

OVERCOMING BARRIERS TO INTERNATIONAL CONSUMER PROTECTION ENFORCEMENT



Michael D. Panzera, Esq.
Office of International Affairs
U.S. Federal Trade Commission
December 2014

The views expressed are the presenter's and do not necessarily reflect those of the Commission.



Overview



- I. General Authority of the FTC**
- II. US SAFE WEB Act**
- III. International Fellows Program**
- IV. International Consumer Protection and Enforcement Network (ICPEN)**
- V. Cross-Border Consumer Complaint Databases (econsumer.gov)**
- VI. Case Studies**



I. FTC's Jurisdiction

The FTC enforces the FTC Act, which prohibits “unfair and deceptive practices.”

■ Section 5 prohibits:

- “Unfair methods of competition”

- “Unfair or deceptive acts or practices”



■ Deceptive practices

- Material representation or omission that is...
- likely to mislead consumers...
- who are acting reasonably under the circumstances

■ Unfair practices

- substantial injury that is...
- not reasonably avoidable and...
- not outweighed by benefits

❖ The FTC Act only covers practices in business - not political, artistic, or social speech.

FTC Jurisdiction



- The FTC enforces the FTC Act in a variety of **contexts**, many of which have **cross-border aspects** (e.g., data privacy and security, financial services, e-commerce, mobile devices)
- Additional jurisdiction under **sector-specific laws**, e.g., Telemarketing and Consumer Fraud and Abuse Act, Children's Online Privacy Protection Act (COPPA).
- No jurisdiction over financial institutions, insurance companies, common carrier activity.



PROBLEM!

- Commerce had become increasingly cross-border in nature... and so had fraud.
- **But the jurisdictional limitations of consumer protection authorities remained in place.**

RESPONSE!



The US SAFE WEB Act:
*Protecting Consumers
from Spam, Spyware, and Fraud*
A Legislative Recommendation to Congress

Federal Trade Commission
June 2005



II. US SAFE WEB Act



- * The U.S. SAFE WEB Act amended FTC Act in 2006 to provide new tools to address cross-border fraud. Renewed 2012.
- * Through cooperation with “**Foreign law enforcement agencies**” =
 - * Agency or judicial authority of a foreign government (includes a political subdivision of a foreign state or a multinational organization comprised of foreign states) vested with **law enforcement** or **investigative** authority in **civil**, **criminal**, or **administrative matters**
 - * Any multinational organization acting on the foreign law enforcement agency’s behalf.
- * Broad scope reflects wide range of agencies (e.g., consumer, police, telecommunications) with whom we cooperate

II. US SAFE WEB Act



*Two principal mechanisms:

A. Information sharing

B. Investigative assistance

A. Information Sharing



- * Adds foreign law enforcement agencies to the list of agencies with whom FTC can share **confidential** consumer protection information
- * Authorizes disclosure of consumer protection material obtained pursuant to **compulsory process**

A. Information Sharing



- * **Confidentiality/Official Purpose Certification**
- * The Act requires a prior agreement, MOU, or other written certification stating that the requestor will:
 - * **protect the confidentiality** of the information and
 - * use it for **official law enforcement purposes.**



A. Information Sharing



* IMPORTANT LIMITATIONS

- * Information may be used in connection with a judicial, administrative or other law enforcement proceeding commenced by recipient provided that **prior to any public disclosure** in such a proceeding, submitter of information must be given notice and opportunity to seek appropriate relief pursuant to FTC Rules
- * No other “**onward sharing**” with recipient is permitted without FTC approval
- * Specific requirements for handling and disposing of Sensitive Personally Identifiable Information.

A. Information Sharing



* Other Limitations

- * Approval of appropriate federal banking agency or credit union is required if target is a bank, savings and loan institution, or federal credit union.
- * State Department has not designated foreign state as one that supports terrorism.
- * Excludes antitrust laws (and information obtained from an antitrust investigation)

A. Information Sharing



* Various Contexts

- * Telemarketing
- * Spam
- * E-commerce
- * Pyramid Schemes
- * Deceptive Advertising
- * Personal data protection & security

B. Investigative Assistance



* Type of Assistance

- * FTC may conduct an investigation to collect information and evidence **using all of its investigative powers**, e.g., Civil Investigative Demand.
- * FTC may seek appointment to conduct **civil discovery** on behalf of civil authorities, or on behalf of criminal authorities when referred by the Attorney General.



