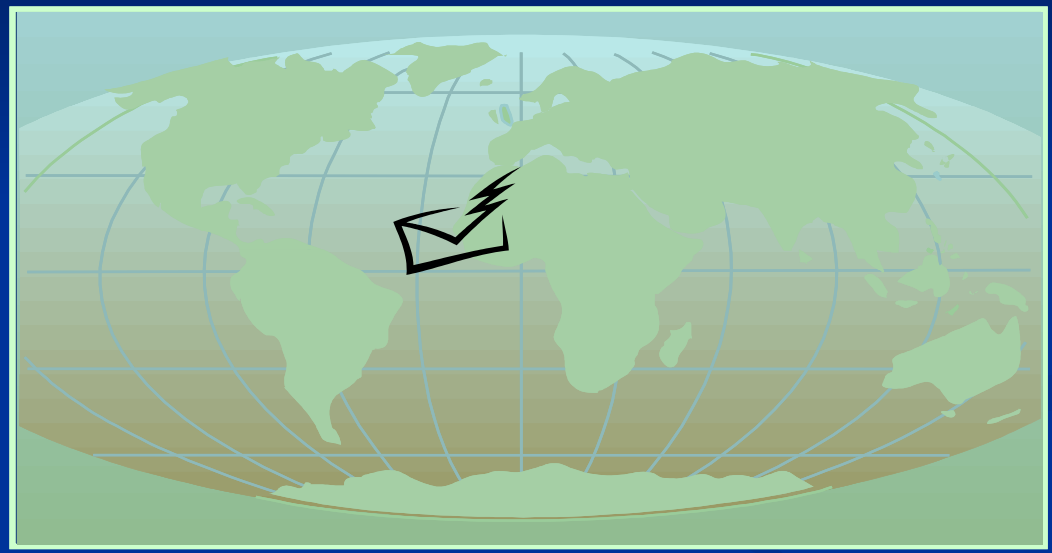
International Law Enforcement Against Spam



Practical solutions for a difficult problem

Hugh Stevenson
U.S. Federal Trade Commission

Nature of the problem

- Fraudulent and deceptive content
- Anonymity: Spammers can easily cross international borders and hide their identity
- Cost: Spam can be profitable

Practical solutions

- Address spam as part of a broader challenge: cross-border fraud and computer crime

The FTC's Role

- Leading U.S. national agency on consumer protection (civil authority)
- Power to bring lawsuits against unfair and deceptive commercial practices
- FTC also has role implementing new U.S. CAN-SPAM Act
- Other U.S. agencies with spam enforcement authority:
  - Federal Communications Commission – Wireless spam
  - Department of Justice – Criminal /computer crimes enforcement

FTC Enforcement Against Spammers

- FTC has filed over 62 spam-related cases.
- Our spam-related cases have targeted:
  - "Spoofing"– forging the sender's identity
  - "Phishing"– spam used to engage in identity theft
  - Failure to honor a "remove me" claim
  - "Subject" lines and "From" lines that deceive recipients into opening a message they would have deleted
  - False claims offering anti-spam services and spam-related business opportunities.
- We have also worked with federal, state, and foreign law enforcement partners.

Can-Spam Act

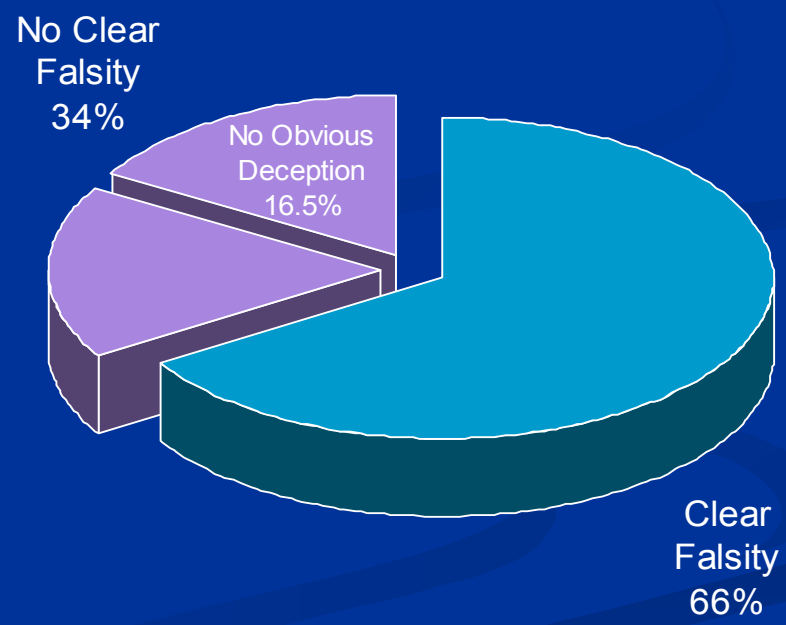
- Prohibits false or materially misleading header information
- Prohibits subject headings that are likely to mislead
- Prohibits sending spam to those who have opted out
- Criminal penalties for certain activities including:
  - Sending over 2500 illegal spam in one day; 25,000 in a month; or 250,000 in a year
  - Committed an offense in furtherance of any federal or state felony
- **Challenge is finding the wrong-doers who can send spam from anywhere in the world**

