. This has allowed the SEC to pursue foreign securities frauds that harm American investors. The CFTC has engaged in similar efforts. Moreover, since passing the SAFE WEB Act, Congress has given similar authority to the Consumer Product Safety Commission. *See* Consumer Product Safety Improvement Act of 2008 - Public Law 110- 314, codified at 15 U.S.C. § 2078.

To continue to protect American consumers in a global economy, the FTC believes it is critical that Congress reauthorize the law enforcement tools provided by the U.S. SAFE WEB Act. Every FTC Commissioner who has addressed the issue — three Democrats, three Republicans, and an independent — has supported reauthorization of the Act.[4]

This testimony first describes the problem of cross-border fraud and provides a brief history of the Act. It then describes how the FTC has used the Act's enforcement tools to protect U.S. consumers, particularly in four key areas: (1) information sharing; (2) investigative assistance; (3) cross-border jurisdictional authority; and (4) enforcement relationships. Finally, it discusses the ongoing cross-border challenges and the continuing need for the SAFE WEB Act.

II. THE CROSS-BORDER FRAUD CHALLENGE AND PASSAGE OF THE U.S. SAFE WEB ACT

Globalization of trade, improvements in international telecommunications, outsourcing, and the advent of the Internet have created unprecedented new opportunities for consumers and businesses. But these developments have also posed new problems for the FTC and American consumers. The problems for American consumers, described in prior FTC testimony,[5] have ranged from traditional scams that thrived online, such as pyramid schemes and business operations making false product claims, and aggressive advance-fee loan, foreign lottery, and sweepstakes telemarketing schemes, to Internet-enabled frauds like spoofed emails, web

---

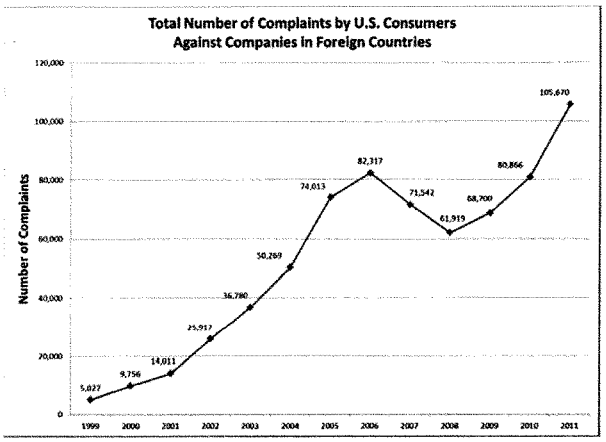
[4] All five of the current Commissioners support reauthorization. Previously, in 2011, all five Commissioners then serving, including former Commissioner William Kovacic, wrote to the leadership of the FTC's authorizing House and Senate committees to urge renewal. In 2009, all four Commissioners then serving, including former Commissioner Pamela Jones Harbour, voted for the 2009 FTC report recommending reauthorization. Similarly, five Commissioners unanimously recommended passage of what became the SAFE WEB Act in a 2005 report to Congress. *See* discussion in section II, *infra*.

[5] *See* Hearing on Internet Fraud Before the Comm. on Finance, 107th Cong. (2001) (statement of the Federal Trade Commission), *available at* http://www.ftc.gov/os/2001/04/internetfraudstate.htm; Hearing on Internet Fraud Before the Subcomm. on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce, 107th Cong. (2001) (statement of the Federal Trade Commission), *available at* http://www2.ftc.gov/os/2001/05/internetfraudttmy.htm; Hearing on Cross Border Fraud Before the Subcomm. on Investigations of the Sen. Comm. on Governmental Affairs, 107th Cong. (2001) (statement of the Federal Trade Commission), *available at* http://www.ftc.gov/os/2001/06/cbftest.htm.

addresses, and computer system scans. The challenges for the FTC and other law enforcers have included the global reach and speed of the Internet; the ability of scammers to cloak themselves in anonymity; the ease of moving ill-gotten gains to offshore asset havens; and the roadblocks to information sharing and cooperation created by national laws and borders.[6]

Cross-border fraud is an ongoing problem. The FTC's *Consumer Sentinel* database, which combines consumer fraud complaints received by an array of enforcement agencies and other organizations,[7] suggests the scope of the problem:

- Between 2006 and 2011, almost half a million U.S. consumers (471,014) complained about transactions involving more than $1.4 billion paid to businesses in other countries.[8]
- The number of U.S. consumer complaints against foreign businesses exceeded 100,000 in 2011 alone:



[6] *Id.*

[7] The Consumer Sentinel Network is a secure online database of millions of consumer complaints, available only to civil and criminal enforcement agencies, that provides immediate and secure access to fraud, identity theft, Internet, telemarketing (including Do Not Call), and other consumer-related complaints. *See* http://www.sentinel.gov. Note that complaints are included in the data by date of consumer complaint. Some organizations, however, transfer their complaints to the Consumer Sentinel Network after the end of the calendar year. As a result, reported totals and percentages may vary compared to previous years' reports.

[8] *See* Consumer Sentinel Network cross-border fraud reports for the calendar years 2002 to 2011, *available at* http://www.ftc.gov/sentinel/reports.shtml.

- Cross-border complaints have accounted for more than 10% of all *Consumer Sentinel* fraud complaints every year since 2000, with a high of 22% in 2006 and 13% for each of the last three years. These numbers likely understate the scope of the problem, as this complaint count includes only those instances where consumers report a foreign address.[9]

- U.S. consumers complain about foreign businesses from an increasingly broad range of countries. In 2002 more than 55% of such complaints were about Canadian businesses; in 2011 more than 85% were about businesses in other foreign countries.[10]

In 2005, the FTC sent a legislative recommendation to Congress to meet these challenges and enhance the FTC's enforcement against cross-border fraud.[11] The FTC also submitted a report to Congress that detailed the types of misconduct involved and the harms its victims experienced.[12] On December 8, 2006, Congress passed the SAFE WEB Act,[13] which was signed into law on December 22, 2006.[14] The Act required the FTC to report on experience with the Act after three years, and included a seven-year sunset.[15]

In 2009, the FTC submitted the required three-year report to Congress, detailing how the agency had used its new authority under each provision of the Act to protect consumers in the global economy.[16] The 2009 report noted the "significant role the Act has played in facilitating cross-border cooperation in investigations and enforcement proceedings, along with the growing need for continued cooperation to combat new and existing global fraud," and requested that

---

[9] In some instances the company address provided by the consumer actually is a mail drop in the consumer's country rather than the physical location of the company in a foreign country. In other cases, the consumer does not know whether the location is in the U.S. or abroad, for example in dealing with a website, email, or phone contact.
[10] *See* Consumer Sentinel Network cross-border fraud reports for 2011 and 2002, *available at* http://www.ftc.gov/sentinel/reports/annual-crossborder-reports/crossborder-cy2011.pdf and http://www.ftc.gov/sentinel/reports/annual-crossborder-reports/crossborder-cy2002.pdf.
[11] FTC, *The US SAFE WEB Act — Protecting Consumers from Spam, Spyware, and Fraud:A Legislative Recommendation to Congress* (June 2005), *available at* http://www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf.
[12] *Id.*
[13] *See* Statement of Federal Trade Commission Chairman Deborah Platt Majoras on Passage of the US SAFE WEB Act by the 109th Congress, *available at* http://www.ftc.gov/speeches/majoras/061211statementUSSafeweb.pdf.
[14] *See* Statement by Federal Trade Commission Chairman Deborah Platt Majoras on US SAFE WEB Act Being Signed Into Law by President George W. Bush, *available at* http://www.ftc.gov/opa/2006/12/safeweblaw.shtm.
[15] *See* Act, §§ 13, 14.
[16] *See* FTC, *The U.S. SAFE WEB Act, The First Three Years: A Report to Congress* (Dec. 2009), *available at* http://www.ftc.gov/os/2009/12/P035303safewebact2009.pdf.

Congress strike the sunset provision.[17] Following this report, in October 2011 the FTC's five Commissioners submitted letters to congressional leaders, including to the leaders of this Subcommittee, urging repeal of the sunset provision and permanent reauthorization of the SAFE WEB Act.[18]

III. FTC USE OF SAFE WEB ACT TOOLS

The FTC has used the SAFE WEB Act's tools to protect American consumers from cross-border threats robustly and responsibly. Some numbers tell the story:

- The FTC has conducted more than 100 investigations with international components, such as foreign targets, evidence, or assets, and has filed more than 50 cases involving cross-border components, since January 2007. The FTC has used the Act's authority in many of these matters, and in related actions brought by other U.S. and foreign enforcement agencies.