B. Investigative Assistance

- * **Foreign Law Enforcement Agency Request**
 - * Written request must state that agency has an investigation or enforcement proceedings for:
 - * violations of laws prohibiting fraudulent or deceptive practices, or
 - * practices “**substantially similar**” to those prohibited by FTC laws.
 - * Excludes federal antitrust laws



B. Investigative Assistance

* Criteria for Determination

- * Whether the requester has agreed to provide **reciprocal assistance**
- * Whether compliance would prejudice US public interest
- * Whether the investigated practice involves injury to a significant number of persons

B. Investigative Assistance



* Procedures

- * Requesters Must Complete “Request for Investigative Assistance” Form, including confidentiality certification, and
 - * Provide copies of applicable statutes, laws, or rules (including translations)
 - * Note any special procedural or evidentiary requirements
- * Office of International Affairs staff then works with foreign agency representative to refine request.
- * Once FTC obtains requested information, it shares it with foreign agency under information sharing authority and procedures.
- * Requester must comply with certification and terms of “Access letter”



B. Investigative Assistance

- * 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 as of mid-2012.
- * The FTC has issued 52 civil investigative demands (equivalent to administrative subpoenas) in 21 investigations on behalf of nine agencies in five countries.
- * In cases relying on the US 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 consumers hundreds of millions of dollars.

II. SAFE WEB: RESULTS



- * 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.
- * Approximately **63 SAFE WEB information sharing requests** completed with 17 foreign enforcement agencies
- * The FTC has issued **93+ civil investigative demands in 39 investigations** on behalf of 9 agencies (criminal and civil) in various countries
- * In cases relying on the US 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 consumers hundreds of millions of dollars.

III. International Fellows Program



- * FTC participates in staff exchanges with non-U.S. competition, consumer protection, and privacy agencies for terms of 3-6 months.
- * International Fellows participate in investigations, enforcement actions, and other projects with FTC attorneys, investigators, and economists.
- * Fellows return to home agencies prepared to share what they have learned and ready to apply their experience to help improve cross-border cooperation through the relationships they have developed.
- * Since 2007, the FTC has hosted 46 staff members from agencies all around the world.



IV. International Consumer Protection and Enforcement Network (ICPEN)



International Consumer
Protection and Enforcement Network

PROTECTING CONSUMERS WORLDWIDE



About ICPEN

Search



[Sitemap](#)

[Contact](#)

[RSS](#)

Welcome to the website of the International Consumer Protection and Enforcement Network (ICPEN) – an organization composed of consumer protection authorities from almost 40 countries, whose aim is to:

- ▶ Protect consumers' economic interests around the world.
- ▶ Share information about cross-border commercial activities that may affect consumer welfare.
- ▶ Encourage global cooperation among law enforcement agencies.

For consumers



Find out how to shop online wisely, avoid scams, where to seek consumer assistance abroad and what ICPEN does for you. ▶

For consumer experts



Find out more about ICPEN, what we do and how you can join in our work. Check out our resources and learn more about consumer protection worldwide. ▶

News

[United States - Telephone Bill Cramming](#)

[United Kingdom - OFT's approach to](#)

[MEMBERS LOGIN](#)

IV. ICPEN



- * Comprises 53 international members. Additional partners orgs and observers & guests.
- * Regional Collaborations created
- *
- * Mission, a strategy and a “Unique Selling Proposition” with the goals of protecting consumers by **encouraging and facilitating practical action** to prevent cross border marketing malpractice, **sharing information** on market developments and regulatory best practice, and **coordinating among members** to tackle market problems.