An FTC perspective

- What we learned from:
  - Research
  - Business and consumer education
  - Investigating and bringing spam cases
- What we need for effective international enforcement

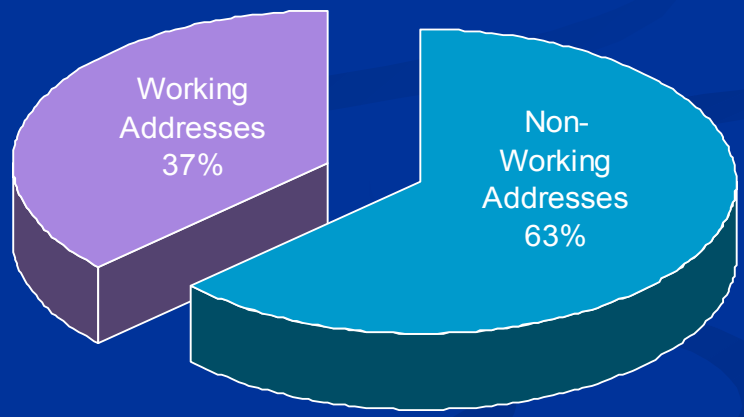
False Claims In Spam Study

- 66% of the spam contained signs of falsity in the from line, subject line, or text
- Only 16.5% of the spam did not sell an illegitimate product or service
- No Fortune 500 companies and only one Fortune 1000 company connected to the spam by hyperlink.