- The FTC has provided evidence in response to 63 information-sharing requests from 17 foreign law enforcement agencies in nine countries as of mid-2012. This evidence sharing was possible only because of the authority granted by the Act.

- The FTC has issued 52 civil investigative demands (equivalent to administrative subpoenas) in 21 investigations on behalf of nine agencies in five countries, agencies that in many cases were investigating frauds targeting Americans.

- In cases relying on the SAFE WEB Act, the FTC has to date collected more than $10 million in restitution for injured consumers, despite the challenges of collecting money from defendants in foreign jurisdictions, and has stopped frauds costing American consumers hundreds of millions of dollars.

Even more important, the Act is key to strengthening a culture of mutual assistance that enables law enforcers to achieve greater results working together than they ever could alone. Tracing cause and effect in each case of cooperation and reciprocity is difficult, but one example of such cooperation and resulting enforcement actions is Operation Tele-PHONEY. There the

---

[17] *Id.* at 20.

[18] *See* Commission Letter to the Honorable Fred Upton, Henry Waxman, Mary Bono Mack, and G.K. Butterfield, U.S. House of Representatives Committee on Energy and Commerce, Requesting Repeal of the Sunset Provision of the U.S. SAFE WEB Act of 2006 (Oct. 3, 2011), *available at* http://www.ftc.gov/os/closings/111003safewebletter congress.pdf.

FTC, armed with SAFE WEB Act authority, worked together with U.S. and Canadian law enforcers to orchestrate a telemarketing enforcement sweep with 180 actions overall, including criminal actions against more than 90 defendants and several Canadian actions. Moreover, the 13 FTC actions brought as part of the sweep involved more than half a million consumers defrauded by unscrupulous telemarketers, resulting in losses of more than $100 million, and the agency estimated that as a result of the law enforcement actions consumers would save approximately $30 million over the following year.[19] Another example is the work of the Toronto Strategic Partnership, which includes the U.S. Postal Inspection Service, the Royal Canadian Mounted Police, and other Canadian civil and criminal enforcement agencies, which since 2000 has involved hundreds of arrests, hundreds of search warrants, and the shutting down of scams cheating U.S. and foreign consumers out of hundreds of millions of dollars.[20] The SAFE WEB Act enables the FTC to cooperate more fully in this kind of crucial partnership activity.

This cooperation has directly benefited U.S. consumers. The Act has improved the quantity and quality of evidence that the FTC can use against common targets, and has encouraged reciprocal assistance from enforcement agencies in other countries, especially Canada, which in 2010 passed a law with mutual assistance provisions modeled on the SAFE WEB Act.[21] This enables the FTC to act more quickly and effectively in shutting down

---

[19] *See* http://www.ftc.gov/opa/2008/05/telephoney.shtm.
[20] *See* http://www.ftc.gov/opa/2008/01/canada.shtm.
[21] The Canadian law, which vests three agencies with powers to cooperate on fraud, deception, spam, and privacy, was passed in December 2010 and is expected to enter into force later this year. More information is available from the Government of Canada at http://fightspam.gc.ca/eic/site/030.nsf/eng/home. At the time the Canadian legislation was under consideration, Canadian officials cited the U.S. SAFE WEB Act as a model for the type of legislation that was required for effective international cooperation. *See* Konrad von Finckenstein, Chairman, Canadian Radio-television and Telecommunications Commission, Speech to the Standing Committee on Industry, Science, and Technology (June 18, 2009), *available at* http://www.crtc.gc.ca/eng/com200/ 2009/s090618.htm (advocating for an amendment that would give his agency power to obtain and share information with authorities in foreign countries, such as the United States, that have reciprocal legislation).

egregious frauds and putting the defendants out of business and under court order, while at the same time helping foreign agencies to bring actions against foreign-based fraudsters that victimize American consumers.

The Act in particular enhances the FTC's consumer protection enforcement authority[22] in four key areas: (1) information sharing; (2) investigative assistance; (3) cross-border jurisdictional authority; and (4) enforcement relationships.[23]

A. Information Sharing

The Act authorizes the FTC to share confidential information in its files with foreign law enforcement agencies, subject to certain statutory safeguards.[24] This enforcement tool has proven particularly useful.

In one of the first uses of this enforcement tool, the FTC shared evidence with enforcers in Australia and New Zealand about an international spam network that peddled bogus prescription drugs, weight-loss pills and male-enhancement products to U.S. and foreign consumers. The network, which the anti-spam organization Spamhaus called the largest "spam gang" in the world, sent billions of spam emails.[25] Using this evidence, the New Zealand agency executed multiple search warrants, filed an enforcement action in New Zealand, and obtained several monetary settlements. The Australian agency also filed suit, obtaining injunctions and a $210,000 penalty from an Australian court. In turn, these actions helped the FTC obtain further evidence and nearly $19

[22] The Act's enforcement tools are not available for competition cases. *See* Act, §§ 4 (b), 6 (a).
[23] The Act also contains important confidentiality-related provisions and other enforcement tools enhancing the FTC's ability to work with both U.S. and foreign agencies, as detailed in the agency's 2009 report to Congress.
[24] *See* 15 U.S.C. §§ 46(f), 57b-2(b)(6). The foreign agency must fall within the FTC Act's definition of foreign law enforcement agency. *See* 15 U.S.C. § 44 (defining "law enforcement agency" as "any agency . . . of . . . a political subdivision of a foreign state . . . that is vested with law enforcement or investigative authority in civil, criminal, or administrative matters"). The requesting agency must certify that the information will be maintained in confidence and will be used only for official law enforcement purposes. Also, the requested material may only be used in connection with investigation and enforcement targeting possible violations of laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by a law administered by the FTC.
[25] *See* Spamhaus News, *available at* http://www.spamhaus.org/news/article/638/herbalking-principals-indicted-by-ftc-and-new-zealand.

million in default restitutionary judgments in its own civil case, and led to the criminal conviction of one of the defendants.[26] As the Australian agency put it, "This type of inter-agency, cross-jurisdictional collaboration is exactly what is required to combat the global scourge of spam."[27]

More recently, the FTC used the Act's information sharing provisions to help build its case against a Canadian and several related defendants who victimized nearly four million consumers—most of them Americans. The FTC alleged that the defendants lured consumers with "free" trial offers for weight-loss pills, teeth whiteners, health supplements, a work-at-home scheme, access to government grants, free credit reports, and penny auctions, and then charged them substantial and recurring fees on their credit cards. The FTC used the SAFE WEB Act to share information about the case with Canadian law enforcers, including the Competition Bureau and the Royal Canadian Mounted Police, which in turn provided investigative assistance to the FTC. The case resulted in the entry of U.S. court injunctions and monetary judgments.[28]

B. Investigative Assistance

The Act also permits the FTC to provide investigative assistance in consumer protection matters to foreign law enforcement agencies for fraudulent and deceptive commercial practices, and other practices "substantially similar" to those prohibited by FTC law.[29] If such requests meet the requirements of the Act,[30] the FTC may issue compulsory process for documents or

---

[26] *See FTC v. Atkinson*, No. 08-CV-5666 (N.D. Ill., filed Oct. 6, 2008), press release *available at* http://www.ftc.gov/opa/2008/10/herbalkings.shtm.

[27] Australia Communications and Media Authority, "Penalties awarded in email spam case in the Federal Court" (Dec. 22, 2009), *available at* http://www.acma.gov.au/WEB/STANDARD/pc=PC_311998.

[28] *FTC v. Jesse Willms*, No. 2:11-CV-00828 (W.D. Wash., filed May 16, 2011). Complaint and other court papers *available at* http://www.ftc.gov/os/caselist/1023012/index.shtm. The settlement order with the Canadian defendant imposes a judgment of $359 million, to be suspended upon Willms' surrender of bank account funds and proceeds from the sale of his house, personal property, and corporate assets, including a Cadillac Escalade, fur coat, and artwork.

[29] *See* 15 U.S.C. § 46(j).

[30] Requests for investigative assistance pursuant to SAFE WEB must be made in writing, and the foreign agency must state that it has an investigation or enforcement proceeding involving possible violations of laws prohibiting (1) fraudulent or deceptive commercial practices or (2) other practices substantially similar to practices prohibited

testimony to a U.S. entity (often a third party, such as a domain registrar) and share the information with the foreign agency. Before the Act was passed, the FTC could not provide such assistance — even if the foreign agency was investigating a fraud, or helping the FTC to investigate a fraud, that victimized U.S. consumers.