IV. ICPEN's International Partners



UNITED NATIONS
UNCTAD

ORGANISATION
FOR ECONOMIC
CO-OPERATION
AND DEVELOPMENT



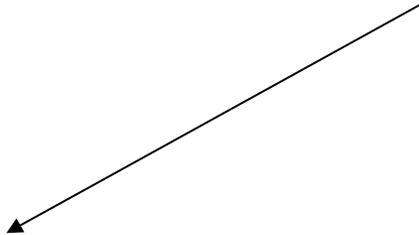
ASSOCIATION
OF SOUTHEAST
ASIAN NATIONS



London Action Plan

International spam enforcement network

V. Shared Databases econsumer.gov



The screenshot shows the homepage of econsumer.gov. At the top, there is a language selection dropdown set to "English" and a "Go" button. Below this is the site's purpose: "Your site for cross-border consumer complaints." Navigation links include "About Us", "Member Countries", and "Privacy Policy". A main menu bar contains "HOME", "REPORT YOUR COMPLAINT", "RESOLVE YOUR COMPLAINT", and "NEWS & RESOURCES". The main content area features a "What is econsumer.gov?" section, a "Report Your Complaint" button with a description of the site's function, and a "Ways to Resolve Your Complaint" button. A "FEATURED STORY" section highlights a "U.S. Court Halts Counterfeit Check and Prize Scam". A "econsumer News Feed" section includes a link to "Commission Proposes New Light Bulb Labels, Seeks Public Comments".

The screenshot shows the "Consumer Sentinel Network" page, which is part of the Federal Trade Commission's "TIP v. Complaint" initiative. The page is titled "Law enforcement's source for consumer complaints". It includes a "Sustained Information" sidebar with links to Home, Consumer Sentinel Fact Sheet, Members, Reports, Newsletters, Consumer Tips, Data Contributors, Econsumer.gov, and Consumer Sentinel/Military. The main content area provides a detailed overview of the network, listing various types of complaints it handles (e.g., Identity Theft, Do-Not-Call Registry violations, Computers, the Internet, and Online Auctions, Telemarketing Scams, Advance-fee Loans and Credit Scams, Sweepstakes, Lotteries, and Prizes, Business Opportunities and Work-at-Home Schemes, Health and Weight Loss Products, Debt Collection, Credit Reports, and Financial Matters). It also describes the network's enhanced search engine and user interface, and provides information on how to become a member and the system requirements.



econsumer.gov provides certified law enforcement and regulatory agencies in over 30 ICPEN member countries access to consumer complaints to assist in investigating fraud and uncovering new scams.

Gaining Access to econsumer.gov Data



- * Set up to be inclusive, so that any ICPEN or OECD country's consumer agency with enforcement-related authority could participate

- * Also permits other consumer enforcement agencies to join as long as no one objects

- * Three main steps required:
 - * (a) signing the basic MOU (most ICPEN members have already done that);
 - * (b) filling out paperwork to confirm the agency's consumer enforcement role; and
 - * (c) signing confidentiality and data security agreements.

- * Foreign criminal law enforcement participants may become certified for access by signing confidentiality and data security agreements, so long as the consumer protection agency in your country is a member and agrees

V. Shared Databases: Consumer Sentinel



- * Through the Consumer Sentinel Network, the FTC shares fraud data with law enforcement officials from U.S., Canadian and Australian federal, state and local agencies, including the 50 state Attorneys General.
- * The Consumer Sentinel Network also serves as a portal through which ICPEN member agencies can access cross-border complaints that have been filed through the www.econsumer.gov site.



V. Shared databases



Consumer Complaints As An Enforcement Tool

- * The Consumer Sentinel / econsumer.gov databases help us identify:
 - * **Patterns and trends** in consumer fraud and identity theft
 - * The **issues and actors** causing the greatest harm to consumers
- * The complaint collection process also helps the FTC assist consumers and businesses by providing them with educational materials.