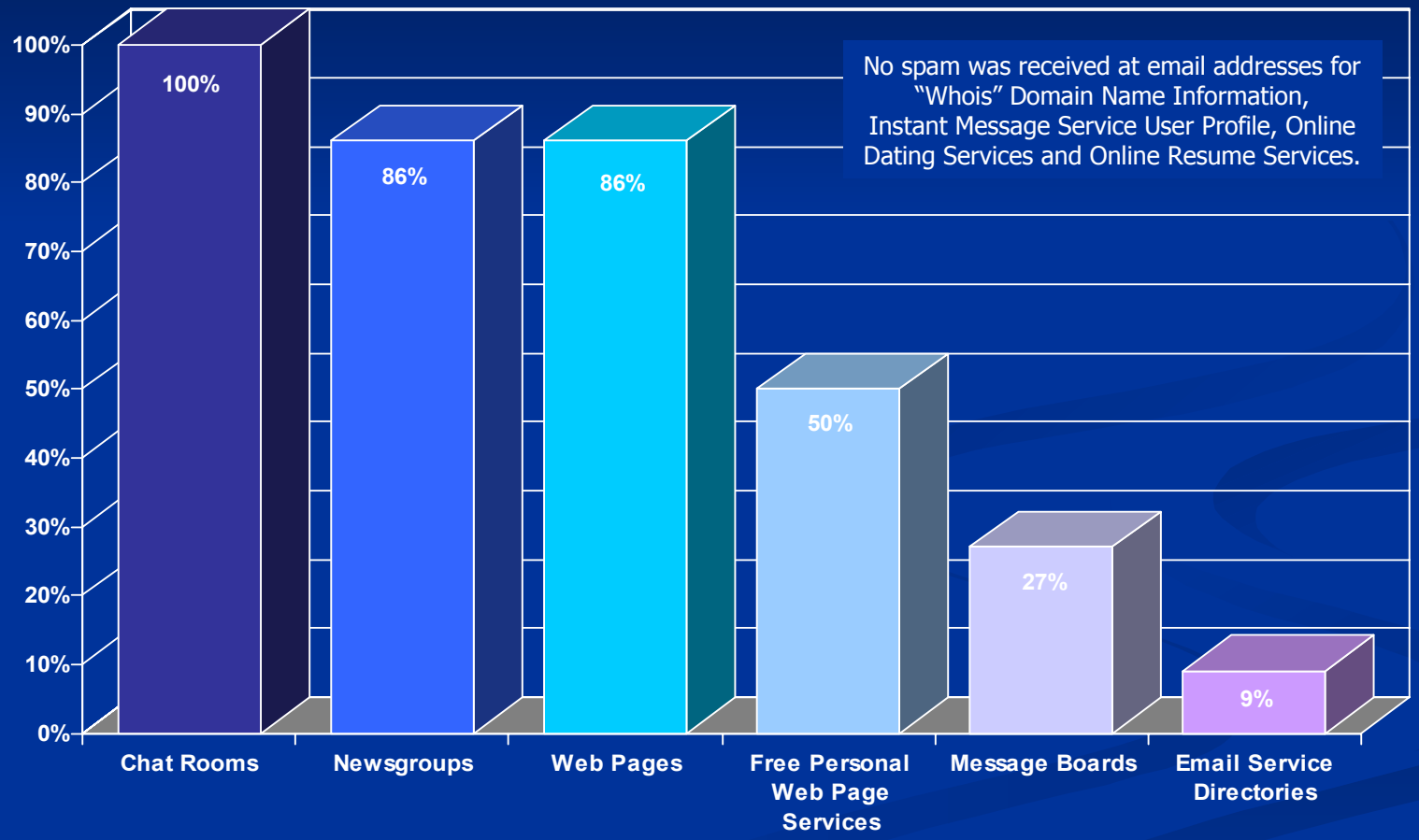


"Remove Me" Surf

- Tested 215 spam messages with "remove me" claims.
  - "Click here to be removed from mailing list."
  - "Reply to this message with 'unsubscribe' in the subject."
- 63% of links and reply options did not function.
- Opting out did *not* result in a greater volume of spam



Email Address Harvesting



Source: Northeast Netforce Investigators seeded 175 different locations on the Internet with 250 new, undercover email addresses and monitored the addresses for six weeks.

Spam Forum

- Three days of discussions with 87 panelists
  - Advocates and opponents, marketers, technologists, law enforcement, and international regulators
- Emphasis
  - How spam works: what we know
  - Potential solutions

Operation Secure Your Server

- International effort to educate owners of open relays and open proxies how to protect their servers from abuse by spammers
- Spammers use these servers to send spam anonymously and avoid anti-spam filters
- 38 international government agencies from 28 countries have sponsored contacting tens of thousands open relay/proxy administrators

Operation Secure Your Server

Authentication

- Discussed in June 2004 FTC Report on feasibility of a "Do Not Email" registry
- Report concludes that, without some authentication, registry would not reduce spam;
- FTC plans Authentication Summit for Fall 2004
  - Effect of domain authentication on enforcement
  - Issue of industry standard

Investigating spam

1. Backwards
   - E-mail tracing

2. Forwards
   - Website investigation
   - Investigating addresses and phone numbers
   - Following the money
     - How did the spammer pay for domain name registration(s)?
     - How did consumers pay for the product?

Backwards
Typical Spam Routing Headers

Return-Path: q0koco@aol.com

Received: from massena-2-81-57-128-46.fbx.proxad.net ([81.57.128.46]) by lakemtai08.cox.net (InterMail vM.5.01.06.05 201-253-122-130-105-20030824) with SMTP id <20040115161857.JKJM5944.lakemtai08.cox.net@massena-2-81-57-128-46.fbx.proxad.net>; Thu, 15 Jan 2004 11:18:57 -0500

Received: from [61.220.187.85] by massena-2-81-57-128-46.fbx.proxad.net id N1tbyb9rILTH; Thu, 15 Jan 2004 13:13:56 -0300