An example of how this enforcement tool has helped U.S. consumers comes from an Edmonton (Canada) Police Service investigation of Hazim Gaber, a Canadian who peddled cancer cure scams mainly to U.S., Canadian, and U.K. citizens. Gaber claimed to sell an experimental cancer drug, but actually sent victims a useless white powder. Using the Act's investigative assistance provisions, the FTC obtained evidence from a U.S. domain registrar that helped tie Gaber to websites associated with the scam. Ultimately, the FBI arrested Gaber in Germany and extradited him to the U.S. In March 2010, Gaber pled guilty to five counts of wire fraud for selling counterfeit cancer drugs. He was sentenced to 33 months in prison and three years of supervised release.[31]

C. Cross-Border Jurisdictional Authority

The SAFE WEB Act also provides enhanced litigation tools. Key among them is the Act's confirmation of the FTC's cross-border jurisdictional authority. The Act amended the core jurisdictional provisions in Section 5 of the FTC Act to confirm the agency's authority to

---

by any provision of the laws administered by the Commission. 15 U.S.C. § 46(j)(1). The Act also requires that the Commission consider all relevant factors, including: (1) whether the agency has agreed to provide or will provide reciprocal assistance to the Commission; (2) whether the request would prejudice U.S. public interest; and (3) whether the foreign agency's investigation or proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons. *See* 15 U.S.C. § 46(j)(3). Finally, section 6(j)(1), (6)-(7) of the FTC Act, 15 U.S.C. § 46(j)(1), (6)-(7), also sets forth exceptions to the Commission's authority to render investigative assistance to foreign law enforcement agencies. The Act prohibits the Commission from providing investigative assistance if: (1) the foreign agency's investigation or enforcement proceeding involves the enforcement of antitrust laws; (2) the targets of the foreign agency's investigation or proceeding are banks, savings and loan institutions, federal credit unions, or common carriers; or (3) the agency is from a foreign state that the Secretary of State has determined repeatedly provides support for acts of international terrorism.

[31] *See* Department of Justice Press Release, "Canadian Man Sentenced to 33 Months in Prison for Selling Counterfeit Cancer Drugs Using the Internet," *available at* http://www.justice.gov/opa/pr/2010/August/10-crm-958.html.

challenge both frauds from abroad that harm U.S. consumers and frauds involving material conduct in the United States, including those that victimize foreign consumers.[32] The amendment also confirms the availability of monetary restitution to consumers as a remedy for domestic and foreign victims of FTC Act violations.[33]

These provisions are crucial to the FTC's ability to sue foreign defendants who harm U.S. consumers, helping the FTC to overcome arguments about the scope of its cross-border consumer protection jurisdiction. In *FTC v. Innovative Marketing, Inc.*,[34] for example, the FTC alleged that defendants used "scareware" to trick millions of consumers around the world into thinking malicious software had infected their computers, then sold them software to "fix" the non-existent problem. The foreign defendants argued that the FTC did not have jurisdiction over them, and thus could not seek return of their assets to the United States. The FTC invoked the SAFE WEB Act amendments in response: "Because the FTC is specifically empowered to redress foreign victims, the defendants' argument that funds derived from defrauded foreign consumers are immune from repatriation must fail."[35] The Court agreed, and the FTC eventually recovered $8.2 million from one of the key defendants, who was based in Canada. The FTC has used this money to send out refund checks to more than 300,000 consumers for consumer redress.[36]

The Act's jurisdictional provisions are even more critical in light of the Supreme Court's 2010 decision in *Morrison v. National Australia Bank Ltd.*[37] The Court there held that the SEC

---

[32] 15 U.S.C. § 45(a)(4)(A)(i), (ii).
[33] 15 U.S.C. § 45(a)(4)(B).
[34] *FTC v. Innovative Mktg., Inc.*, No. RDB 08CV3233 (D. Md., filed Dec. 2, 2008), initial press release *available at* http://www.ftc.gov/opa/2008/winsoftware.shtm.
[35] Plaintiff's Consolidated Reply to Sam Jain and Kristy Ross's Opposition to the FTC's Motion for an Order Holding Sam Jain and Kristy Ross in Contempt of Court and Requiring Repatriation of Their Assets in *FTC v. Innovative Mktg, Inc.*, No. RDB 08CV3233 (D. Md., filed Mar. 3, 2009) (internal citations omitted).
[36] *See* http://www.ftc.gov/opa/2011/12/rebates.shtm.
[37] 130 S. Ct. 2869 (2010).

Act did not have extraterritorial effect, and therefore could not apply to the sale of foreign securities outside the United States. Though the case involved only private parties, the *Morrison* decision also presented hurdles to the SEC's ability to sue foreigners selling securities to U.S. citizens. Congress therefore promptly amended the law to provide that the SEC could bring cases involving transnational securities fraud.[38]

The FTC Act, before the SAFE WEB amendments, contained jurisdictional language similar to that in the SEC Act. Though the ultimate effect of *Morrison* on the FTC's jurisdiction is not clear, there is a risk that the federal courts would not permit the FTC to pursue foreigners victimizing U.S. consumers if the SAFE WEB Act were to sunset. Without the power to sue foreign wrongdoers, the FTC's cross-border consumer protection enforcement would be crippled.

D. Enforcement Relationships

Finally, the Act strengthens the FTC's enforcement relationships with foreign agencies. In particular, the Act authorizes the FTC "to retain or employ officers or employees of foreign government agencies on a temporary basis as employees of the Commission."[39] With this tool, the FTC created an International Fellows Program so that foreign agency officials can work side-by-side with FTC staff on investigations and cases, subject to appropriate confidentiality

[38] 15 U.S.C § 77v(c). The SEC Act, as amended, now confers on federal district courts jurisdiction over actions involving: (1) conduct within the United States that constitutes significant steps in furtherance of the violation, even if the securities transaction occurs outside the United States and involves only foreign investors; or (2) conduct occurring outside the United States that has a foreseeable substantial effect within the United States. These jurisdictional provisions do not contain a sunset provision or any other time limitation. *See also Study on the Cross-Border Scope of the Private Right of Action Under Section 10(b) of the Securities Exchange Act of 1934* by the Staff of the U.S. Securities and Exchange Commission at 6, *available at* http://www.sec.gov/news/studies/2012/929y-study-cross-border-private-rights.pdf (by this amendment "Congress restored the ability of the Securities and Exchange Commission ("Commission") and the Department of Justice ("DOJ") to bring enforcement actions under Section 10(b) in cases involving transnational securities fraud").

[39] 15 U.S.C. § 57c-1.

restrictions and security measures.[40] This kind of arrangement is key to establishing trust and the understanding between agencies on basic functions crucial to developing meaningful case cooperation.

A standout example of this program was the work done by a Fellow from the FTC's Canadian counterpart agency in connection with "Operation Tele-PHONEY," described earlier. As part of this enforcement sweep against deceptive telemarketers, the Fellow played a key role, working at FTC offices on investigations and facilitating close coordination and reciprocal assistance between her agency and the FTC on several cases. The resulting sweep counted 180 civil and criminal actions by the FTC, the Canadian agency, and various other enforcement partners.[41] Building these kinds of enforcement relationships is more important than ever, as the range of foreign countries involved in the agency's work continues to grow.

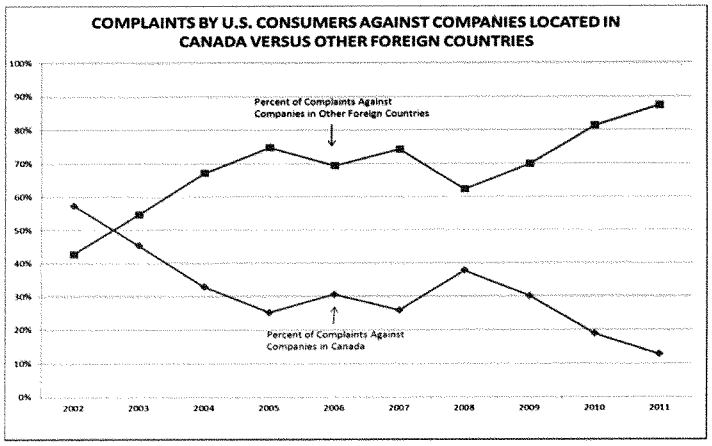
IV. CROSS-BORDER CHALLENGES AND THE CONTINUING NEED FOR U.S. SAFE WEB ACT AUTHORITY

Despite the FTC's successes in using the SAFE WEB Act, cross-border fraud remains a significant problem for U.S. consumers. Though overall percentages of cross-border complaints have remained steady in the past few years, U.S. consumers and the FTC are facing new and emerging cross-border challenges. For example, whereas much of the cross-border fraud in the 1990s involved telemarketing from Canada, newer threats to U.S. consumers are coming from all over the world. This general trend appears, for example, in the percentage of *Consumer Sentinel* cross-border complaints that involve companies in countries other than Canada:

---

[40] To date, the agency has hosted 48 international foreign officials, 13 of them working on some aspect of the consumer protection mission. The officials have come from Argentina, Austria, Australia, Brazil, Canada, China, Colombia, Egypt, the European Commission, France, Hungary, India, Israel, Kazakhstan, Mauritius, Mexico, Peru, Poland, Singapore, South Africa, South Korea, Switzerland, Tanzania, Turkey, United Kingdom, and Vietnam. Fellows have also made significant contributions to the FTC's competition work, as this provision of the Act, unlike other sections, also covers the agency's competition mission.