V. Shared Databases



How Members Use Complaint Information

- * Staff who are **investigating a business** can search the appropriate complaint databases
- * In some instances, staff calls a complaining consumer for more information about the business
- * **Voluntary** (may be anonymous)
- * **Individual consumers and organizations** (like BBB)
- * In some instances, the FTC asks consumers who have filed complaints with the FTC to serve as **witnesses** in the cases we file in federal court





CASE STUDIES

1. Best Price Brands
2. Designer Brand Outlet
3. Tech Assistance Scams
4. Aegis
5. Nigerian Spam Scams
6. Skechers sneakers case

1. Best Priced Brands, LLC



- The FTC's first case against a U.S. company doing business *exclusively* abroad since the US SAFE WEB Act took effect in 2006.
- Best Priced Brands is a California company that deceptively sold electronic products to consumers in the United Kingdom through its websites, www.bestpricedbrands.co.uk and www.bitesizedeals.co.uk.
- The company mislead consumers into believing they were purchasing items from a UK-based company in part to various deceptive tactics:
 - Including use of the “.co.uk” top-level domain name
 - Stating prices in British Pounds (£)
 - Using the term “Royal Mail” to describe shipping methods.
- Upon receiving the items, consumers discovered they had been charged unexpected import duties, and that many of the items had invalid warranties; if they tried to return the items, they would be charged exorbitant refund and cancellation fees.

Best Priced Brands: FTC Allegations



- Through the econsumer.gov portal, many consumers in the UK registered complaints with the FTC.
- Assisted in its investigation by the U.K. Office of Fair Trading, the FTC filed a complaint against Best Priced Brand parent company, Balls of Kryptonite, and its owner Jaivin Karnani.
- The FTC's complaint alleged the following counts:
 1. False and Misleading Representations that Defendants were located in the UK and thus items would come with British manufacturers' warranties.
 2. False and Misleading Representations that the price for goods sold was the total cost delivered.
 3. False and Misleading Representations that Defendants were located in the UK and thus give unconditional right to cancel orders and have no restocking fees for returned merchandise.
 4. Violations of the Joint US-EU Safe Harbor Framework.
 5. Violations of the Mail Order Rule.

2. Designer Brand Outlet (DBO)



- * Online business that sells and designer brand name clothes at prices significantly below retail costs. DBO represents itself as operating out of Sydney, Australia.
- Consumers' complaints alleged DBO engaged in the following deceptive practices:
 - Accepting payment and failing to deliver goods (including provision of allegedly false shipping details);
 - Goods returned with no refund given;
 - Consumers receiving goods that vary from those advertised, are defective or are non-authentic; and
 - Consumers unable to elicit response from the business