Message-ID: oj$73un7$palnx2617cbe0@wuy7.69oi.k2

From: "Chris Chamberlain" <q0koco@aol.com>

Reply-To: "Chris Chamberlain" <q0koco@aol.com>

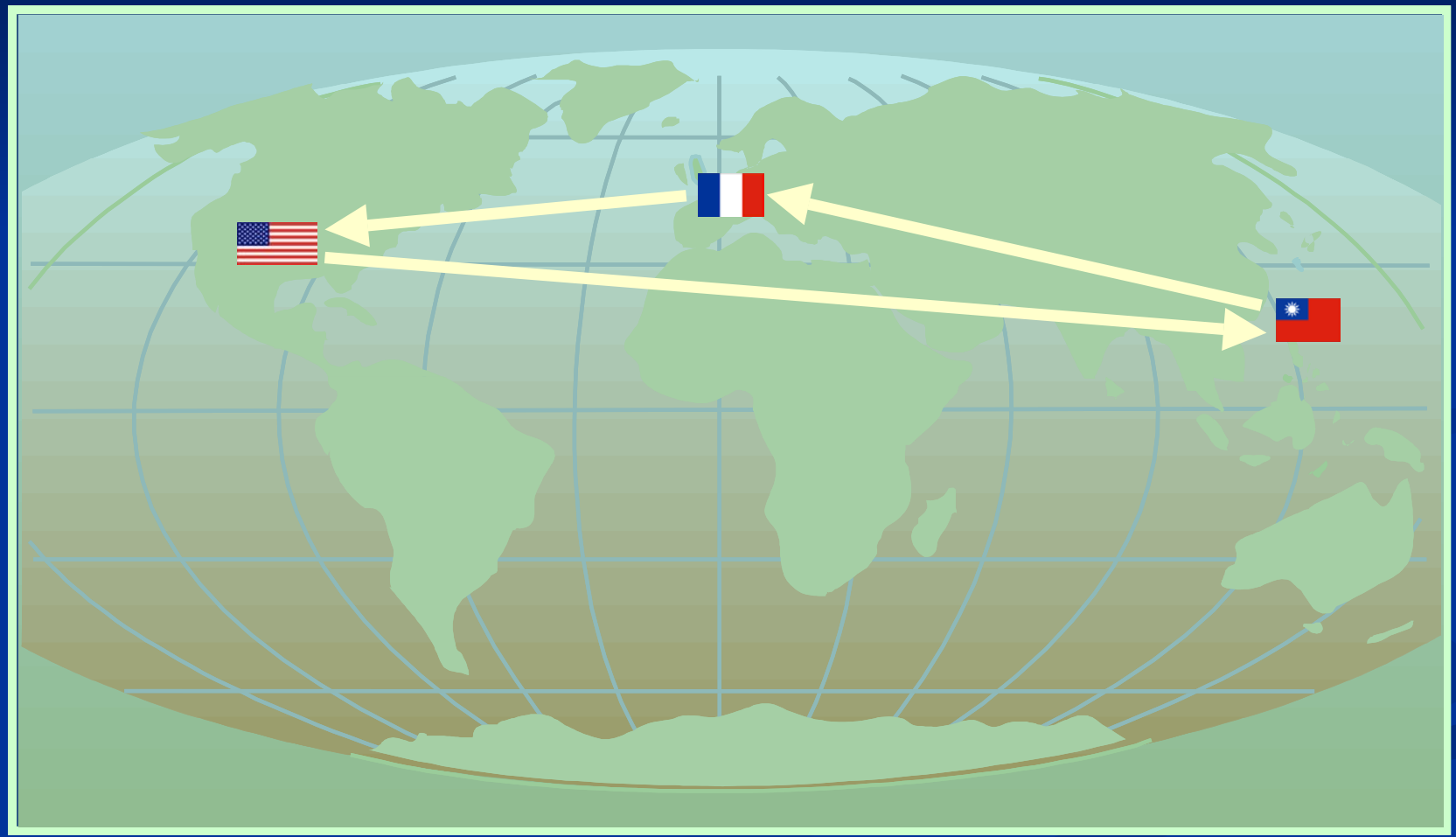
To: dblumenthal@cox.net

Subject: Fwd:I need your help...