[41] *See* http://www.ftc.gov/opa/2008/05/telephoney.shtm and http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/02677.html.



Several recent FTC cases illustrate this trend. In the past few months, the FTC filed cases involving "phantom" debt collection frauds, which appear to be based in India, targeting hundreds of thousands of financially vulnerable U.S. consumers to collect debts the consumers did not owe to the defendants or did not owe at all.[42] One of these cases was recently featured on ABC News' *Nightline*.[43] This is consistent with the 2011 complaint data in *Consumer Sentinel*, which shows India as the sixth most frequent location of companies complained about, after the United States, Canada, the United Kingdom, Nigeria, and Jamaica.[44] Another FTC case involved more than six million pre-recorded "robocalls" sent to U.S. consumers through facilities in the

[42] *See FTC v. Broadway Global Master, Inc.*, No. 2:12-CV-00855 (E.D. Cal., filed Apr. 3, 2012), initial press release *available at* http://www.ftc.gov/opa/2012/04/broadway.shtm; *FTC v. American Credit Crunchers*, No. 12cv1028 (N.D. Ill., filed Feb. 13, 2012), initial press release *available at* http://www.ftc.gov/opa/2012/02/acc.shtm.
[43] Phantom Debt Collectors From India Harass Americans, Demand Money (June 7, 2012), *available at* http://abcnews.go.com/Blotter/phantom-debt-collectors-india-harass-americans-demand-money/story?id=16512428.
[44] Consumer Sentinel Network Data Book for January-December 2011, *available at* http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf.

Philippines, by defendants with principals and employees in the Philippines and in Thailand.[45] Further complicating these challenges is the fact that not just wrongdoers, but also evidence and assets, can be located around the globe.

Reauthorization of the Act would enable the FTC to continue its current cross-border enforcement efforts and deal with new threats to U.S. consumers emanating from a growing number of jurisdictions. Like the SEC, CFTC, and CPSC, the FTC needs these enhanced enforcement tools to carry out its mission of protecting American consumers.

V. CONCLUSION

We urge Congress to promptly reauthorize the SAFE WEB Act, and we look forward to working with this Subcommittee on its proposed legislation.

[45] *See FTC v. Navestad*, No. 09-CV-6329 (W.D.N.Y., filed June 25, 2009), *available at http://www.ftc.gov/os/caselist/0923099/index.shtm.*

Mrs. BONO MACK. Mr. Stevenson, I think that is a world record. Good job. So I will recognize myself for 5 minutes for questioning. And again, thank you for your testimony.

Can you just give us sort of a worst-case scenario of what exactly happens or could happen if you lose this authority that you are granted under this U.S. SAFE WEB Act?

Mr. STEVENSON. Well, first and foremost, we would lose the enforcement tools of investigation and information sharing that we use now increasingly, frequently, to work with these other agencies. That means we would be less effective in a number of these cases. It would take more time to do these cases or, in some cases, we just couldn't bring the cases at all. We also wouldn't be in the position we are now to assist agencies in other countries that often are acting on investigations—take the Toronto example I mentioned—to protect U.S. consumers. And so we lose that benefit as well.

Mrs. BONO MACK. Can you talk a little bit about what the consumer might see rather than in the halls of the FTC? What do you think will happen? What would the consumer see, perhaps, if you cease to have these opportunities under this Act?

Mr. STEVENSON. Well, the consumer is going to have more and more of these kinds of challenges as we see it. Just by carrying around our Smartphone, you know, we can be spammed and spimmed and spear phished and robocalled and just ripped off, and that is from anywhere in the world. And so the challenge is, what can we do and step in to deal with these problems? There are some things that we can try to continue to do as we did before the Act, but we are simply not in the position to be as effective as we are now.

Mrs. BONO MACK. How did you pursue these things before the Act?

Mr. STEVENSON. Well, we could share limited forms of information, consumer complaint information, for example, under our statute. We could bring our own actions and coordinate as well as we might with agencies in other countries. But we weren't in the position, really—which is so critical—of being able to share information, particularly as the investigation goes on. Sometimes we don't even know where the fraud is located when we start the investigation. Neither do some of our counterparts. So some of it is just that challenge of even finding the people we want to go after.

Mrs. BONO MACK. Was the FTC ever denied from bringing cases prior to SAFE WEB?

Mr. STEVENSON. There are certainly cases that I think it is fair to say would have been very difficult if not impossible to investigate for that kind of reason. When we would come to the border in terms of information, if the evidence is somewhere else—for example, the domain name registrar information about who is behind a Web site was somewhere else and we didn't have a way to get at it without using these powers, or maybe an agency that was working with us didn't have the ability to get at it because we were able to assist them—that kind of thing could shut down investigations. It is a matter of degree of how fast and how well we can bring these cases in terms of developing the evidence, but fast is important here because fraud is even faster.

Mrs. BONO MACK. Thank you. And turning to something that we all care deeply about in this town, and that is the amount of money it costs. CBO originally scored U.S. SAFE WEB at $9 million over 5 years from 2006 through 2011. Do you believe that that score was accurate, and if not, do you know how much the activities pursued under the U.S. SAFE WEB authority have cost?

Mr. STEVENSON. Well, it is difficult to provide an exact estimate since these authorities are all intertwined with the FTC Act. And indeed, a lot of these tools are part and parcel of this sort of ongoing enforcement activity. Since we don't do our budget items by statute, it is hard to parcel all of that out.

Having said that, I would also add there was no specific appropriation for SAFE WEB when it was enacted and we did the implementation work, for example, in the beginning without an additional—beyond our regular appropriation.

In terms of the $9 million figure, while there are various ways in which, depending on exactly what one counts in calculating this, we think under any reasonable calculation it would be significantly less than 9 million. Probably less than half that would be the cost attributable to this. The fact is a lot of it is just that we were able to do the same work but better, and we were able also—and bearing in mind not only the costs here but the benefits—to stop more frauds involving tens of millions of dollars, even recover money in some cases that we may not have recovered otherwise.

Mrs. BONO MACK. Thank you. Doing the same work but better, would you say your office has grown larger or small since the passage of the SAFE WEB Act?

Mr. STEVENSON. The Office of International Affairs has, I think, grown a little larger. But looking at it from the point of view of the FTC, as I said, the work was generally done within the appropriation envelop that we had when we were doing the first implementation. The other thing I might mention is that some of the costs that we have here such as doing the report, such as writing the internal procedural rules to implement this, would not be necessary to repeat as we go forward.

Mrs. BONO MACK. Thank you very much.

I am going to recognize Mr. Butterfield for 5 minutes.

Mr. BUTTERFIELD. Thank you, Madam Chairman.

In your testimony, Mr. Stevenson, you mentioned spammed, spimmed, and spear phish. I know what spam means but I don't know the other two. Would you elaborate on those two?

Mr. STEVENSON. Well, I think spim is sort of like the spam equivalent but in terms of messaging on phones. Phishing spelled with a "ph" is the idea that you might get the message from Wells Fargo Bank saying we have a problem with your account, please sign in here with your account details, when in fact it is somebody else trying to——

Mr. BUTTERFIELD. Um-hum.

Mr. STEVENSON [continuing]. Steal those. And spear phishing is using some particular information that they may know about you to make the phishing even more effective.

Mr. BUTTERFIELD. All right. I have learned something. All right. You also indicate that the full commission—I believe there are five of you on the Commission, Democrats and Republicans—that the

five of you have twice called on Congress to completely repeal the sunset provision. Are you reflecting a sentiment that is part of the record or are these the informal feelings of the commissioners?