www.designerbrandoutlet.com

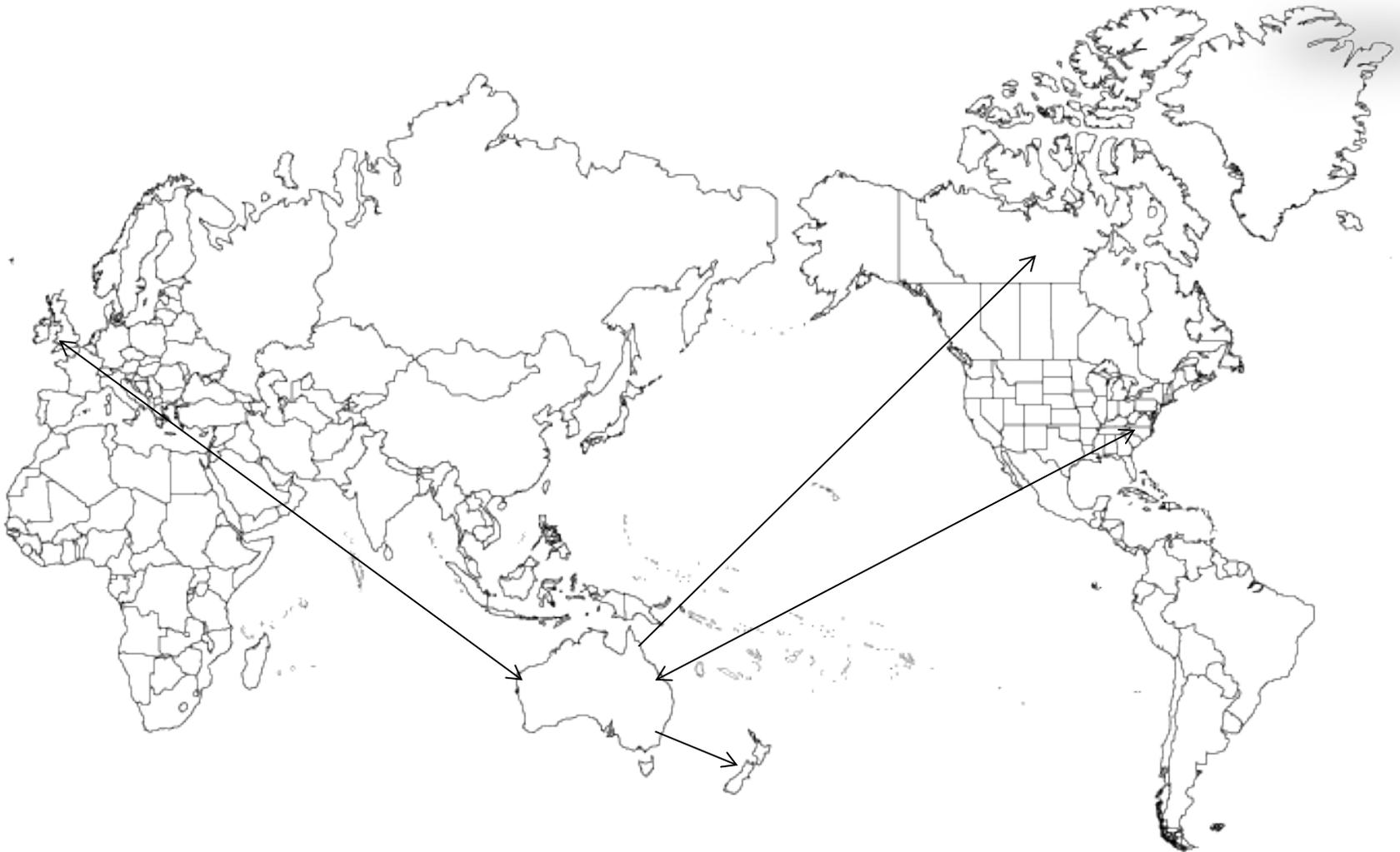
2. DBO



Cross-Border Cooperation

1. FTC identifies series of complaints on **eConsumer.gov** and provides them to the Australian Competition and Consumer Commission (ACCC) to initiate an investigation
2. ACCC makes inquiries with UK, Canada & NZ counterparts about any complaints regarding DBO
3. Based on info provided by FTC and others, ACCC obtains restraining order and brings case against DBO
4. FTC and UK Office of Fair Trading provide witness statements for proceedings
5. Outcome: Australian court bars DBO from engaging in similar conduct for five years and demands payment of ACCC's legal costs

2. DBO Cross-Border Cooperation



3. Tech Support Scams



- * Scammers pretending to be employees of Microsoft, Dell, Norton or McAfee call consumers and say they have detected a virus or “issues” with their computers.
- * The callers offer to provide a software “fix” by asking the victim to visit a third-party website that enables remote access to their computer, for which the scammer charged up to \$450.
- * The operations were largely based in India and are estimated to have ripped off tens of thousands of consumers in Australia, New Zealand, Canada, Ireland, the U.K., and the U.S.
- * Scammers attempt to avoid detection by using 130 different phone numbers and 80 different domain names online.