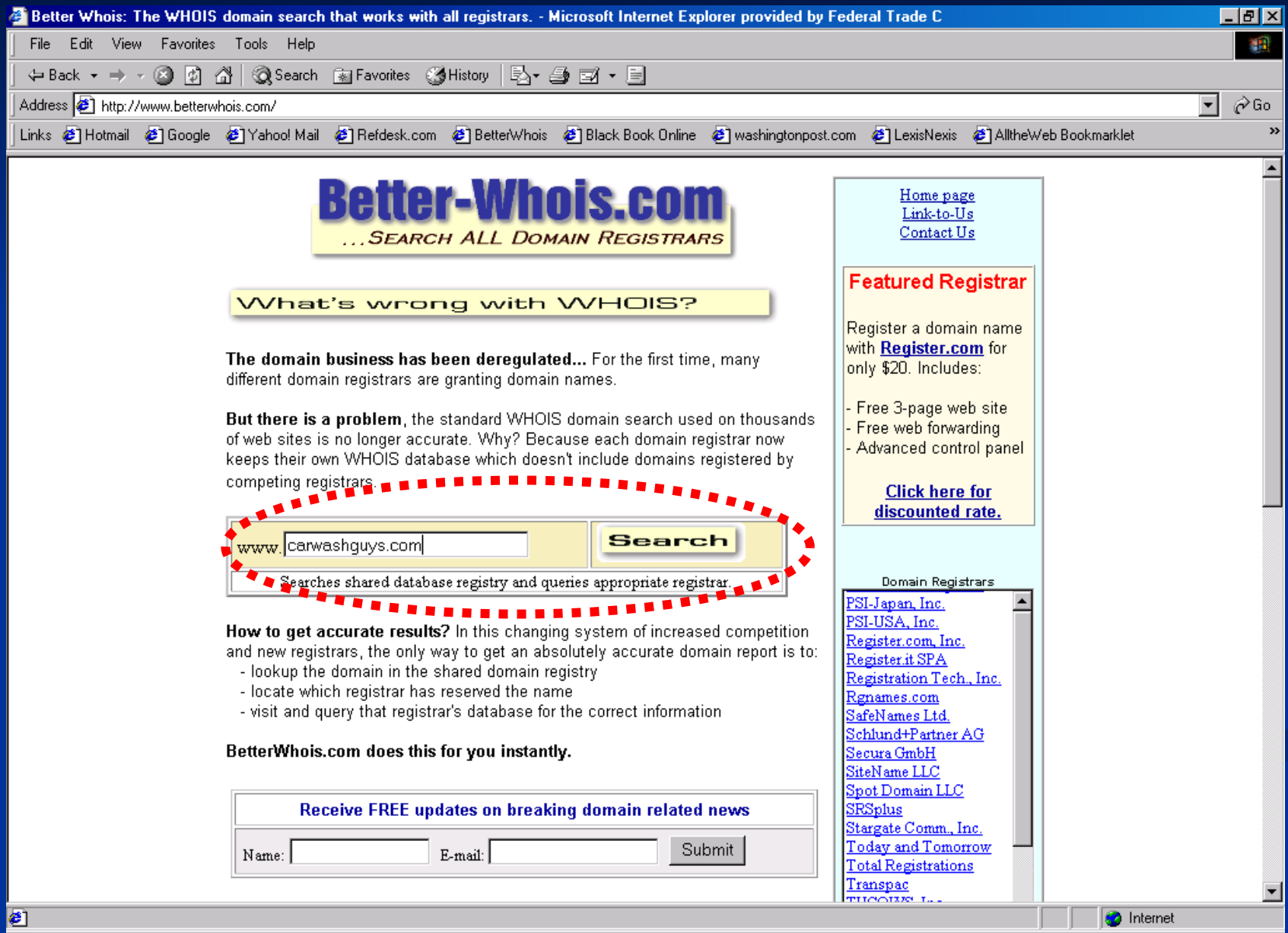
Date: Thu, 15 Jan 04 13:13:56 GMT

Possibly Forged

Backwards Multinational Path



Forwards - Investigating a Web site - Whois



Forwards – Following the money

- Credit card records
- Checks/Bank records
- Postal money orders

Federal Trade Commission

SUBPOENA #1

IP Address

Web host

SUBPOENA #2

Subscriber info

ISP

SUBPOENA #3

Phone records

Phone Co.

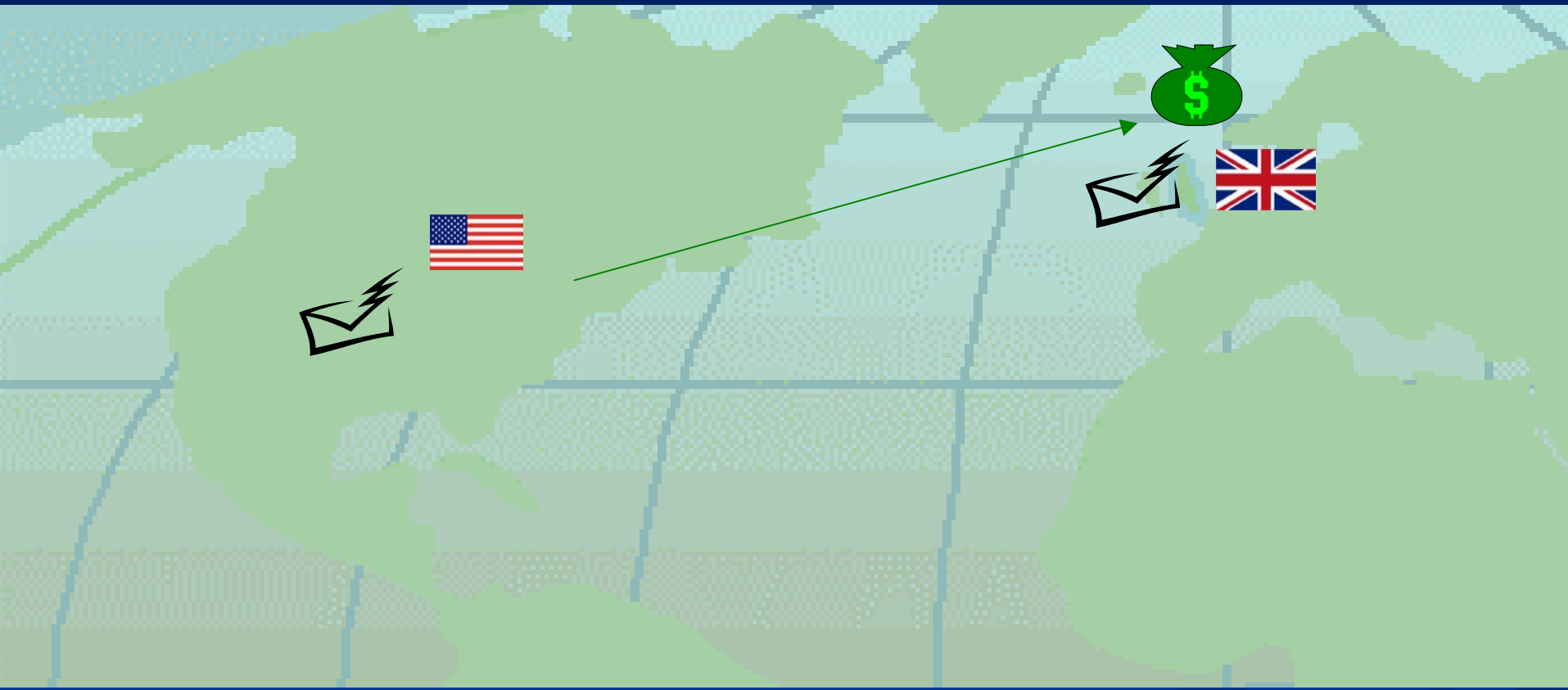
CID Response:
Registration Information for Free Web Page