Mr. STEVENSON. The Commission in its 3-year report to Congress did request the repeal of the sunset provision.

Mr. BUTTERFIELD. And that opinion is unanimous among your colleagues?

Mr. STEVENSON. Yes, as I understand.

Mr. BUTTERFIELD. All right. Can you please discuss with us some of the disadvantages to renewing these authorities for only 7 years, some of the disadvantages?

Mr. STEVENSON. Well, one issue that arises is that as the time comes for the provisions to expire that obviously investigations can take months, cases can take years, and as we get closer to the end of the time available to us, then the time left on the statute, so to speak, is less than the time that we need to pursue those cases. It also does affect, of course, the end of the sunset period and the potential willingness of others to cooperate with us. Underlying a lot of this is developing this kind of cultural reciprocity of going back and forth, and obviously we want to be in the position as strongly as we can to assure our partners that indeed we will be in the position to reciprocate just as we expect that they will be.

Mr. BUTTERFIELD. And the opposite of that, can you think of any benefits to sunsetting at 7 years?

Mr. STEVENSON. Well, the process of oversight—obviously, I defer to you on the possible benefits of oversight. I would emphasize here that the type of law that we are dealing with here involves not the kind of substantive rules but more of the enforcement tools that the need for which we don't expect to be going away any time soon.

Mr. BUTTERFIELD. And finally, can you please discuss with us why it is important to reauthorize the Act now and not wait until sometime closer to December 2013? In particular, can you please address how delaying this reauthorization might affect your international investigative and enforcement efforts?

Mr. STEVENSON. Well, mostly for the reasons that I mentioned. In terms of particular investigations in cases, as we get closer to the time that it expires, the time for which we exercise these powers may run out before the investigation is completed, for example. So that is one kind of concern. We do have the power also under the Act to negotiate formal agreements where those are necessary according to the opposite side's law, which they aren't always required. But we have been negotiating some of those. It is difficult to pursue negotiations of that sort as we get very close to the end of a sunset period, and so that is why we are requesting a prompt renewal.

Mr. BUTTERFIELD. Can you please discuss what kinds of complaints by and frauds against the U.S. consumer you are seeing originating in other countries?

Mr. STEVENSON. We see all manner of frauds. As I say, the technology these days means the communications can come from anywhere and the money can go anywhere, so we see pretty much the full range of frauds and deceptions. I would say that they tend to be the particularly egregious ones that we have seen or certainly

that we have acted on when we are dealing with the cross-border——

Mr. BUTTERFIELD. But Canada is in the number one position, are they not?

Mr. STEVENSON. Canada has been historically where we have seen the most complaints going back to the 1990s where we saw extensive telemarketing issues. One of the interesting trends is that more and more though we see other countries involved. And so in the testimony we gave the example of these bogus debt collection calls from India and we had two cases there, the robocall case that used facilities in the Philippines to send complaints, and we are seeing a larger and larger percentage of the cross-border fraud complaints by U.S. consumers to involve these other countries. We also have a range of countries where we have seen the money go and have tried to——

Mr. BUTTERFIELD. The U.K. is an example? Would the U.K. be an example?

Mr. STEVENSON. The U.K. would be one of the——

Mr. BUTTERFIELD. Yes.

Mr. STEVENSON [continuing]. Countries where we have seen the numbers. We do about a 100-page report a year from our Consumer Sentinel Database, which is combined data from the FTC, the FBI, the U.S. Postal Inspection Service, Better Business Bureau, various Canadian sources, and we have seen in that data an increase in frauds from other countries so that the largest number would be from Canada, for example. But then the United Kingdom would be after that, Nigeria, Jamaica, India, Spain, China, Mexico, and Ghana would be the top ones in terms of complaints. Obviously, the complaint data doesn't give us a precise calculation of what is happening out there, but it is certainly indicative of general trends.

Mr. BUTTERFIELD. Thank you.

Mrs. BONO MACK. Thank you, Mr. Butterfield.

The chair now recognizes Dr. Cassidy for 5 minutes.

Mr. CASSIDY. Good morning, Mr. Stevenson. I am a doctor so as I was reading your testimony I was struck by some of the prosecutions or cooperations you have had regarding bogus medical products sold. So none of this is the challenge. All of this is for me to learn. We may have a restriction on the sale of a drug without a medical prescription but Mexico may not. So if the online pharmacy is originating a drug from Mexico—one, do you know that that pharmacy is based in Mexico, that online pharmacy; and two, do you get cooperation not just from Mexico but from any country for a statute which is U.S.-specific but doesn't necessarily apply to their methods of dispensing drugs as one example?

Mr. STEVENSON. Well, the powers the SAFE WEB Act give us, as I mention, are limited in the kinds of cases we can cooperate on, are ones where the law is substantially similar to practices that violate our Act. So in the case——

Mr. CASSIDY. Now, if Mexico does have a requirement that for controlled substances there be a physician's prescription with their version of a DEA number and we have that same and someone is buying controlled substances from an overseas online pharmacy, would they cooperate with us on that regard?

Mr. STEVENSON. Well, it would require under our statute for us to cooperate with them that it would be substantially similar to practices that violate the FTC consumer law. So if we, the United States, might have such a provision, it wouldn't give the FTC the power——

Mr. CASSIDY. I see. So it would have to be fraudulent. It couldn't be, "Here is pure-grade morphine." We would require a prescription—they do—but it is still being sold. It would have to be adulterated morphine. Yes. So if they were saying adulterated morphine, billing it as pure grade, you could prosecute?

Mr. STEVENSON. Yes. If it was something that was a fraud, for example, and the large, large percentage of the cases that really have implicated SAFE WEB have been hard core fraud and deception.

Mr. CASSIDY. So do you know those Web sites which are notorious for fraudulent sales? I mean do you have a roster, a registry of those Web sites? Wow, man, we are getting adulterated drugs from this particular Web site.

Mr. STEVENSON. I think that the drug issues tend to be addressed more by other agencies, the FDA, for example——

Mr. CASSIDY. The only reason I raise that, though, is you mentioned a couple of—and I don't have your testimony in front of me open now——

Mr. STEVENSON. Right.

Mr. CASSIDY [continuing]. But you mentioned a couple of medical-type stuff, drugs-type stuff that you did prosecute on.

Mr. STEVENSON. Yes.

Mr. CASSIDY. So what would make those your jurisdiction if you will as opposed to someone else's, FDA's?

Mr. STEVENSON. Right. Well, it is partly what we can cover with our law. Although the fraud provisions reach broadly, they wouldn't reach everything. So another would be just in terms of allocating where the expertise lies for doing certain kinds of things——

Mr. CASSIDY. So you mentioned a——

Mr. STEVENSON [continuing]. For example, we are not in a position to do a medical analysis of drugs or——

Mr. CASSIDY. But you mentioned that there was a cancer agent that was sold that turned out to be nothing but white powder.

Mr. STEVENSON. Yes.

Mr. CASSIDY. So did you all prosecute that one or did the FDA?

Mr. STEVENSON. In fact, in that case I think it was prosecuted by the Department of Justice and the FBI made the arrest. So that was in that case a criminal one. And that is actually an important point to emphasize, that we accomplish things with this law not only by bringing our own cases but where we can cooperate as appropriate with other authorities——

Mr. CASSIDY. So let me go back——

Mr. STEVENSON [continuing]. That may be more in a——

Mr. CASSIDY. I accept that, but I just have limited time——

Mr. STEVENSON. Sorry.

Mr. CASSIDY [continuing]. And I might interrupt. I apologize. But again, do you have a registry, if you will, of Web sites that we know these are the bad actors, we are going to watch them for pro-

moting fraudulent products, and we are just going to hover over them, if you will? Do you keep such a list or does it just kind of randomly pop up that, wow, somebody saw white powder, called it a cancer cure?

Mr. STEVENSON. Well, our cases can start in a number of ways but one major way is from looking at the complaint data that we get from consumers and from other agencies.

Mr. CASSIDY. But I guess my specific question is do you monitor certain Web sites? You have a certain amount of complaints; a lot of them come back to a particular Web site. Does that go on your monitor-this-one-closely list?

Mr. STEVENSON. As I say, we look at the complaints; we look at other factors that may influence whether the case is an appropriate one to bring. We usually don't lack for potential targets. There are usually a lot of different fraud targets.

Mr. CASSIDY. But somehow you are not answering my question——

Mr. STEVENSON. Sorry.