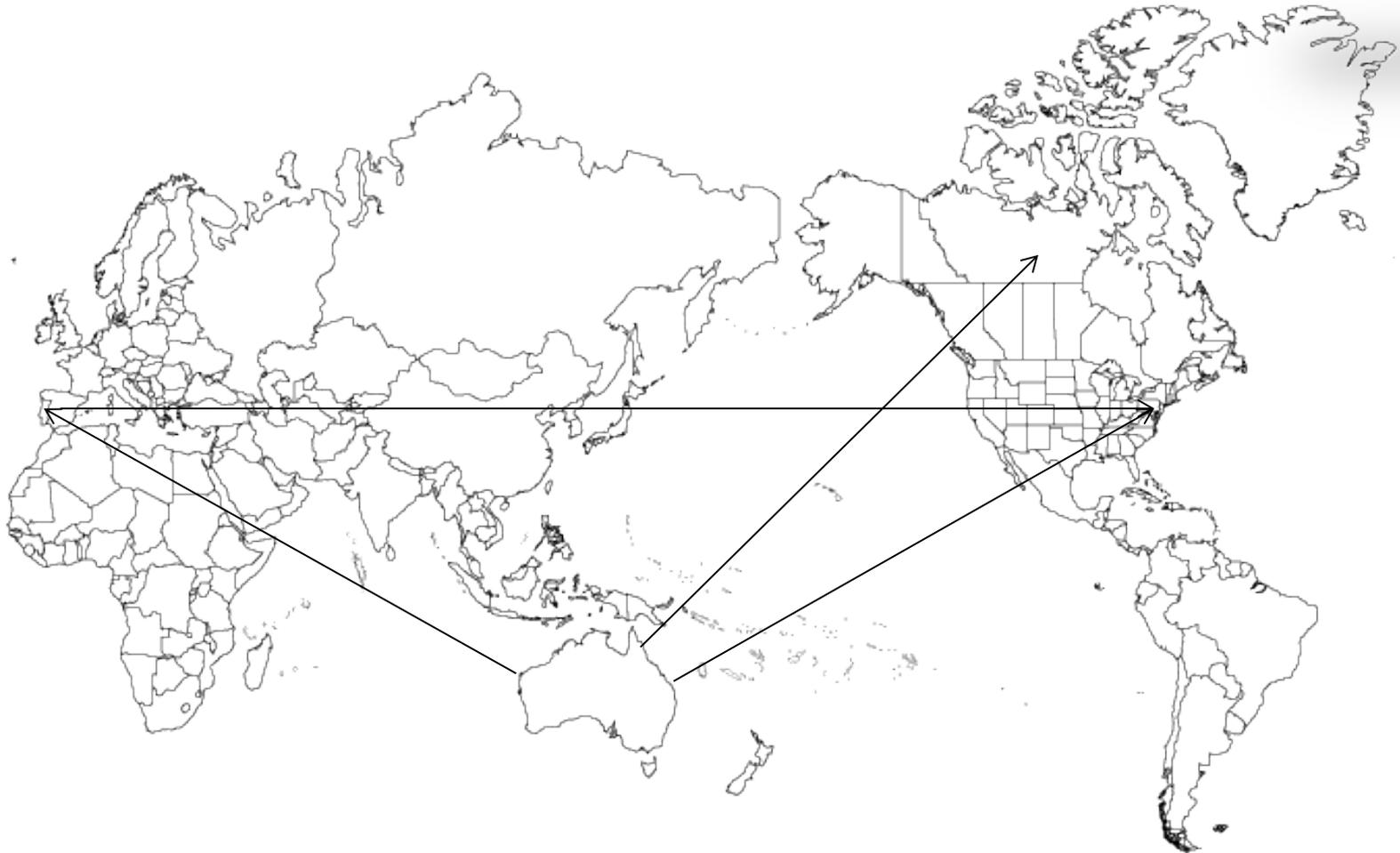


3. Tech Support Scams: Cross-Border Cooperation



- * From 2009 to 2011, the Australian Communications and Media Authority (ACMA) received nearly 10,000 complaints via its Do-Not-Call Hotline.
- * The ACMA, Canadian Radio-television and Telecommunications Commission (CRTC) and United Kingdom's Serious Organised Crime Agency (SOCA) all shared data with the FTC to pursue individual enforcement actions against the scammers.
- * The FTC froze funds of U.S.-based parties alleged to be involved in the scam, while Canadian authorities administered a fine of \$490,000 to one of the companies involved, Pecon Software.