Mickey Mouse **FAKE**
123 Disney Center **FAKE**
Orlando, FL 12345 **FAKE**
Scammer@realaccount.com **REAL**

Registered 4 AUG 2003 04:34:25 GMT **REAL**
Set up IP 12.123.12.1 **REAL**

The Dominica Spam Case

The TLD CASE



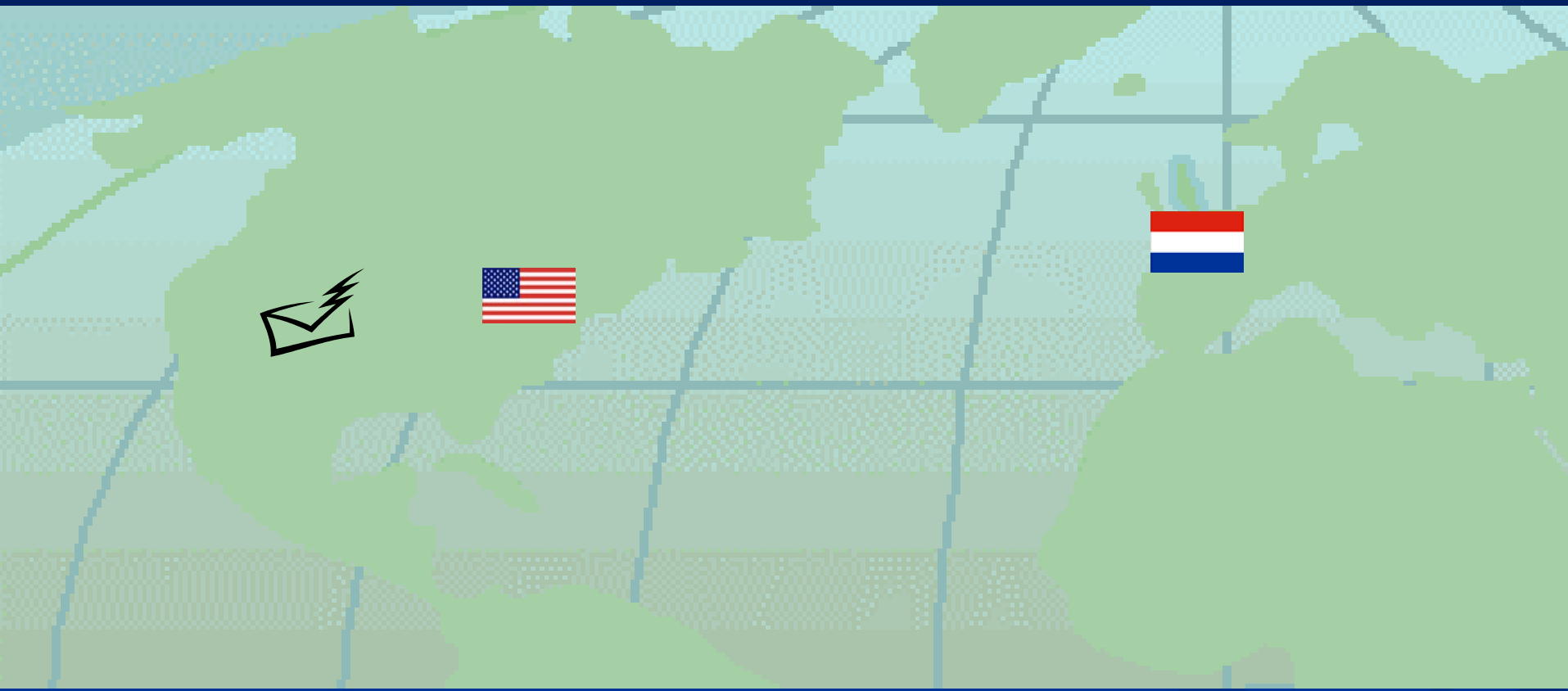
The TLD Case

- The OFT:
  - helped FTC with serving process
  - got an assurance of voluntary compliance from the defendants
- The FTC:
  - shut down the Web sites & froze assets
  - reached a settlement with injunctive relief

The TLD Case

- The challenge: consumer redress-get to the assets
- OFT: no jurisdiction for recovering assets
- Difficulties in recovering money held by third parties in foreign countries