Mr. CASSIDY [continuing]. Asking my question correctly. Intuitively I know that there are going to be some Web sites that you are able to identify as being particular bad actors in terms of purveying fraudulent material. Do they go on a watch-closely list or is it always generated from your complaints and it may be this Web site and it may be another next time?

Mr. STEVENSON. I would say we do not have a watch-closely list as in the sense that you are describing. The other thing about that is that, in terms of Web sites, what we see is often fraud operators operate multiple fraud Web sites, move around quite a bit, use the process of registering them to use phony names and whatnot so that actually that is a chunk. But we do not have the list that you are asking about.

Mr. CASSIDY. May I have one more question? The only thing in the medical sphere, people are obviously depositing prescriptions on the Web site and then they are getting refills. It is not a one-time, you know, buy a bicycle that whatever, whatever; it is, no, I want refills. So even in those sorts of pharmaceutical-oriented Web sites, do you find this constant changeover?

Mr. STEVENSON. That, I am sorry, I don't know the answer to that.

Mr. CASSIDY. Thank you for your indulgence, Madam Chair.

Mr. STEVENSON. Thank you.

Mrs. BONO MACK. Thank you, Dr. Cassidy.

And good morning, Mr. Gonzalez. You are recognized for 5 minutes.

Mr. GONZALEZ. Thank you very much, Madam Chair.

Mr. Stevenson, let me ask you. Democratic staff has prepared a memo, in essence, telling us what we would be reauthorizing, whether it is for a limited period of time or no restriction, but it says it exempts financial institutions, payment system providers, Internet service providers, telephone service providers, and domain name registrars, among others, from liability for voluntarily providing certain information to the FTC when they might otherwise be prohibited from sharing such information. Now, that is very important, is it not, that provision?

Mr. STEVENSON. Yes, that is one of the provisions in the SAFE WEB Act, yes.

Mr. GONZALEZ. And the reason is there may not be any liability, but it definitely might interfere with the business relationships that some of these providers of this information have with customers that utilize their services? Would that be true? Now, they may be bad purpose, bad actors, but they still have a business relationship. What I am getting at is a very simple proposition, and that is surely not everyone is happy with this particular authority that you have. I agree that you should have the authority. I don't think that we have to sunset the thing either and I commend the work that you have done. I just want to get at all of the different stakeholders because I think we are all in agreement that this is a good authority for you to have and we need to accommodate you.

The question comes down to surely someone out there in the business community, in the Internet or in the stakeholders, business stakeholders have some concerns that they expressed to you regarding this authority and the exercise of it. So what is it out there in the business community that we might have some stakeholders, legitimate ones, that are complaining to you, the nature of the complaint, and your response?

Mr. STEVENSON. Thank you. We have not had any complaints about this provision since the Act was passed. We did have concerns raised in the several years leading up to the passage of the Act about the scope and nature of this provision, and then accordingly, it was narrowed. You mentioned that this information can be shared in certain instances. The certain instances here really are focused on essentially where there is a third party that has some reason to believe there may be a fraud or a deception or a violation of our law going on, or they have reason to believe that they have information about money that is ours to recover. So it is focused on those instances where they essentially have some reason to say we have complaints, we have suspicious charged back rates, or in some manner they have information to say this is something that we should notify the authorities about. And the effect of the provision is really just aimed at the liability or, in this case, lack of liability for the act of notifying us.

So we have not heard complaints about that since the Act was passed. It is something that is useful to us. It has not been as central as the information sharing and investigation, other provisions that I have already talked about.

Mr. GONZALEZ. Now, as much is going out there in the Internet world, and you just indicated it has revolutionized just in the past couple of years the use of mobile devices and how people get information out there, tremendous opportunities for many good things and tremendous opportunities for many bad things, as happens. Bottom line, though, is the consumer needs to be protected and we need to educate the consumer. And the best thing always—and Dr. Cassidy probably would agree if he was here—and that is prevention. So what is it that the FTC does to educate the consumer, to protect them and so they don't fall victim, so that then you are not there investigating and pursuing on the civil side and maybe DOJ pursuing things on the criminal side? What about education?

Mr. STEVENSON. We place a very high priority actually on education, have a number of different campaigns we have done, including with foreign partners in a number of cases. One example of an education campaign that I think we launched just this week if I am not mistaken involves, for example, the problem of robocalls, which we mentioned earlier. And so we have done videos to put out for consumers. We have robocall advice on what to do if you receive them if you are a consumer. We also have a robocall action plan with several items and several steps we are trying to take to alert consumers to the problems that they see.

Another example is in the area of remittances, sending money back home to another country, and this is an issue that affects us as Americans, including when we don't speak English. And so we have actually put that piece of advice in six different languages to make sure that we are reaching as many people as we can with the important messages. Some of these messages about the fraud prevention are not exclusively international obviously because it has become so much part of our sort of everyday life and the kind of thing we have to communicate to consumers.

Mr. GONZALEZ. Thank you very much for your testimony.

And I yield back, Madam Chair.

Mrs. BONO MACK. Thank you.

The chair recognizes Mr. Guthrie for 5 minutes.

Mr. GUTHRIE. Thank you, Madam Chair.

Thank you so much for being here today. I was trying to get kind of a better feel for the process that the FTC uses to engage in international cooperation to the SAFE WEB Act. So in SAFE WEB I believe parts of it are self-executing and there are other areas that you have to have Memorandums of Understanding with other countries. Can you walk through that process? What are the impediments of those Memorandums of Understanding?

Mr. STEVENSON. Sure. Well, one of the things that the Act requires is, before we share information, that the other side certify that they have the law to keep the information confidential, that they are investigating laws that are fraud, deception, or something substantially similar to our statutes.

Mr. GUTHRIE. Um-hum.

Mr. STEVENSON. We have actually developed a sort of form, the checklist of the factors that we have to take into account. We have to look at whether their law meets that standard. Usually, it is fraud and deception as I mentioned and that part is straightforward. We also need to take into account the general public interest, the likelihood of reciprocity if we assist another party, and the amount of injury and the number of consumers affected. And we have to use our resources wisely in choosing where to provide that assistance. If we want to go and get investigative assistance, that needs to go through one of our commissioners to use that process.

We don't require a formal agreement in the formal sense in order to do that kind of cooperation, but there are some countries where their laws may require that.

Mr. GUTHRIE. OK.

Mr. STEVENSON. And in that event, then, we work with the State Department to develop the text to negotiate—in this case with the

European Commission and Canada where it appeared that their law would require a more formal arrangement.

Mr. GUTHRIE. You mentioned other emerging threats like Jamaica and some other countries that aren't European Commission or Canada—have the same kind of systems, I guess, that we have. I mean who are the big emerging threat countries and what are the impediments between us being able to work with them or them working with us I guess? I think you mentioned Jamaica earlier.

Mr. STEVENSON. Right. Well, there can be several sort of issues. In some cases there may not be a clear counterpart agency for us, and that is why it is important that the authority enables us to cooperate not just with civil regulatory agencies but also criminal agencies. So that part is important to us. And in some cases, obviously, language is a certain kind of barrier, and others not so much. And the challenges can differ. And it does take time to develop the relationships. We want to make sure that we can trust the agency we are dealing with on the other side; they want to be able to trust us. So that is also part of the ongoing process.

Mr. GUTHRIE. Is there like a top two or three countries that you are most concerned about——

Mr. STEVENSON. As I mentioned——

Mr. GUTHRIE [continuing]. International fraud that we are not able to really——

Mr. STEVENSON. Yes.

Mr. GUTHRIE [continuing]. Get an agreement with or work with?

Mr. STEVENSON. As I mentioned, the complaint data suggests that there are certain countries that are where there are a particularly large number of complaints. I think I mentioned India, Jamaica among them. The——

Mr. GUTHRIE. So there are large complaints with them and they are cooperating with us, or are there large complaints in those countries and we are really having trouble cooperating with them?

Mr. STEVENSON. Well, we are working in a number of countries on further improving our relationship. As I say, it varies depending on also the state of their agency in that country, the degree to which we have had occasion to work with them before.

Mr. GUTHRIE. I guess the question—the worst-offending countries, are they serious about it and want to get it fixed? Or this is just something that is not on their agenda?

Mr. STEVENSON. Well, sometimes there is a challenge of making this high enough on the agenda from the point of view of the agencies in another country, and that is something then we also try to work on in our enforcement work and technical assistance work.