3. Tech Support Scams: Cross-Border Cooperation



4. Aegis



- The Canadian Competition Bureau litigated a “**cramming**” case against several players in the Canadian wireless telephone market, alleging that Canada’s three largest wireless companies deceptively marketed premium text messaging and digital content services, and is seeking over 30 million dollars in penalties.
- The Bureau requested the FTC’s assistance after it was revealed that key evidence in the case was located in the U.S.
 - One of the defendants, an industry association, had contracted with a third-party company in the U.S. to capture and monitor the exact marketing messages at issue in the case.
- The FTC obtained a court order requiring the third party to turn over their records, which the FTC then shared with the Canadian Competition Bureau.

5. Fraudes Nigerianos

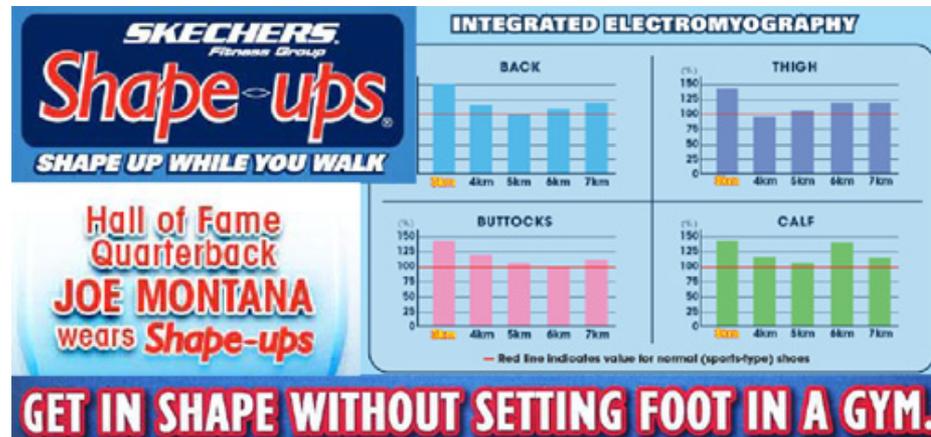


- Since 2012, the Spanish National Police have been pursuing a criminal ring that has laundering millions of euros in proceeds from the “Nigerian scam.”
 - The scheme involved spamming victims with emails that persuaded them to pay large sums of money upfront for future financial rewards that never materialize.
 - Between January 2011 and December 2012, the victims – mostly in the U.S., Canada, and Germany – sent over \$15 million to transfer booths across Spain.
 - Using fake IDs, the scammers wired small amounts of money back to Nigeria through Western Union.
- The FTC, U.S. Criminal Complaint Center, and the Canadian Anti-Fraud Center shared consumer complaints with the Spanish National Police via Europol, and in July 2014 this culminated with the Spanish National Police arresting 84 Western Union agents involved in the frauds, 80% of whom were Nigerian citizens.

6. Skechers Toning Sneakers



- In May 2012, Skechers USA, Inc. agreed to pay \$40 million to settle charges with the FTC that it deceived customers by making unfounded claims about its “Shape-up” and “toning” sneakers.
- Skechers’ ads claimed the shoes would help people lose weight, promote cardiovascular health, and strengthen and tone their buttocks, legs and abdominal muscles.
- Ads also included an “endorsement” from a chiropractor based on an “independent clinical study,” which Skechers allegedly paid for.
- The sneakers ranged in price from \$60-\$100 a pair, and the settlement was used to provide eligible consumers with a refund.
- In Colombia and Mexico, the FTC’s consumer protection counterparts filed similar claims against Skechers’ subsidiaries doing business in their respective countries.



THANK YOU!



Michael D. Panzera, Esq.

Office of International Affairs
U.S. Federal Trade Commission
600 Pennsylvania Ave, N.W.
Washington, DC 20580
(202) 326-2256 (tel)
(202) 326-3045 (fax)
dwoodsbell@ftc.gov