The Westby Case

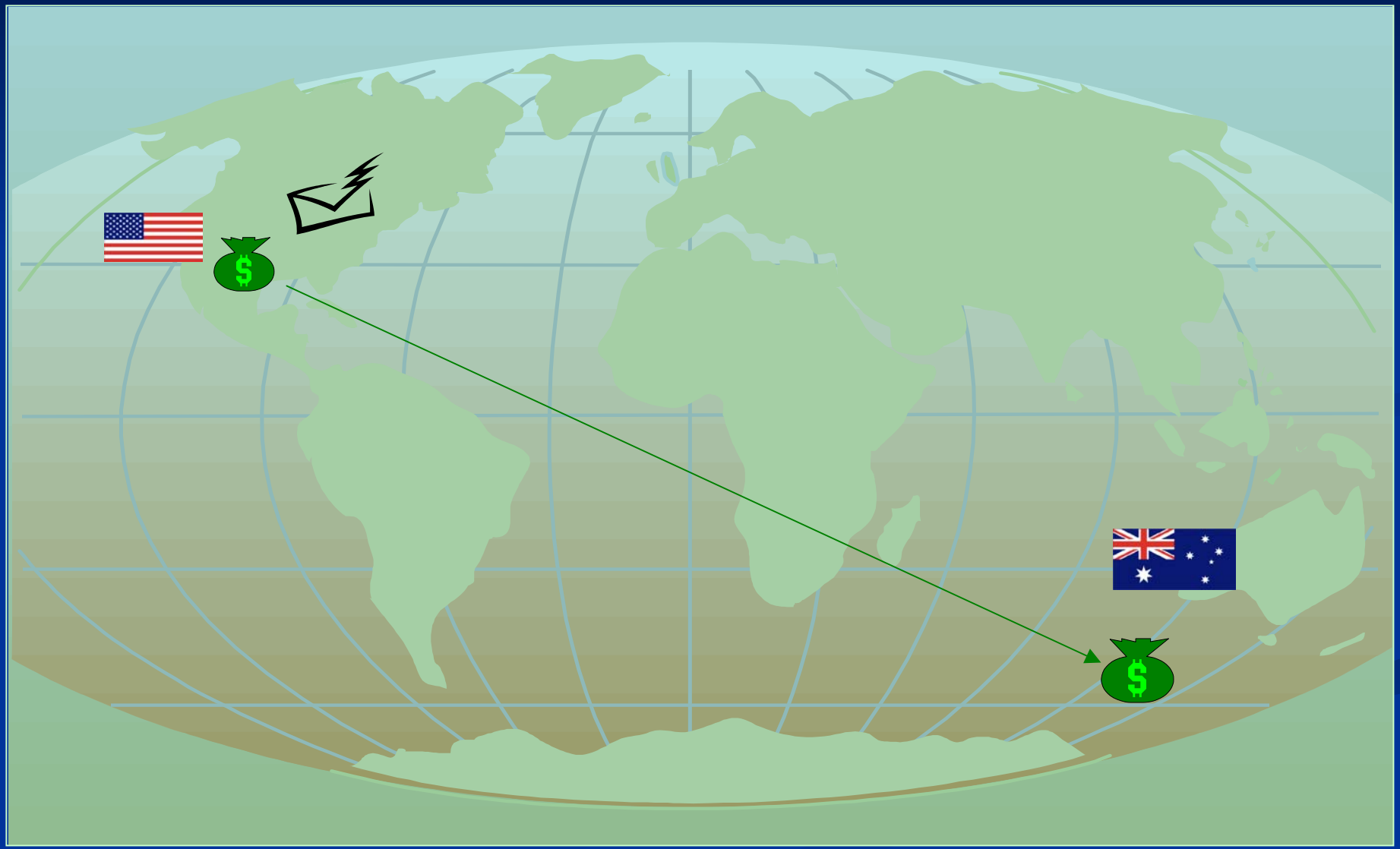


Amended complaint named Dutch individual and two Dutch corporations

The Westby Case - Tracing the money

- The link in the spam directed consumers to an adult page
- A couple of pages into the web site took consumers to a "payment page"
- The payment page identified the third party payment processor
- The source code on the page identified the "merchant" and affiliate of the merchant who were being paid by the payment processor

The Global Web Promotions Case



The Global Web Promotions Case

- Violations of the FTC Act: Deceptive claims
- Violations of the CAN-SPAM Act
  - Spoofing
  - Failure to provide "opt out"
- Assistance from Australia and New Zealand Authorities
- Global Web Promotions agreed to a preliminary injunction

Challenges for Cross-border enforcement

Around the world

Obtaining Evidence

Sharing Evidence

Moving fast

Stopping Misconduct

Recovering Assets

Cross-border enforcement cooperation

Important factors

- Build domestic enforcement capacity
- Look for common ground
- Coordinate between agencies with different functions
- Maximize benefits in case selection
- Information sharing

Cross-border enforcement cooperation

- OECD: Guidelines on Protecting Consumers Across Borders From Fraud and Deception
- US: Proposed International Consumer Protection Act
  - Investigative assistance
  - Information sharing
  - Clarification of jurisdiction and redress authority
  - Authority to negotiate international agreements
- EU: Proposed Enforcement Cooperation Regulation