Mr. GUTHRIE. Because location is not important. It is the web so people can just gravitate, and once you fix it in one country, it is going to gravitate to another. So I appreciate the struggle you are in and how difficult it is for what you are doing. And the anonymity of the web allows people to do things that we don't want them to do. So I appreciate what you are doing.

And I yield back.

Mr. STEVENSON. Thank you.

Mrs. BONO MACK. Thank you, Mr. Guthrie.

Mr. Harper, you are recognized for 5 minutes.

Mr. HARPER. Thank you, Madam Chair.

Thank you, Mr. Stevenson, for being here with us today. Your written testimony indicates that the Act authorizes the FTC to share confidential information with its foreign counterparts subject to certain safeguards such as restrictions on foreign governments' use of information for a purpose other than the investigation that triggered the information request. Have you received any complaints of misuse of information?

Mr. STEVENSON. Misuse by agencies in other countries?

Mr. HARPER. Yes.

Mr. STEVENSON. No, I don't believe so.

Mr. HARPER. OK. Are you aware of any such misuses of information whether you have received complaints about that or not?

Mr. STEVENSON. No.

Mr. HARPER. OK. Does the FTC have formal agreements with other nations to address information sharing, and if so, how many agreements are in place?

Mr. STEVENSON. In terms of SAFE WEB Act agreements, we have no formal agreements. We have, dating from before the SAFE WEB Act, mostly some informal Memoranda of Understanding. And as I mentioned, we can cooperate case-by-case if they provide the required certifications of information. So we do have those kinds of arrangements.

Mr. HARPER. Do the protections for information shared internationally closely resemble those for sharing with State attorneys general or are they different?

Mr. STEVENSON. They are very similar.

Mr. HARPER. OK. Are there any countries where you have shared information that did not have reciprocal information sharing agreements with the U.S.?

Mr. STEVENSON. Well, as I said, we don't have the formal agreements. One of the factors that we take into account in sharing is whether there is the likelihood of reciprocal assistance, and we do find that—I can't think of an example where someone has indicated they will not provide that under any circumstances, and certainly generally they are more than happy to. And that is part of what we are trying to achieve. Sometimes they have their own legal restrictions on doing it. So if they didn't have that ability to share everything back with us, we take that into account. But there are sometimes limited things they can do and other things they can't. And we see the important issue as getting the bad buys.

Mr. HARPER. Well, what are the conditions you look for or establish in order to share information?

Mr. STEVENSON. Well, so, first and foremost, they provide the certification that they can maintain the information in confidence. They tell us the nature of their legal authority to do investigations. So we ask them under what authority are you pursuing a possible violation? So often they will cite to us their fraud statute, their deception statute, or whatever. Then, we will look at whether that complies with the statutory requirement, that it is substantially similar. We also would look at the general public interest, as I mentioned, the likelihood of reciprocity, and also whether there is real injury involved and whether there is a significant number of people. We don't want to be doing this kind of work for, you know, one-off disputes obviously or even, you know, small disputes.

Mr. HARPER. You testified earlier that Canada recently enacted a law similar to our SAFE WEB. Does their law affect your ability to investigate or litigate fraud originating from Canada?

Mr. STEVENSON. Yes, it does. We have seen that as a very positive development in testifying in support of the legislation, they are actually—the government official, the head, I think, of the FCC pointed to the experience of the SAFE WEB Act in the United States and the importance of that kind of reciprocal assistance. It hasn't yet all played out. I don't believe it is completely in effect, but we are already seeing the benefits. We have several Canadian agencies—the Competition Bureau, the CRTC, which is more like the FCC—have already detailed people to us to work with us under his cases and that has been very effective.

Mr. HARPER. Are you doing anything to encourage other countries to enact similar laws to what Canada has done?

Mr. STEVENSON. We had done work at the OECD on protecting consumers from cross-border fraud and deception focusing particularly on those kinds of practices and encouraging a consensus on the approach to be taken. And a number of the items in that OECD recommendation are reflected in the SAFE WEB Act and are indeed reflected in some aspects of European Union law and now in the Canadian provisions. Different countries have obviously variations on that theme, which is part of the challenge here of working it out so that the rails of the two train tracks fit together when they meet.

Mr. HARPER. Thank you, Mr. Stevenson.

I yield back.

Mr. STEVENSON. Thank you.

Mrs. BONO MACK. Thank you, Mr. Harper.

Mr. Lance? OK. He waives his questions.

Mr. LANCE. That is you, then.

Mrs. BONO MACK. Then, it is me. All right. We are going to move to a quick second round of questions, and I recognize myself for 5 minutes.

If a foreign government—kind of continuing on in the same vein—if they are not interested in cooperating with the FTC, what can the FTC do about perpetrators in that nation? Do you ever pursue enforcement in such cases? And does the FTC ever obtain default judgments against absent foreign defendants?

Mr. STEVENSON. Starting with the last one first, we do sometimes obtain default judgments. We have had cases where we have done that. There then becomes the challenge obviously of taking those to enforce them in some other country. We do work with the office of foreign litigation at the Department of Justice, which is another provision we haven't had a chance to talk about in SAFE WEB Act. That does require the development of case law and the development of other arrangements for us to hire counsel to pursue the money.

In some occasions, we can get the receiver, who is appointed in the case by the court, to take some action in another country by virtue of being the court-appointed trustee, if you will, to take action. So that is another possibility.

Sometimes there are assets that are reachable in some other country even if the defendants are in some way not reachable.

Sometimes there are assets in the United States for some defendants but not others. So there are various of those kinds of measures that we can take, and it really is a case-by-case challenge how we handle that.

Mrs. BONO MACK. Thank you.

There have been a handle of U.S.-based large, multinational companies that have been the target of FTC investigations or legal action that have also been the subject of investigations, reviews, or legal actions abroad for the same activities. Has the FTC shared information gleaned from its legal actions here that has been used in international legal actions for the same activities?

Mr. STEVENSON. The Act permits us to share information in our files with agencies in other countries that are doing investigations. We do take into account various public interest factors and do take into account whether the laws that they are investigating are substantially similar. So there might be some examples where the laws that they may be looking at to pursue, the other companies may not be substantially similar to the laws that we have.

Mrs. BONO MACK. Thank you. I think that is very important.

And how would you explain the pattern of complaints against foreign businesses since the U.S. SAFE WEB Act passed? For a few years it declined and then just last year, which was 2011, the number jumped substantially and exceeded the number of 2006 complaints for the first time. Is the number of complaints rising generally, or are the complaints about foreign companies increasing disproportionately? And are complaints based on Internet fraud rising generally, foreign and domestic? That is a mouthful but——

Mr. STEVENSON. Well, in terms of the trends, it is, as I mentioned, somewhat challenging to really discern the exact trend versus the data that we have in the system, because it sometimes comes in—it depends on the sources. Our sources from the U.S. and Canada are more extensive, obviously, in contributing to the database, so that has some effect on what the data looks like. And I think we had seen a higher percentage of foreign complaints in 2006 than we have in the last couple of years where it has remained stable and around, I think, 13 percent.

Having said that, a number of complaints that aren't marked as cross-border may indeed be cross-border because all we are reporting is what the consumer knows or thinks they know about where the problem is. They don't know about those cases where maybe the money went somewhere else, so they don't know about those cases where the web host is in another country. They don't know about a lot of these instances. Or they may think that the company is in the United States but it is really a mail drop that then sends it on to some other country. So we take it as indicative in a larger sense of this being a substantial part of what is going on, but it is all woven in to the general fraud challenge of finding the bad guys and their money.

Mrs. BONO MACK. All right. Thank you.

Lastly, the Act permits the FTC to issue compulsory process for documents and testimony from a U.S. citizen upon request for investigative assistance by foreign governments. Has the FTC ever refused such a request because a foreign government's request does not meet the legal burden under U.S. law?

Mr. STEVENSON. Yes, if I understood the question. We have certainly been approached by agencies who asked us about help in cases where their laws were not—or at least the legal provisions they we're dealing with were not substantially similar. This might come up, for example, in the context of European privacy laws which are not, in a number of respects, substantially similar.

Mrs. BONO MACK. All right. Thank you very much.

Mr. Butterfield, would you like 5 minutes for question?

Mr. BUTTERFIELD. Five minutes or less, thank you.

Mrs. BONO MACK. OK. You are recognized.

Mr. BUTTERFIELD. All right.