Gathering Information:

Consumer Complaints, Related Information

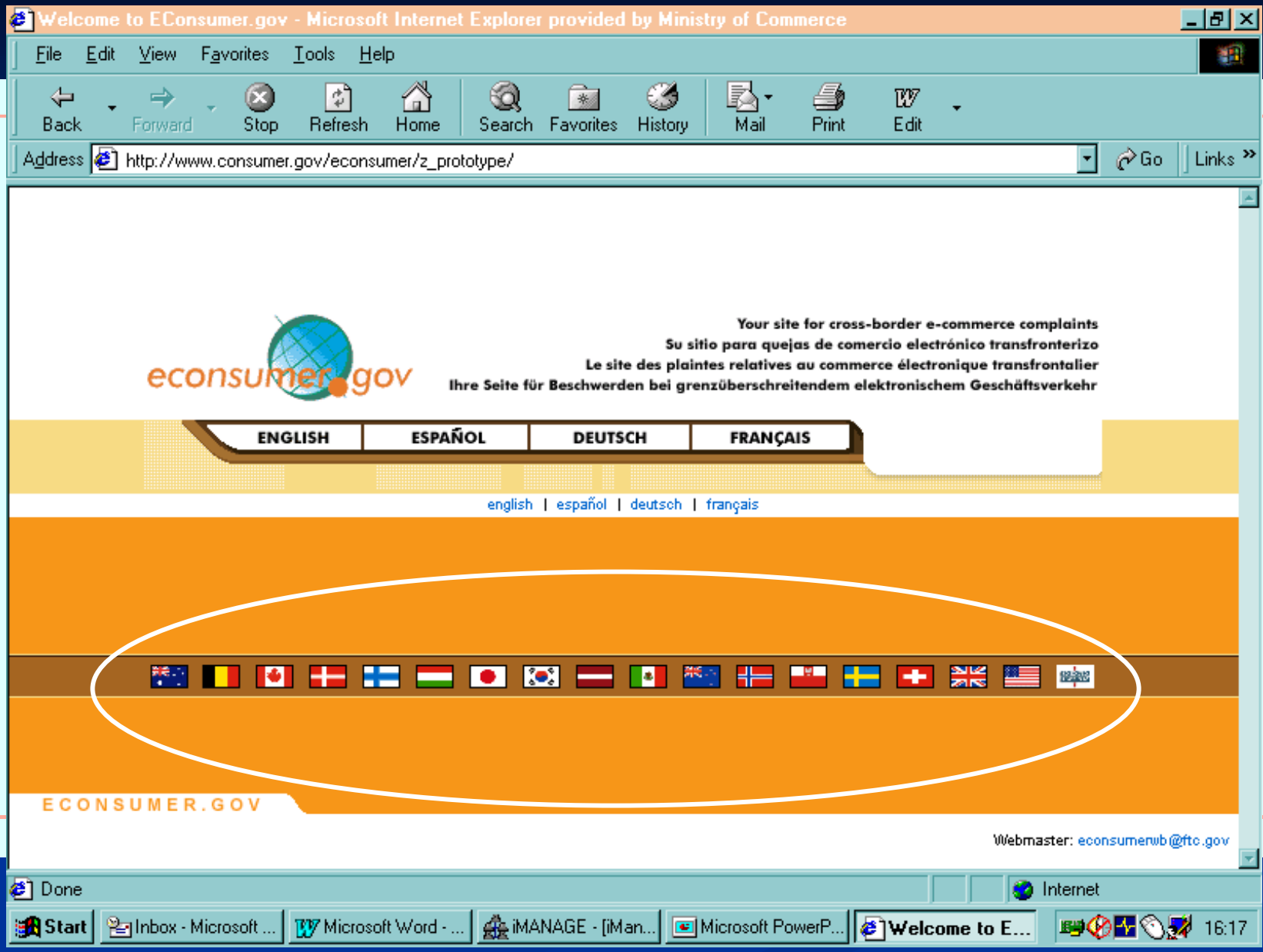
- Restricted-access law enforcement site
- National and international scope (U.S., Canada, Australia)
- Consumer Planet Sentinel: 17 countries can access *econsumer.gov* complaints
- Law enforcers can search for complaints and alert each other of ongoing issues

- Public sites
- Trend information
- Consumer education materials

Spam "refrigerator"

- **More than 100 Million UCEs**

Information Gathering



Looking ahead

- Technology:
  - OECD Korea workshop, September 8-9, 2004
- Enforcement:
  - Meeting on spam enforcement cooperation, London, October 11, 2004
- Authentication
  - FTC Summit, Fall 2004

International Law Enforcement Against Spam

Practical solutions for a difficult problem

Hugh Stevenson
U.S. Federal Trade Commission

FTC Staff presentation. Does not necessarily reflect the views of the Commission or any individual Commissioner.