Mr. Stevenson, I am informed that cross-border fraud complaints remain steady at about 13 percent of all fraud complaints in '09, '10, and '11. However, as a raw number, both non-cross-border and cross-border fraud complaints grew in each of those years. Specifically, in '09 the fraud complaints were about 700,000. In 2010 that number was about 815,000. In 2011 it was pretty close to a million with nearly one million fraud complaints in total. Cross-border fraud complaints stood at about 88,000 in '09, 104,000 in '10, 132,000 in '11. With that background, the percentage of cross-border fraud complaints dropped from 2006 to 2007 and then remained steady following enactment of the WEB Act. Do you think that there is a relationship between enactment of that law and the decline and then leveling of cross-border fraud complaints as a percentage of total complaints in the last 3 years?

Mr. STEVENSON. I would like to think so but it is difficult to see cause and effect there. We did have an international program before that. We certainly think that we have become more effective in addressing these problems. The scale though, as I mentioned, of the problems make it difficult to quantify the exact effect. And you are correct that the numbers—although the percentage in terms of cross-border fraud complaints has been largely flat—in absolute numbers we have seen, for example, this year over 100,000 U.S. consumers making such a complaint even with the caveat that there are probably more that don't even realize they are cross-border complaints.

Mr. BUTTERFIELD. Can you tell us whether particular types of frauds are driving the increase in the overall number of consumer complaints about fraud, both with respect to cross-border and non-cross-border?

Mr. STEVENSON. Particular types of frauds?

Mr. BUTTERFIELD. Yes.

Mr. STEVENSON. We certainly see and lay out in our reports the trends that we have seen and certain kinds of problems being more apparent. Robocalls, for example, I think have been an area where we have seen more activity. There has been probably more activity in the kind of grandparent imposter fraud and that kind of thing, people contacting someone saying, "I am out of money, you need to wire it to me really quickly," that kind of thing. So we have seen various trends of that sort.

The cases we brought in India recently involve bogus debt collection fraud where people were called and said we are going to put you in jail, we are going to get you fired, that kind of thing, if you

don't pay off this couple-hundred-dollar debt that it turned out the consumer in fact didn't owe to them or didn't owe at all.

Mr. BUTTERFIELD. Can you speak for a moment about the FTC's Consumer Sentinel Database? Is that in any way related to the watch list that one of my colleagues raised a few moments ago?

Mr. STEVENSON. Yes, the Consumer Sentinel Database is a database that we set up to try to combine from as many sources as possible the complaints that people were seeing. And consumers don't all report to the same place, and so we want no wrong door, that wherever they get reported, we try to gather it together. If we just rely on FTC complaints, we might see them arriving 10 in a week, 20 in a week. We combine it all together, we might see them coming in at 100 a week. We can see where there is the real problem as opposed to the legitimate disputes that obviously consumers have with businesses. And so it has been very useful for that purpose.

We are trying to combine more and more data from other participants. We get data from the Canadian enforcement agencies, the complaint data. We get data through something called econsumer.gov that now is, I think, in eight languages of complaints involving ecommerce online that we have 20-some partner agencies around the world. So we are trying to collect that information.

I hope I did not misunderstand your colleague's message, but that is different from a watch list. And this is unverified, obviously. We want to look at it as the lead, as the starting point for our investigations, but it gives us a tremendous running start if we have it.

Mr. BUTTERFIELD. Are there law enforcement agencies or governmental agencies or even other countries that you would like to work with to enforce the law that you are not currently working with?

Mr. STEVENSON. We certainly are interested in developing further our relationships with a lot of other countries. As I mentioned, in some ways the relationships we have built with the Canadians are a model and have been very extensive. In other countries we have had less experience, it is a newer issue, they may have newer agencies, it may be not yet the higher priority for them, and so we are certainly doing that. And some of our technical assistance work in consumer protection, it also has the benefit, in addition to the good government—larger sense—benefits of developing our relationships with those agencies in those other countries, and to make them aware of this work and to make them aware of why it should be a high priority.

Mr. BUTTERFIELD. Very good. Thank you.

Mr. STEVENSON. Thank you.

Mrs. BONO MACK. All right. Seeing no other members present, we are going to begin wrapping up.

I want to again thank you very much, Mr. Stevenson, for being with us today. You have been very gracious for your time. I know I certainly appreciate what you are doing. I look forward to working with you in the future as the U.S. SAFE WEB Act moves through the legislative process.

I remind members that they have 10 business days to submit questions for the record and I would ask the witness to please respond promptly to any questions that you might receive.

And with that, the hearing is now adjourned.

Mr. STEVENSON. Thank you.

[Whereupon, at 10:55 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Statement of Rep. Henry A. Waxman
Ranking Member, Committee on Energy and Commerce

Subcommittee on Commerce, Manufacturing, and Trade Hearing on H.R. ____, a bill to renew the Federal Trade Commission's authority to combat cross-border spam, spyware and fraud through reauthorization of the U.S. SAFE WEB Act of 2006

July 12, 2012

Thank you, Chairman Bono Mack, for holding this hearing on legislation to reauthorize the U.S. SAFE WEB Act of 2006.

The U.S. SAFE WEB Act granted the Federal Trade Commission new authorities to combat unfair or deceptive acts or practices that are international in scope, but harm consumers in the United States. The Act has worked well, but it sunsets on December 22, 2013 – so if we don't renew it, this critical authority and related investigative tools will disappear and the FTC's ability to fight international frauds will be impeded.

The world is becoming more and more connected. This connectedness has created great opportunities for commerce and economic growth. But the spread of telecommunications infrastructure and growing access to telephones and the Internet have also created opportunities for schemers and scammers operating in other nations to try to defraud U.S. consumers. Because of this, fighting consumer fraud requires that the FTC be able to work closely with foreign consumer protection agencies so that we can all protect our citizens from these schemes. The U.S. SAFE WEB Act granted the FTC the tools it needed to do that.

As today's witness from the FTC, Mr. Stevenson, points out in his testimony, more than 100 of the agency's investigations since 2007 have involved an international component, such as foreign targets, foreign evidence, or foreign assets. And since that time, the FTC has also filed more than 50 cases with an international component. In addition, due to the authorities provided through the U.S. SAFE WEB Act, the FTC has collected more than $10 million in restitution and has prevented U.S. consumers from losing hundreds of millions of dollars to fraudulent schemes.

We need to reauthorize the U.S. SAFE WEB Act to maintain these authorities.

One issue I believe needs to be explored today is the length of the reauthorization and whether there should be any time limit at all.

The bill we are considering today provides another 7-year reauthorization – through September 30, 2020. The FTC recommends that there should be no sunset. All five of the FTC Commissioners wrote me, Ranking Member Butterfield, Chairman Bono Mack, and Chairman Upton last October urging that the sunset clause in the Act be repealed. That would make the authority and investigative tools permanent. In 2009, in a report to Congress required by the Act, all members then serving on the Commission also backed a full repeal of the sunset clause.

I hope we can have a thoughtful and complete discussion about why a changing and bipartisan membership of the Commission has urged complete repeal, and the advantages and disadvantages to revisiting this authority again in another 7 years or some other set timeframe.

Madam Chair, I stand ready to work with you to make sure the FTC continues to have the authority and investigative tools it needs to effectively protect U.S. consumers from fraud, whether homegrown or from abroad.

Statement of Rep. Ed Towns (NY-10)
Before the US House of Representatives
Energy and Commerce Committee

I want to thank Chairman Bono Mack and Ranking Member Butterfield for holding this hearing today to examine the U.S. SAFE WEB Act of 2006. Combating Internet scams and fraud against U.S. citizens by individuals abroad should be a top priority of this subcommittee. According to the FTC, in 2005 almost 1/5 of all consumer complaints that were received by the FTC involved fraud that originated outside the United States. Prior to the enactment of the SAFE WEB Act in 2006 consumers suffered huge losses to foreign companies of almost $219 million.

Unfortunately the FTC was limited in its authority to act against these foreign operators because they could not share information with foreign law enforcers. Upon listening to the recommendations from officials at the FTC, Congress enacted the SAFE WEB Act. The sharing of

information is key in law enforcement, and victims of malicious acts by foreign operators want to know that their government is doing all it can to protect them.

The legislation before this committee reauthorizes the provisions in the SAFE WEB Act for an additional 7 years and allows the continued sharing of information with law enforcement officials. I strongly support this legislation and I'm looking forward to hearing from our witness today on how the provisions in this act are working to protect and secure the American people from fraud. This Congress must do all it can to ensure that the various streams of commerce in our society are safe and secure from foreign criminals intent on causing harm to our citizens.

Thank you Madam Chairman, I yield back the balance of my time.

○